“VASIL LEVSKI” NATIONAL MILITARY UNIVERSITY

“ARTILLERY, AIRCRAFT DEFENSE AND CIS” FACULTY

INTERNATIONAL SCIENTIFIC CONFERENCE “DEFENSE TECHNOLOGIES” 2026

C O N F E R E N C E P R O C E E D I N G S

DEFENSE AND SECURITY

WEAPONS, TECHNOLOGIES, LOGISTICS

COMMUNICATION AND COMPUTER TECHNOLOGIES

CYBERSECURITY AND AI

SOCIAL STUDIES

GEODESY

Shumen, Bulgaria
2026

TO THE READERS

This collection is divided in three parts and includes science papers presented on the International Scientific Conference "DEFENSE TECHNOLOGY 2025" in "Artillery, Aircraft Defense and CIS" Faculty, Shumen, Bulgaria. Authors are responsible for the contents and the papers are not further edited after sending for publication.

The reviewers committee will be thankful for all proposed notes, corrections and replies.

Reviewers committee

REVIEWERS COMMITTEE

Prof. Eng. **K. KALEV**, PhD, NMU
Col. Assoc. Prof. Eng. **S. CHANEV**, PhD, NMU
Prof. Eng. **Ch. MINCHEV**, PhD, NMU
Col. Assoc. Prof. Eng. **M. LAMBEVA**, PhD, NMU
Col. Prof. Eng. **C. CONEV**, PhD, NMU
Col. Assoc. Prof. Eng. **S. ANTONOV**, PhD, NMU
Assoc. Prof. **R. BOGDANOV**, PhD, NMU
LTC Assoc. Prof. Eng. **L. NIKOLOV**, PhD, NMU
Col. Eng. **A. C. SAVA**, PhD, MTA"Ferdinand I", Romania
Maj. Eng. **C. GRUMĂZESCU**, PhD, MTA "Ferdinand I", Romania
Col. Prof. Eng. **E. TRANĂ**, PhD, MTA "Ferdinand I", Romania
Col. Prof. Eng, **A. ROTARIU**, PhD, MTA "Ferdinand I", Romania
Col. Prof. Eng. **L. MATACHE**, PhD, MTA "Ferdinand I" Romania
Col. Assoc Prof. Eng. **S. TOMA**, MTA "Ferdinand I", Romania
Maj. Assoc. Prof. Eng. **F. BUCUR**, PhD, MTA "Ferdinand I", Romania
Maj. Assoc. Prof. Eng. **A. CÎRNEANU**, PhD, MTA "Ferdinand I", Romania
LTC **C. ENE**, PhD, "Henry Coanda" AFA
Col. Prof. Eng. Grzegorz **PILARSKI**, PhD, WSU, Poland
LTC Assoc. Prof. Eng. **B. BIERNACIK**, PhD, WSU, Poland
LTC Assoc. Prof. Eng. P. **OSTOLSKI**, PhD, WSU, Poland
LTC Assoc. Prof. Eng. Michał **WILK**, PhD, WSU, Poland
LTC Assoc. Prof. Eng. Tomasz **SURWIŁŁO**, PhD, WSU, Poland
Col. Eng. **J. ZELKOWSKI**, PhD, MUT, Poland
DSc Prof. Eng. **R. WOŹNIAK**, PhD, MUT, Poland
DSc Prof. Eng. **J. JANISZEWSKI**, PhD, MUT, Poland
Col. DSc Prof. Eng. **A. KOZAKIEWICZ**, PhD, MUT, Poland
Lecturer. **D. DUMITRU**, PhD, "Spiru Haret "University, Romania
Assoc. Prof. **M. MIHĂILESCU**, PhD, "Spiru Haret" University, Romania
P. BERNAT, PhD, Polish Air Force University, Demblin, Poland
Prof. D.Sc.Eng. **A. TEILANS**, Riga Technical UNIVERSITY - Rezekne Academy, Latvia
Prof. D.Sc. Eng. **L. LAZOV**, D.h.c, Riga Technical UNIVERSITY - Rezekne Academy, Latvia

© "Vasil Levski" National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, 2026.

c/o Jusautor, Shumen

Национална научна програма 7.1 „Сигурност и отбрана"

ISSN 2815-4282 - онлайн издание

CONTENT

PLENARY SESSION..... 11

ATTACK SURFACE OF OPEN SPATIAL DATA INFRASTRUCTURES: A SYSTEMATIC THREAT MODEL FOR OGC SERVICE STACKS
Stefania Loredana Nita[1], Alexia Ioana Dragomir[1], Marius Iulian Mihailescu[2], Valentina Marascu[3]12

EMERGING AND DISRUPTIVE TECHNOLOGIES IN ARMAMENT SYSTEMS: TECHNICAL, EDUCATIONAL AND REGULATORY PERSPECTIVES
Marius Valeriu Cîrmaci Matei 22

THE GROWING IMPORTANCE ON AN ARTIFICIAL INTELLIGENCE IN MILITARY AND PUBLIC SERVICES ACTIVITY – CASE STUDY
Bartosz K. Biernacik.....30

MODERN VS. TRADITIONAL BINDERS IN ILLUMINATING PYROTECHNIC COMPOSITIONS: A COMPARATIVE STUDY
Florin-Marian Dîrloman[1], Mario-Gabriel Văncică[1], Sebastian Nistor[1], Sergiu-Emilian Țurloiu[1], Bogdan-Gheorghe Pulpea[1], Constantin Enache[1], Octavian Chiriac[1] 43

DEFENSE AND SECURITY 61

THE ILLEGAL TRAFFICKING OF CULTURAL PROPERTY
Veliko P. Petrov.....62

DEFINITION OF THE CONCEPT OF "CULTURAL VALUE" IN INTERNATIONAL DOCUMENTS
Veliko P. Petrov.....74

TRENDS AND CHALLENGES IN THE DEVELOPMENT OF ANTI-TANK ROBOTIC SYSTEMS
Veliko P. Petrov.....87

HISTORY OF THE DEVELOPMENT OF THE LEGAL PROTECTION OF CULTURAL VALUES
Veliko P. Petrov.....102

ANTI-TANK MISSILE COMPLEXES IN MODERN ARMED CONFLICTS
Veliko P. Petrov.....112

THE COMBAT EMPLOYMENT ON ANTI-TANK MISSILE COMPLEXES IN MODERN ARMED CONFLICTS
Veliko P. Petrov.....121

THE NORTHERN SEA ROAD – WHAT IS IT IMPORTANT FOR? A BRIEF ANATOMY OF THE ARCTIC BRIDGEPORT.
Stoyan G. Stoychev 130

MAPPING THE EVOLVING ADVERSARY - A LONGITUDINAL ANALYSIS OF ADVANCED PERSISTENT THREAT TACTICS AND DEFENSIVE CO-EVOLUTION
Marius Iulian Mihailescu[1], Stefania Loredana Nita[2], Laurentiu Bogdan Asalomia[4], Valentina Marascu[1,3] 141

CRISIS MANAGEMENT AS A GUARANTEE OF NATIONAL SECURITY
Kaloyan A. Iliev, Ivan K. Vladov 151

COMMAND AND CONTROL IN THE AGE OF ARTIFICIAL INTELLIGENCE
Kaloyan A. Iliev, Alexandra K. Vladova 159

RESILIENT NAVIGATION AND CONTROL OF STRIKE UAVS IN GNSS-DENIED AND ELECTROMAGNETICALLY CONTESTED ENVIRONMENTS
Jordan Alexiev 166

CLASSIFICATION OF AUTONOMOUS FUNCTIONS IN STRIKE UAVS
Jordan Alexiev 174

AUTONOMOUS EXECUTION OF STRIKE UAV MISSIONS: FUNCTIONAL AUTONOMY PROFILES
Jordan Alexiev 182

TECHNOLOGICAL EVOLUTION OF THE MINE COUNTERMEASURES SHIP SUBSYSTEM: TRANSITION TO INTEGRATED UNMANNED MODULES AND SENSOR NETWORKS
Krasimir S. Angelov 189

CURRENT CAPABILITIES OF THE MINE COUNTERMEASURES FORCES OF THE BLACK SEA FLEET OF THE RUSSIAN FEDERATION IN THE CONTEXT OF MODERN NAVAL CHALLENGES
Krasimir S. Angelov 197

QUANTITATIVE AND QUALITATIVE ANALYSIS IN CHOOSING OPTIONS FOR DEVELOPING NAVAL MINE COUNTERMEASURES CAPACITY
Krasimir S. Angelov 206

CIVIL-MILITARY COOPERATION IN NON-MILITARY CRISIS
Anton I. Manchev 213

BULGARIA AND THE BLACK SEA DIMENSION OF Regional SECURITY THROUGH THE PRISM OF THE MILITARY SPHERE OF THE TURKISH GEOSTRATEGIC PROJECT `BLUE FATHERLAND` AND THE RUSSIAN `NEUTRAL UKRAINE`
Michael P. Kozarski 221

CHALLENGES ENCOUNTERED IN EMERGENCY MANAGEMENT INVOLVING THE ARMED FORCES OF THE REPUBLIC OF BULGARIA
Ivan K. Vladov 234

ANALYSIS OF ATTITUDES AND MOTIVATION FACTORS IN CHOOSING HIGHER MILITARY EDUCATION
Ivaylo Zh. Bozov 239

INFLUENCE OF ATGMS IN COMBAT OPERATIONS
Ivaylo Zh. Bozov 246

EVOLUTION OF TECHNOLOGIES USED BY INTERCEPTOR DRONES
Ivaylo Zh. Bozov 251

OPPORTUNITIES FOR THE USE OF ATGM IN OPERATIONS
Ivaylo Zh. Bozov 256

LAYERED AIR-DEFENCE SYSTEM: SYNTHESIS, OPERATIONAL ANALYSIS AND MATHEMATICAL MODELING
Stoyan N. Chanev, Matei K. Kirov, Stanimir H. Parvanov 263

RECONNAISSANCE UNMANNED AERIAL SYSTEMS IN ARTILLERY: MODERNIZING TARGET ACQUISITION AND FIRE CONTROL FOR THE BULGARIAN LAND FORCES
Ivan K. Vladov, Daniel R. Rusev, Viktor D. Marinchev 272

ERASMUS+ KA02 PROJECT DIMAS FINAL ISSUES AND RESULTS ANALYSIS
Linko G. Nikolov[1], Dilyan I. Dimitrov[2], Krasimir O. Slavyanov[3].....281

FUNCTIONING AND MILITARY EMPLOYMENT OF UNMANNED AERIAL SYSTEMS: STATISTICAL ANALYSIS OF DESIGN CONCEPTS, MISSION ROLES AND EMPLOYMENT TRENDS
Deyan N. Dimitrov 292

INNOVATIVE ALGORITHMS FOR RADAR INFORMATION PROCESSING: SPARSE RECOVERY, TRANSFORMERS, DEEP UNFOLDING AND COGNITIVE RADAR
Stanimir H. Parvanov, Ivan Y. Radev, Dilyan I. Dimirov.....302

ANALYSIS AND MATHEMATICAL MODELING OF AIR AND MISSILE DEFENSE SYSTEMSWITH EMPHASIS ON THE RADAR EQUATION
Matei K. Kirov, Vencislav M. Vasilev, Vladislava S. Georgieva 315

MATHEMATICAL MODEL FOR ASSESSING THE EFFECTIVENESS OF INTEGRATED AIR AND MISSILE DEFENSE IN MULTI-DOMAIN OPERATIONS
Matei K. Kirov, Stanimir H. Parvanov.....325

SYSTEM BOUNDARY AND ANALYTICAL LEVEL IN LOSS ANALYSIS
Nikolay T. Iliev.....335

REALIZED AND SCENARIO-BASED LOSS: DIFFERENCES IN ANALYTICAL AND EVIDENTIARY STATUS
Nikolay T. Iliev.....340

WEAPONS, TECHNOLOGIES, LOGISTICS 346

MODIFICATION OF THE BURNING RATE OF A LIGHTING PYROTECHNIC COMPOSITION IN LIGHTING AIR BOMBS BY INTRODUCING AN INHIBITOR – STEARIC ACID
Ivelina Ivanova Angelska 347

ANALYTICAL MODEL FOR THE PREDICTIVE DETERMINATION OF SMALL-ARMS SHOT GROUPING IN SINGLE-SHOT FIRING
Conyu G. Conev 351

A MODEL FOR DETERMINING A CRITERION FUNCTION
Ivo Georgiev Radulov.....358

FUNCTIONAL CLASSIFICATION AND COMPARATIVE ANALYSIS OF METHODS FOR THE DEMILITARIZATION OF ARTILLERY ROUNDS AND THEIR COMPONENTS
Miroslav P. Dimitrov.....368

SURVEY OF THE CONDITION OF TECHNICAL OBJECTS
Andrei I. Bogdanov 380

ADAPTED ANALYSIS OF THE IMPACT OF CRISES IN THE BLACK SEA REGION ON THE NATIONAL SECURITY OF THE REPUBLIC OF BULGARIA
Anastas M. Chitakov 385

MILITARY-TECHNOLOGICAL ASYMMETRY IN THE ALGORITHMIC ERA: RECONCEPTUALIZATION OF STRUCTURAL NEOREALISM AND THE PHENOMENON OF "ALGORITHMIC VETO"
Dilyan Markov.....391

INSTITUTIONAL, LEGAL, AND SOFTWARE DIMENSIONS OF DEFENSE CONTROL: FROM HARDWARE GEOPOLITICS TO ALGORITHMIC SOVEREIGNTY
Dilyan Markov.....398

THE EFFECT OF VARIABLE FOCAL DISTANCE TO THE ASPEN SAMPLES SURFACE ON CO_2 LASER ENGRAVING PARAMETERS
Daivis Rāviņš, Imants Adijans, Dzintars Rāviņš,.....409

LASER SURFACE HARDENING OF MEDIUM-CARBON STEELS: PROCESS OPTIMIZATION, MICROSTRUCTURAL EVOLUTION, AND INDUSTRIAL APPLICATIONS
Normunds Teirumnieks 427

A MISO 2×1 SOFTWARE-DEFINED RADIO MODEM WITH ALAMOUTI TRANSMIT DIVERSITY: DESIGN AND EXPERIMENTAL EVALUATION
Ivan P. Ivanov.....455

RFNOC-BASED FMCW WAVEFORM GENERATION FOR USRP SDR Ivan P. Ivanov, Sevdalin Spassov 463

A SIMO 1×2 SOFTWARE-DEFINED RADIO MODEM WITH MAXIMUM-RATIO COMBINING: DESIGN AND EXPERIMENTAL EVALUATION
Ivan P. Ivanov.....471

INVESTIGATION OF THE TECHNOLOGICAL PROCESS IN TRANSFORMING PET WASTE INTO FDM FILAMENT
Martin G. Dimitrov.....479

METROLOGICAL SUPPORT FOR WEAPON SYSTEMS FOR DETERMINING THEIR TECHNICAL CONDITION
Vanko V. Ganev[1], Yana D. Dimitrova[2], Petya N. Stefanova[3] 485

APPLICATION OF THE SYSTEM OF TOLERANCES AND FITS IN INDUSTRY 4.0
Rosen N. Lazarov 491

COMPUTATIONAL ANALYSIS OF SINGLE-PIECE AND SEGMENTED FRANGIBLE CORE DESIGNS FOR PROJECTILE IMPACT ON STEEL ARMOUR
Mirel Nană[1], Constantin Enache[1], Florin-Marian Dîrloman[1], Adrian-Nicolae Rotariu[1], Octavian-Gabriel Chiriac[1] 500

EXPERIMENTAL STUDY ON THE BALLISTIC IMPACT PERFORMANCE OF MULTILAYER SIDE BODY ARMOR
Alexandru-G. Vintilă[1], Florina Bucur[2]*, Adrian-N. Rotariu[3], Savu-E. Dima[4], Andrada-M. Sandu[5]515

RESEARCH ON THE RELIABILITY AND SERVICE LIFE OF SPECIAL MECHANICAL SYSTEMS
Andrada-M. Sandu, Pamfil Șomoiag, Liviu-C. Matache, Alina Plesca, Alexandru-G. Vintilă ..524

THE SYSTEM OF SISTEMS CONCEPT IN MULTIDOMAIN ENVIRONMENT
Valentin S. Vasilev 532

A MULTI-CRITERIA MODEL FOR ASSESSING THE RESILIENCE OF COMMUNICATION SYSTEMS UNDER NUCLEAR, CHEMICAL AND BIOLOGICAL THREATS
Nikolay Iliyanov Padarev 539

AUTOMATED QUALITY CONTROL SYSTEMS FOR WATER HEATING APPLIANCES
Aleksandra P. Docheva[1], Daniel R. Denev[2] 546

A METHOD FOR OPTIMIZING COMBINED USE OF UNMANNED AERIAL SYSTEMS AND ARTILLERY FORMATIONS TO ENGAGE TARGETS IN CONTEMPORARY ARMED CONFLICTS
Ivelin G. Katsev 555

FIELD ARTILLERY SYSTEMS AND TECHNOLOGIES:ASSESSMENT OF CAPABILITIES AND TECHNOLOGICAL DEVELOPMENT
Ivan K. Vladov, Yavor Y. Valkov, Yuliadi P. Keranov 565

INTEGRATED DIGITAL-PHYSICAL APPROACH TO DEVELOPING DEFENSE AND DUAL-USE TECHNOLOGIES THROUGH SIMULATIONS, ADDITIVE MANUFACTURING AND ARTIFICIAL INTELLIGENCE
Stamen I. Antonov, Mariela L. Antonova 572

COMMUNICATION AND COMPUTER TECHNOLOGIES 580

APPLICATION OF THE MUSIC ALGORITHM FOR DIRECTION OF ARRIVAL ESTIMATION IN RADAR SYSTEMS
Georgi P. Iliev, Stanimir H. Parvanov, Nikolet G. Luledzhieva 581

COMPARATIVE ANALYSIS OF THE BASIC METHODS FOR 3D STEGANOGRAPHY
Georgy A. Kozarev 588

MODELING AND ANALYSIS OF A COMMUNICATION CHANNEL IN THE GNU RADIO SIMULATION ENVIRONMENT
Vladislava S. Georgieva 598

IMPACT OF ASSESSMENT INDICATORS ON CONTENT GENERATED BY LARGE LANGUAGE MODELS
Miroslav G. Nedelchev 611

A SINGLE APPROACH TO MANAGEMENT AND MONITORING OF MILITARY COMMUNICATION AND INFORMATION SYSTEMS
Miroslav G. Nedelchev 618

SECURITY AND RESILIENCE OF TRANSFORMER ARCHITECTURES AND LARGE LANGUAGE MODELS
Miroslav G. Nedelchev 625

CREATION OF A PARAMETRICALLY CONTROLLED SYNTHETIC IMAGE DATASET OF ISHIHARA-LIKE PLATES FOR COMPARING HUMAN AND COMPUTER VISION
Lyubomir E. Manov 631

RISKS TO PERSONAL INFORMATION AND ITS PROTECTION ON THE INTERNET
Borislava T. Nedkova[1], Daniel R. Denev[2] 640

PASSWORD SECURITY ASSESSMENT THROUGH ENTROPY ANALYSIS AND DIFFERENT GENERATION STRATEGIES
Gabriela S. Markova[1], Daniel R. Denev[2] 649

USING COMMUNICATION NETWORKS AND GRAPH MODELS TO PREDICT ACADEMIC ACHIEVEMENT IN GEOGRAPHY EDUCATION
Daniel R. Denev[1], Madlen A. Todorova[2] 658

CONCEPT DRIFT IN STREAMING INFORMATION DATA IN INTELLIGENT ENERGY SYSTEMS
Milen S. Davidkov 667

ASSESSMENT AND IMPROVEMENT OF STREAMING INFORMATION DATA QUALITY
Milen S. Davidkov[1], Tsvetoslav S. Tsankov[2] 677

HYBRID APPROACH TO NETWORK TRAFFIC ANOMALY DETECTION USING WIRESHARK, CISCO PACKET TRACER AND IDS
Dimitar R. Iliev[1], Ekaterina M. Hristova[2] 686

DECISION-MAKING MODEL FOR ADAPTIVE ACCESS CONTROL IN A UNIVERSITY INFORMATION SYSTEM
Radostin H. Lefterov 694

CONCEPTUAL MODEL AND MULTILAYER ARCHITECTURE FOR REAL-TIME STREAMING DATA QUALITY MANAGEMENT
Svetlana M. Davidkova[1], Milen S. Davidkov[2] 702

REAL TIME HIGH ORDER QUADRATURE AMPLITUDE MODULATION IMPLEMENTED VIA SOFTWARE-DEFINED RADIO: FUNDAMENTAL STRUCTURE, EMPIRICAL CHARACTERIZATION, AND MILITARY APPLICATION
Ivan I. Ivanov 709

SHUMENTECH AS A REGIONAL HUB FOR DUAL-USE TECHNOLOGIES AND DEFENSE INNOVATION IN BULGARIA'S NATIONAL SECURITY SYSTEM
Vladislav Milkov Genoff[1], Hristo Atanasov Hristov[2] 718

APPLICATION OF SATELLITE COMMUNICATION SYSTEMS IN AIR DEFENSE
Yoana A. Pashkuleva 729

CYBERSECURITY AND ARTIFICIAL INTELLIGENCE 736

CALIBRATED DIPLOMACY - A TIERED RESPONSE FRAMEWORK FOR CYBERSECURITY INCIDENTS UNDER ATTRIBUTION UNCERTAINTY
Marius Iulian Mihailescu[1], Stefania Loredana Nita[2], Valentina Marascu[1,3] Laurentiu Bogdan Asalomia[4] 737

IMPROVING BLUE TEAM THREAT HUNTING CAPABILITIES THROUGH CYBER DEFENSE EXERCISES
Radostin S. Dimov 746

THE ROLE OF TRUE ENTROPY IN POST-QUANTUM CYBERSECURITY
Zhaneta N. Savova*, Antoniya T. Tasheva** 754

RESPONSIBLE INTELLIGENT GEOSPATIAL SYSTEMS: GEO-PRIVACY, CYBERSECURITY AND AI IN DEFENSE APPLICATIONS
Ani A. Stefanova 760

ETHICAL CHALLENGES IN IMPLEMENTING AUTOMATION AND AI
Ekaterina M. Hristova[1], Aleks Ya. Danev[2] 768

CYBERSECURITY IN AUTOMATED INDUSTRIAL SYSTEMS
Petar G. Sotirov[1], Ilker A. Hatib[2] 777

HYBRID MODEL FOR RELIABILITY ASSESSMENT OF INTELLIGENT VIDEO SURVEILLANCE SYSTEMS USING FMEA AND MONTE CARLO SIMULATIONS
Silvia Hr. Nikolova 786

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON SOCIAL WORK
Stefaniya M. Chervenkova[1], Daniel R. Denev[2] 793

EXPLAINABLE ARTIFICIAL INTELLIGENCE IN MANUFACTURING SYSTEMS
Yuray Yu. Mehmedov[1], Ivaylo I. Petrov[2] 801

QUANTITATIVE ASSESSMENT OF RADIO-FREQUENCY COUNTERMEASURES AGAINST CONSUMER UNMANNED AERIAL VEHICLES
Deyan N. Dimitrov, Nikola P. Petrov 810

CYBERSECURITY ANALYSIS USING DEEP LEARNING NEURAL NETWORKS
Nikola R. Lazarov 820

MALICIOUS ACTIVITIES HUNTING IN NETWORK DEVICES
Linko G. Nikolov, Svetoslav Kirilov 829

MALICIOUS ACTIVITIES HUNTING IN WINDOWS SERVER
Linko G. Nikolov, Evlogi Grigorov 839

MALICIOUS ACTIVITIES HUNTING IN LINUX DEVICES
Linko G. Nikolov, Akan Hilmi 847

MODERN TECHNOLOGIES FOR SECURE STORAGE AND PROTECTION OF CRITICAL INFORMATION AGAINST CONTEMPORARY CYBER THREATS
Daniel Mitich, Elena Karadzhova, Nikoleta Pehlivanova 855

IMPACT OF HYPERPARAMETERS AND DATA SCALING METHODS ON THE PERFORMANCE OF DEEP NEURAL NETWORKS FOR NETWORK ATTACK DETECTION
Angela R. Borisova 860

ARTIFICIAL INTELLIGENCE-BASED FACIAL RECOGNITION SYSTEM FOR DIGITAL IMAGES
Emil T. Ivanov 875

SOCIAL STUDIES 890

THE LOOK AND THE SMILE AS A MEANS OF COMMUNICATION
Valya M. Simeonova 891

INFORMATION PROVISION OF MACROCONFLICT MANAGEMENT
Asen Zahariev 898

CULTURAL NATIONALISM AS A POLICY FOR THE PRESERVATION AND SUSTAINABLE DEVELOPMENT OF THE BULGARIAN IDENTITY AND STATESHIP
Petar Givkov, Stoyan G. Stoychev 911

ARCH SYNDROME AND CRITICAL THINKING IN A MILITARY ENVIRONMENT
Viktor T. Dobrev 921

VULNERABILITY ASSESSMENT IN THE VARNA REGION IN THE CONTEXT OF DISASTERS AND EMERGENCIES
Mariya Dimitrova 928

APPLICATION OF GRAPH THEORY IN THE ANALYSIS OF DEPOPULATED REGIONS
Milena H. Lambeva 936

GEODESY 945

THE IMPACT OF GRAVITY CORRECTIONS ON NORMAL HEIGHTS DETERMINED BY PRECISE GEOMETRIC LEVELLING
Marko Markov 946

GIS AS A TOOL FOR INTEGRATING, ANALYSING, AND VISUALISING SPATIAL DATA TO SUPPORT ROAD SAFETY DECISION-MAKING
Marko Markov....952

INTEGRATION OF MACHINE LEARNING IN CLASSICAL GRAVIMETRY AND GNSS STUDIES
Marko Markov....962

ANALYSIS OF METHODS FOR CREATING AN UNDERGROUND CADASTRE
Petina A. Andreeva, Hristiyan Georgiev....968

FLOODING RISK ASSESSMENT IN THE KAMCHIA RIVER BASIN AFTER APPLICATION OF MULTI-CRITERION ANALYSIS
Gergana Dimova....975

SURVEY AND RENOVATION OF THE GEODETIC NETWORK OF THE "V. LEVSKI" NATIONAL MILITARY UNIVERSITY – SHUMEN CAMPUS
Viktor Dragiev, Andrey Andreev....987

LINEAR MEASUREMENT WITH LIGHT RANGEMETERS ON A REFERENCE GEODESIC NETWORK
Maria Cendova, Andrey Andreev....998

ANALYSIS OF EXISTING SPECIAL GEODETIC NETWORKS IN BULGARIA
Georgi Tanev....1011

METHODS FOR ESTABLISHING SPECIAL GEODETIC NETWORK
Georgi Tanev....1018

METHODS FOR INVESTIGATING VERTICAL DEFORMATIONS Tsvetelina T. Mateeva,
Vladimir M. Petrov....1024

BASICS OF REMOTE SENSING AND SATELLITE SYSTEMS
Desislava A. Delkova, Momchil G. Georgiev, Veselin H. Gepov....1029

METHODS FOR MAPPING THE BOTTOM OF A WATER BASIN
Tanislav Tanev....1034

MODERN MEANS FOR HYDROGRAPHIC SURVEYS
Tanislav Tanev....1040

THE LIGHTHOUSES AND AIDS TO NAVIGATION SYSTEM ALONG THE BULGARIAN BLACK SEA COAST: HISTORY, CURRENT STATUS, CHALLENGES, AND FUTURE DEVELOPMENT
Aleksandra P. Zidarova, Aylin N. Dzhom....1047

PLENARY SESSION

ATTACK SURFACE OF OPEN SPATIAL DATA INFRASTRUCTURES: A SYSTEMATIC THREAT MODEL FOR OGC SERVICE STACKS

Stefania Loredana Nita[1], Alexia Ioana Dragomir[1], Marius Iulian Mihailescu[2], Valentina Marascu[3]

[1]Faculty of Information Systems and Cyber Security, Military Technical Academy "Ferdinand I", Bucharest, Romania, stefania.nita@mta.ro; alexia.dragomir@mta.ro
[2]Faculty of Engineering and Computer Science, Spiru Haret University, Bucharest, Romania, m.mihailescu.mi@spiruharet.ro
[3]National Institute for Laser, Plasma and Radiation Physics Magurele, Romania; Faculty of Mathematics and Computer Science, Bucharest University, Bucharest, Romania, v.marascu.mi@spiruharet.ro

***Abstract**: Public map services support planning, utilities, and emergency response, and have received little security attention. We model the attack surface of open spatial data infrastructures across four layers of trust, from data production through to the end user. Because much of this data is published openly, the main risk is silent alteration rather than theft. Three plausible searches of public scan data returned three different deployment counts for the same software. We give a procedure for separating real installations from artefacts.*

***Keywords:** Spatial data infrastructure, OGC web services, Data integrity*

1 Introduction

Public authorities publish geographic data as a matter of obligation. In Europe, Directive 2007/2/EC requires member states to expose discovery, view and download services over their spatial datasets [1]. Municipalities publish cadastral boundaries and zoning. Utility operators publish network extents, and emergency services publish road closures and hazard zones. The data is meant to be read by anyone, and decisions are taken from it: whether a site floods, which street a crew can reach, where it is safe to dig.

The software serving it is standardised and concentrated. A small number of implementations answer requests through interfaces defined by the Open Geospatial Consortium (OGC) and adopted as ISO standards. Interoperability follows from that concentration, and so does the reach of any single fault. Security work on these services has addressed which client may retrieve which layer, through access control, authentication and licensing. Section 3 sets out that work. It leaves the question this paper is about. Data published under an open mandate needs no protection from disclosure. It needs protection from alteration, and a client that receives a map has no way to establish that what it received is what the authority published.

We make two contributions. The first is a threat model for SDI deployments, decomposed into four zones by who controls what rather than by network position, with the threats at each boundary mapped to ATT&CK techniques. The second came out of trying to measure how many of these services are exposed. Four defensible queries against public scan data returned four populations for the same software, differing by a

factor of 3.4, and the largest consisted mostly of 8,240 hosts serving one byte-identical page across nine hosting operators. We give the procedure that separated the real deployments from the artefacts.

2 Reference architecture and trust zones

An SDI publishes geographic data held by one organisation for use by others. In Europe the obligation is set by Directive 2007/2/EC [1], which requires member states to expose discovery, view and download services over their spatial datasets. The components are standardised. A web map service [2] returns rendered images. A web feature service [3] returns geometry and attributes. A catalogue service answers questions about what a provider holds. We decompose a deployment into four zones, shown in Figure 1. The division follows control rather than network topology, because the security question at each boundary is what the receiving party can verify about data it did not produce. Data production covers surveying, cadastral registration, sensor feeds, and editing in desktop software, together with the database holding the authoritative copy. One organisation controls the zone and normally operates it on an internal network.

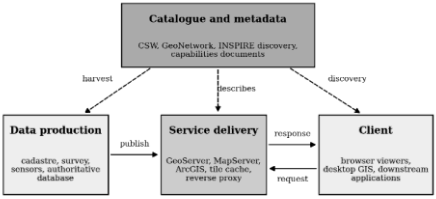


Figure 1: Reference architecture of an open spatial data infrastructure, divided into four trust zones.

Catalogue and metadata covers the services that describe holdings: which datasets exist, who maintains them, and where they can be retrieved. Discovery services and GeoNetwork deployments sit here, as do the capabilities documents each endpoint returns on request. The zone is federated, so catalogues harvest from one another and a record may travel several steps from the authority that wrote it, with the client that reads it having no view of that path. Service delivery faces the internet. GeoServer, MapServer and ArcGIS Server sit here, usually behind a reverse proxy. The 4,565 hosts characterised in section 4 belong to this zone, which is also the only zone passive scanning reaches. The client zone covers browser viewers, desktop GIS, and applications that consume responses without a person examining them, under the control of whoever runs the client rather than the provider.

Each boundary carries an assumption the receiving party cannot check. A client requesting a map image receives pixels, and nothing in the response establishes that they were rendered from the authoritative dataset. Delivery trusts production, since a service renders whatever the database contains and holds no independent statement of what it

should contain. Discovery trusts the catalogue, which authenticates neither the enquirer nor the origin of a harvested record.

Where confidentiality controls exist they are enforced at the delivery boundary, through access restrictions on individual layers. No boundary carries an equivalent control for integrity. A provider can decide who may read a layer. Neither the provider nor the client can establish, from the protocol alone, that what was read is what the provider published.

3 Threat taxonomy

Security work on OGC services has followed two tracks. OGC's own standardisation produced a sequence of engineering reports establishing a security baseline across service types [4], extending it across the suite of service standards [5], and annotating the capabilities document so that a service can advertise the controls it enforces [6], with the result consolidated as a common security standard [7]. The academic track proposed mechanisms: spatially aware authorisation rules through XACML and GeoXACML [8], the same combined with SAML for authentication [9], integration with federated identity through Shibboleth [10], and authorisation services for layer protection within an SDI [11].

The question addressed across both tracks is which client may retrieve which layer. The most recent of these appeared in 2019, and citation counts across the set do not exceed two. Our searches returned nothing later, and we make no claim about work those search terms did not reach. Access control answers a question about withholding. Three properties of spatial services fall outside it.

The first concerns what a client can check. Layers published under an open data mandate carry no confidentiality requirement, so an attacker gains nothing by reading them. Altering them is another matter. A WMS response is an image rendered on request [2], and the client holds no reference copy to compare it against. A WFS response is structured data [3] and is checkable in principle, but no field in it binds the geometry to a published dataset version. An altered flood boundary enters a planning decision looking exactly like an unaltered one. Detection rests on somebody recognising that a line is in the wrong place. Provenance recording has been proposed for geospatial work as a route to verifiable reuse [12], though the mechanisms described there serve replicability rather than live verification by a client. Layers that carry no restriction individually may combine into information that would not be released as a single dataset. Statistical disclosure control handles this for fixed publications through suppression or coarser aggregation [13], but a WFS operator has no equivalent, because the client chooses the extent, the attributes and the filter. How far aggregate data permits recovery of underlying records is disputed [14].

The second is discovery. A capabilities document returns layer names, bounding boxes, supported operations and often a version string, without authentication, because discovery cannot work otherwise [2], [3]. An operator who treats a layer as hidden because nothing links to it will find it enumerated there. Our own results qualify how much this matters. We identified 4,214 hosts through a servlet container's error page and 8,240 through a shared page hash, and neither route required a capabilities request.

Capabilities disclosure widens what an attacker learns about a service already located. It is not what locates the service.

We map threats to ATT&CK rather than to STRIDE. ATT&CK describes techniques observed in use and is organised for mapping onto concrete systems [15], and it has been applied across a wide range of security tasks [16]. STRIDE classifies by violated property, which fits poorly here because one OGC request can serve several categories at once, and mapping STRIDE categories onto concrete weaknesses is itself unsettled [17]. Table 1 gives the mapping. Data production is reached through credentials rather than through the protocol. An account with edit rights on the authoritative database alters source geometry, and every downstream service then renders the alteration faithfully. Nothing in the delivery path detects it, because the service is behaving correctly.

Table 1. Threats by trust zone with corresponding ATT&CK techniques.

Zone	**Threat**	**ATT&CK**
Data production	credentialed alteration of source geometry	T1078 Valid Accounts; T1565.001 Stored Data Manipulation
Catalogue and metadata	unauthenticated enumeration of holdings	T1596 Search Open Technical Databases
Catalogue and metadata	harvested record altered in the federation path	T1199 Trusted Relationship
Catalogue and metadata	metadata mined for targeting	T1213 Data from Information Repositories
Service delivery	exploitation of the service itself	T1190 Exploit Public-Facing Application
Service delivery	persistence through an exposed admin interface	T1505.003 Web Shell
Service delivery	modification of published features via WFS-T	T1565.001 Stored Data Manipulation
Client	response altered in transit	T1565.002 Transmitted Data Manipulation

The catalogue zone inherits its weakness from federation. A record harvested across several catalogues arrives carrying no evidence of who wrote it, so a client that trusts a record trusts the whole harvesting chain. Metadata retrieval is also the cheapest reconnaissance available against an SDI, and it is answered without authentication by design.

The transactional surface at the delivery zone is the one usually treated as dangerous. A WFS-T endpoint accepting unauthenticated Insert, Update or Delete operations permits direct modification of published features, and an exposed administrative interface permits reconfiguration of layers, data stores and security rules. Both warrant the attention they receive. Parameter handling deserves more. CVE-2024-36401 allowed unauthenticated remote code execution against default GeoServer installations before versions 2.23.6, 2.24.4 and 2.25.2, through property names evaluated as XPath expressions [18]. It was reachable through GetMap, GetFeatureInfo, GetLegendGraphic, GetFeature and GetPropertyValue, all of them read operations. A deployment serving nothing but map images, with no transactional endpoint configured and no administrative interface

exposed, was open to code execution as the account running the service. The fault sat in parameter parsing that every OGC request passes through, so the exposure followed from implementing the standard rather than from operating it carelessly.

That case bears on how the taxonomy should be read. Threats against the transactional surface can be removed by removing the surface. Threats against parameter handling cannot, because the request path is the service.

4 Establishing a deployment population

The threat model assumes a population of reachable services. Counting that population proved harder than the modelling. We queried Shodan for internet-facing GeoServer instances and obtained four totals, each from a query that is defensible on its own terms. Table 2 lists them. The largest exceeds the smallest by a factor of 3.4.

Table 2. Candidate queries for internet-facing GeoServer, with totals and assessment.

Query	Hosts	Assessment
http.html:"GeoServer"	15,752	Matches pages referencing the software; 59% is nginx
http.title:"GeoServer"	10,536	78% is a single replicated page
http.html_hash:-1011724024	8,240	One artefact, nine operators
http.html:"GeoServer" product:Jetty	4,565	Decomposes without residue

The broadest query matches any page whose HTML contains the string GeoServer. Of the hosts it returns, 9,294 run nginx and 4,583 run Jetty, and 8,662 carry jQuery. GeoServer ships standalone on Jetty and deploys as a WAR under Tomcat. A result set in which the application server is absent from most hosts is measuring something other than the application. Restricting the match to the page title removes part of that and introduces a larger problem. Of the 10,536 hosts returned, 8,240 share one HTML hash, -1011724024. All of them serve nginx, all carry jQuery, and all present the title "GeoServer: Welcome". They sit with nine hosting operators in ten countries across ten autonomous systems, no operator holding more than 20.0%, as shown in Table 3. Green Floid appears twice in the organisation facet under two autonomous systems, which is why nine operators occupy ten entries.

Table 3. Distribution of the 8,240-host cluster sharing HTML hash -1011724024. Countries: FR

Operator	Hosts	Share	AS
OVH SAS	1,652	20.0%	AS16276
Alta Gracia Project Holding Ltd	1,519	18.4%	AS6400
EDIS Infrastructure in Czechia	962	11.7%	AS174
EDIS Infrastructure in North Macedonia	836	10.1%	AS25467
nic.at GmbH	712	8.6%	AS30971
Edge connect (pty) Ltd	695	8.4%	AS32437
G-Core Labs	618	7.5%	AS202422
EstNOC OY	461	5.6%	AS36352
Green Floid LLC	339	4.1%	AS21100
Green Floid LLC	228	2.8%	AS204957

1,652; DO 1,519; CZ 962; SG 846; MK 836; AT 712; ZA 695; US 464; NL 344; CA 201.

Port allocation separates the cluster from operational service. Its most common port carries seven hosts, 0.085% of the total, and its ten most common ports account for 59 hosts between them. The 8,240 hosts therefore occupy at least 1,178 distinct ports. In the validated population described below, 1,146 hosts, 25.1%, sit on port 8080 alone. Figure 2 gives the contrast.

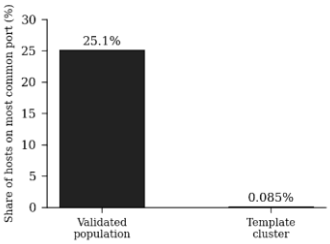


Figure 2: Share of hosts on the most common port, validated population against template cluster.

The cluster does not behave like deployed infrastructure. Byte-identical pages replicated across nine unrelated providers, on arbitrary high ports, without the servlet container the page advertises, are not independently operated spatial data infrastructure. Honeypot deployment is one candidate explanation, GeoServer having become an attractive lure since CVE-2024-36401. Proxy infrastructure using a decoy landing page is another. Aggregate counts cannot separate the two, and we make no claim between them.

The validated population rests on a mechanism that can be checked. Jetty's default not-found page enumerates the web application contexts deployed on the server. Querying for that page text together with a geoserver context returns 4,214 hosts. A further 351 serve a live root, of which 99 present a WFS interface and 37 a redirect. Those two figures sum to 4,565, the total for GeoServer HTML restricted to Jetty, and the decomposition leaves no residue. Figure 3 shows the composition.

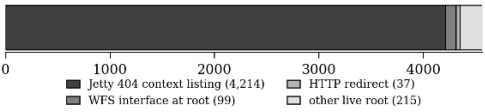


Figure 3. Composition of the 4,565-host validated population

Tomcat contributes little to the undercount. GeoServer HTML on Apache Tomcat returns 33 hosts, with 11 on the Coyote variant and 12 by component detection. Restricting to Jetty therefore discards tens of hosts rather than thousands. One discriminator failed in a way worth recording, because it looked sound. Favicon hash -629047854 covers 4,190 of the Jetty-hosted population, 92%, and 3% of the template cluster. The hash appears on 14,724 hosts, of which 10,382 contain no reference to

GeoServer, and the titles in that set include unrelated software. It does not identify Jetty either: 307,334 Jetty hosts carry no GeoServer reference, and 2.3% of them carry the hash. A coverage figure of 92% within a candidate population says nothing on its own about the false positive rate outside it. The procedure detects contamination and does not produce a census. Shodan crawls root paths and common ports, so services published behind application paths do not appear. Deployments behind reverse proxies that strip application identifiers are also missed, and the WMS and WFS capabilities documents that would identify them returned counts in the single figures. The 4,565 figure is a floor.

Counts drifted between runs on two consecutive days in September 2026. The broad query returned 15,752 and 15,748, the title query 10,540 and 10,536, and the Jetty-restricted query 4,587, 4,562 and 4,565. Drift of that size follows from index updates between queries and does not affect the separation between the four totals.All figures were obtained through the Shodan count endpoint with facet aggregation, which returns totals and top-value distributions without retrieving host records. No requests were sent to any surveyed host, no host identifiers were collected, and no authentication was attempted. Collection ran on two consecutive days in September 2026.

5 Mitigations and open problems

Section 2 identified the delivery boundary as the one carrying an integrity assumption with nothing behind it. The measures below address parts of that. One measure in common use turns out to be unsupported by our own results, and the residue is stated rather than resolved.

Separating transactional from read-only operations at the network boundary has the clearest scope. A WFS-T endpoint and an administrative interface reachable only from the producing network cannot be reached from the internet whatever their configuration says, which removes the dependence on a setting that an operator may change and forget. Figure 4 shows the arrangement: editing acts on the authoritative database, publication is one-way onto a replica, and the public endpoint serves reads from the replica.

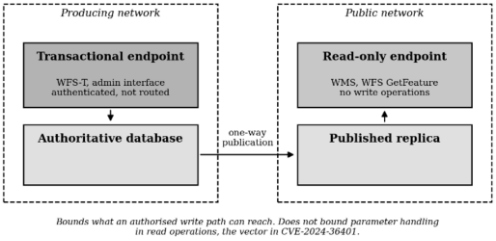


Figure 4. Separation of transactional and read-only endpoints across a network boundary.

CVE-2024-36401 bounds what this buys [18]. That vulnerability was reachable through GetMap, GetFeatureInfo, GetLegendGraphic, GetFeature and GetPropertyValue, and it affected default installations of every version before 2.23.6, 2.24.4 and 2.25.2. All of those are read operations. A deployment with no transactional endpoint at all was

exposed to unauthenticated code execution. Endpoint separation limits what an authorised write path can reach. It does not limit what parameter handling in a read path can reach, and the read path cannot be removed without removing the service.

Signing capabilities documents is deployable now. A capabilities document is generated from configuration, changes rarely, and is returned whole on request, so a detached signature over it costs a provider almost nothing. It gives a client a way to establish that the advertised layers, endpoints and supported operations came from the provider, which no part of the current protocol supports. The same construction extends to WFS responses, where features are returned as structured data and can be signed at publication. Figure 5 shows the workflow.

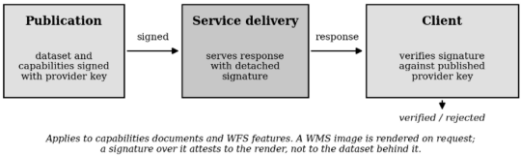


Figure 5. Signature at publication and verification at the client

Harvested catalogue records carry no evidence of origin. Signing a record at the point of authorship, and preserving that signature through harvesting, would let a client distinguish a record written by the responsible authority from one altered somewhere along the federation path. Suppressing version banners is often recommended and our results do not support it. We identified 4,214 hosts through Jetty's enumeration of deployed contexts and a further 8,240 through a shared page hash. Neither route read a version string. An operator who removes version disclosure and changes nothing else remains as identifiable as before. What remains open is the WMS case. A web map service returns an image rendered on request from parameters the client chose, so a signature over the response attests to the rendering and not to the dataset it was drawn from. Binding a rendered tile to the dataset version it came from, in a way a client can check without holding the source data, is unsolved. Until it is, integrity guarantees for published maps stop at the boundary of the services that return structured data.

Conclusion

The protocols that make spatial data infrastructure interoperable give a client no way to establish that a response came from the dataset the authority published. That gap sits in the standards rather than in any operator's configuration, and no amount of access control closes it. The measurement carries a separate caution. Deployment counts drawn from public scan data are query artefacts until something independent of the query confirms them. For GeoServer the difference between defensible queries was a factor of 3.4, and the largest figure consisted mostly of one page copied 8,240 times. There is no reason to expect other server software to behave better.

References

1. Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE). [Online]. Available: https://eur-lex.europa.eu/eli/dir/2007/2/oj/eng [Accessed: Sep. 3, 2026]
2. ISO 19128:2005 - Geographic information — Web map server interface. [Online] Available: https://www.iso.org/obp/ui/#iso:std:iso:19128:ed-1:v1:en [Accessed: Sep. 3, 2026]
3. ISO 19142:2010, Geographic information — Web Feature Service. [Online] Available: https://www.iso.org/standard/42136.html [Accessed: Sep. 3, 2026]
4. OWS-6 Security Engineering Report, Open Geospatial Consortium Inc. [Online] Available: https://docs.ogc.org/per/09-035/09-035.pdf [Accessed: Sep. 3, 2026]
5. Testbed-11 Engineering Report: Implementing Common Security Across the OGC Suite of Service Standards, Open Geospatial Consortium Inc. [Online] Available: https://docs.ogc.org/per/15-022/15-022.pdf [Accessed: Sep. 3, 2026]
6. Testbed-12 OWS Common Security Extension ER, Open Geospatial Consortium Inc. [Online] Available: https://docs.ogc.org/per/16-048r1.html [Accessed: Sep. 3, 2026]
7. Matheus, A. (2019). OGC Web Services Security.
8. Herrmann, J. (2011, November). Access control in ogc web service based architectures. In Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS (pp. 60-67).
9. Lin, J., Tao, H., & Zhu, G. (2009, December). An access control mechanism for geospatial information services. In 2009 First International Conference on Information Science and Engineering (pp. 1971-1974). IEEE.
10. Matheus, A., & Higgins, C. (2009). A Shibboleth Service Provider for OGC Web Map Services.
11. Kubik, T. (2009). Design Security and Geo-Rights Management Services In Spatial Data Infrastructure.
12. Tullis, J. A., & Kar, B. (2021). Where is the provenance? Ethical replicability and reproducibility in GIScience and its critical applications. Annals of the American Association of Geographers, 111(5), 1318-1328.
13. Olav Skøien, J., Lampach, N., Ramos, H., Seljak, R., Koeble, R., See, L., & Van der Velde, M. (2025). A flexible approach for statistical disclosure control in geospatial data: JO Skøien et al. Journal of Geographical Systems, 27(3), 341-367.
14. Muralidhar, K., & Domingo-Ferrer, J. (2023). Database reconstruction is not so easy and is different from reidentification. Journal of Official Statistics, 39(3), 381-398.
15. Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). Mitre att&ck: Design and philosophy (pp. 30-73). Technical report.

16. Al-Sada, B., Sadighian, A., & Oligeri, G. (2024). MITRE ATT&CK: State of the art and way forward. ACM Computing Surveys, 57(1), 1-37.
17. Honkaranta, A., Leppänen, T., & Costin, A. (2021, May). Towards practical cybersecurity mapping of stride and cwe—a multi-perspective approach. In 2021 29th Conference of Open Innovations Association (FRUCT) (pp. 150-159). IEEE.
18. CVE-2024-36401, National Vulnerability Database, NIST. [Online] Available: https://nvd.nist.gov/vuln/detail/cve-2024-36401 [Accessed: Sep. 3, 2026]

EMERGING AND DISRUPTIVE TECHNOLOGIES IN ARMAMENT SYSTEMS: TECHNICAL, EDUCATIONAL AND REGULATORY PERSPECTIVES

Marius Valeriu Cîrmaci Matei

Military Technical Academy "Ferdinand I", 39-49 Av. George Coșbuc, Bucharest, Romania
marius.cirmaci@mta.ro

Abstract. *Emerging technologies in armament engineering are frequently described as disruptive before their operational significance is demonstrated. This paper proposes a qualitative, case-based assessment framework linking technological maturity, engineering performance, military adoption, specialist education and regulatory response. Selected examples from the research portfolio of the Military Technical Academy "Ferdinand I" include ballistic modelling, energetic materials, munition geometry, terminal effects and standardisation. A historical comparison involving nineteenth-century small-arms ammunition illustrates how regulatory assessment can lag behind technical innovation. The paper argues that disruption is a system-level outcome rather than an inherent attribute of technology.*

Keywords: *emerging technologies; disruptive innovation; armament systems; ballistics; military education; regulation; standardisation.*

1. Introduction

Armament engineering develops through the interaction of scientific discovery, manufacturing capability, operational requirements and institutional constraints. Technological development is often portrayed as a progression from an emerging technology to a disruptive capability. However, emergence and disruption describe different dimensions of change: emergence concerns novelty and uncertainty, whereas disruption concerns the transformation of established practices or structures. Not every emerging technology becomes disruptive, and substantial technological change need not rely on an entirely new scientific principle.

This distinction is important for defence research management. Advances in artificial intelligence, autonomous systems, directed energy, energetic materials and additive manufacturing may indicate promising research opportunities without demonstrating operational transformation. Conversely, comparatively modest changes in ammunition design or testing methods may have substantial consequences when adopted across military organisations. Drawing on selected research examples presented by the Military Technical Academy "Ferdinand I" [2], this paper proposes an interpretative framework for assessing technical developments and their relationships with specialist education, interoperability and regulation.

For the purposes of this paper, an emerging technology is a technical approach at an early or rapidly evolving stage of development or application, characterised by uncertainty regarding its performance, adoption or potential impact. The term disruptive is used here in a broader operational and institutional sense to describe an adopted

technology that substantially changes military capability, doctrine, supply chains, standards or established practices. This working definition extends beyond Christensen's market-oriented account of disruptive innovation [1] and should be distinguished from it.

The proposed framework addresses four questions: (i) what is technically novel; (ii) which performance claims are supported by evidence; (iii) whether the technology has been integrated into operational use; and (iv) what organisational or regulatory effects have been demonstrated. Distinguishing these dimensions helps prevent planned projects, laboratory demonstrations and deployed systems from being treated as equivalent forms of evidence.

2. Language, terminology and technical knowledge

Defence technology is communicated across engineering, procurement, operations, translation and law. Terminological inconsistency can therefore become a practical obstacle to interoperability. General-language search systems and artificial-intelligence tools do not necessarily recognise the specialised sense intended by an engineer. For example, "receiver" may denote an electronic device or a structural weapon component; an appropriate Romanian rendering in the latter context is "*cutia mecanismelor*" (Fig. 1). Similarly, acronym interpretation cannot be separated from domain context: "UAV" commonly denotes unmanned aerial vehicle, while autonomous underwater vehicles are conventionally described by "AUV". These examples in the source presentation demonstrate the need for contextual validation rather than unrestricted automatic term substitution [2].



Fig. 1. Context-dependent meanings of "receiver": electronic equipment and firearm components.

These issues extend beyond translation accuracy. The interpretation of a requirement, test report or safety assessment may depend on how a component is defined in terms of its function, configuration or intended use. Terms such as "upper receiver" and "lower receiver" illustrate how a single general term can encompass distinct components within a particular firearm architecture. Precise definitions become especially important when technical terminology is incorporated into contractual specifications, standards or legislation. A practical terminology-validation process should document the underlying concept, the preferred term, accepted synonyms, the relevant technical context and the

supporting source, followed by expert review. AI-assisted retrieval can help identify candidate terms and references, but its outputs require verification before incorporation into authoritative documentation. This is particularly important in multilingual European projects, where inconsistent terminology can propagate across research deliverables, safety documentation and procurement requirements.

3. Technological innovation in armament systems: research directions, educational enablers and regulatory considerations

The European Defence Agency (EDA) CapTech Missiles and Munitions portfolio provides an organisational framework for examining developments relevant to armament engineering. The areas identified in the source presentation include energetic materials, lethality and platform protection, propulsion, ballistics and weapon design, sensors, and weapon systems [2, 3]. These areas are closely interconnected. For example, a new propellant concept can affect interior ballistics, barrel stresses, storage safety, qualification testing and operational logistics. Several research priorities illustrate different pathways to innovation. Precision guidance can alter the relationship between accuracy and ammunition expenditure. Additive manufacturing may enable new component geometries and changes in production processes. Improved lifecycle monitoring may provide substantial safety and logistical benefits without changing a munition's fundamental function. Concepts such as railguns and directed-energy weapons, however, require careful assessment of power requirements, thermal management, reliability and system integration before claims of disruptive impact can be substantiated.

Innovation also encompasses standardisation. For non-lethal kinetic-energy projectiles, a common framework for testing and capability assessment can improve the comparability of results and support interoperability. Its principal contribution may therefore lie in harmonising evaluation practices rather than replacing established technologies. The activities relating to NATO Standardisation Agreements (STANAGs) and Standardisation Recommendations (STANRECs) discussed in the presentation illustrate this incremental but strategically valuable contribution [2].

3.1. Numerical modelling and terminal ballistics

Within this research framework, numerical simulation supports several related areas of investigation, including weapon mechanism dynamics, interactions between firing pins and slides, flechette impact and three-dimensional modelling of terminal effects. The methods presented include finite element analysis and smoothed particle hydrodynamics, with selected analyses performed using AUTODYN [2]. Figure 2 illustrates the projectile geometry and target discretisation used to model projectile impact on ballistic gelatin. These approaches support the investigation of nonlinear contact, large deformation and fragmentation, provided that the constitutive models, boundary conditions, discretisation methods and validation procedures are adequately defined.

Ballistic gelatin illustrates the sensitivity of numerical predictions to material characterisation. The source presentation describes its rate-dependent mechanical behaviour, reporting an indicative increase in compressive resistance from the kilopascal

range under quasi-static loading to the megapascal range at high deformation rates [2]. These reported values should be interpreted within their respective test conditions rather than treated as universal material constants. Their application in predictive simulations requires careful consideration of gelatin preparation, temperature, strain rate, calibration procedures and the selected constitutive model.

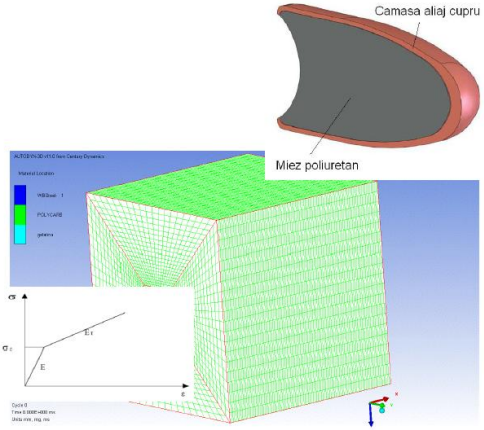


Figure 2. Finite element model of projectile impact on ballistic gelatin, showing projectile construction and target discretisation

3.2. Energetic materials and international research cooperation

Complementing the modelling activities described above, Military Technical Academy “Ferdinand I” (MTA) participates in multinational research cooperation on energetic materials, including EMPOF-related activities [2]. Such collaboration provides opportunities to harmonise testing methods, combine complementary expertise and exchange research findings. Its technical contribution should be assessed through documented procedures, reproducible results and verified deliverables, distinguishing institutional participation from demonstrated technological readiness.

Within this broader research landscape, RECBALL addresses inverse problems in interior ballistics, the development of burning-surface models and the potential use of additive manufacturing to produce novel propellant grain geometries [2]. The work explores the relationship between grain geometry, combustion behaviour and pressure evolution, while accounting for material properties and manufacturing constraints.

As further modelling and validation remain planned activities, these concepts represent ongoing research rather than established technical solutions. Their feasibility must be evaluated through material characterisation, reproducible manufacturing and appropriate qualification procedures. Together, these examples illustrate the complementary roles of numerical analysis, experimental validation and international cooperation in advancing armament research. Figure 3 summarises three representative research directions discussed in this section

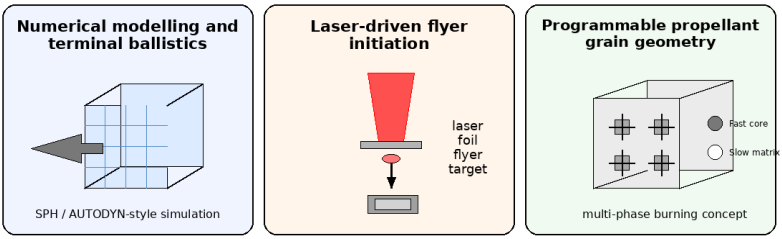


Figure 3. Representative research directions discussed in the paper: numerical modelling, laser-driven flyer initiation and programmable propellant grain geometry.

3.3. Education as an enabler of technological innovation

The research directions outlined above depend on engineers capable of connecting theoretical knowledge, numerical methods, experimental evidence and safety requirements. In specialised armament fields, fragmented educational provision can limit the development of expertise spanning mechanics, thermodynamics, ballistics, materials science, system safety and regulatory interpretation. The source presentation highlights educational cooperation in the ammunition sector, including interest from the European Commission's Directorate-General for Defence Industry and Space in existing ballistics programmes, industrial needs and opportunities for collaboration [2]. MTA's examples include four-year engineering programmes comprising 240 ECTS credits in armament and fire-control systems, aviation armament and rescue systems, energetic materials and CBRN defence, and munitions, rockets, explosives and propellants [2].



Figure 4. Educational cooperation in the ammunition sector: ballistics programmes, industrial needs and European collaboration [2].

An integrated teaching approach combines theoretical problem formulation, numerical modelling, supervised experimental verification, uncertainty and safety assessment, and the communication of findings through consistent technical terminology.

This approach also develops students’ ability to distinguish validated findings from preliminary simulations, early prototypes and prospective applications.

The presentation explicitly includes education among the technology building blocks associated with the EDA framework [2]. Skilled personnel support both the adoption of innovation and the reliability of testing and qualification processes. International educational cooperation can further promote consistent terminology, learning outcomes and engineering practices. Its effectiveness should nevertheless be assessed through demonstrated learning gains and the application of acquired competences, alongside mobility and participation indicators.

3.4. Technological change and regulatory assessment

Alongside research and education, regulatory assessment forms an essential part of technological development. The source presentation uses nineteenth-century ammunition developments to illustrate how technical change and humanitarian regulation can evolve at different rates [2]. The Minié projectile provides a historical example of changes in small-arms performance, while subsequent jacketed and pointed projectiles further altered ballistic behaviour. The 1868 St Petersburg Declaration and the 1899 Hague Declaration concerning expanding bullets provide distinct examples of legal responses to particular ammunition characteristics [4, 5]. Their provisions should be considered separately, without assuming that either instrument constitutes a general prohibition on all projectiles producing severe terminal effects. The historical comparison therefore highlights the importance of relating technical evidence to the precise scope of the relevant legal instrument. Engineering findings and legal conclusions address different questions. Assessment requires an understanding of both the technical evidence and the applicable legal framework, with a clear distinction between measured physical effects and normative judgements (Figure 5).

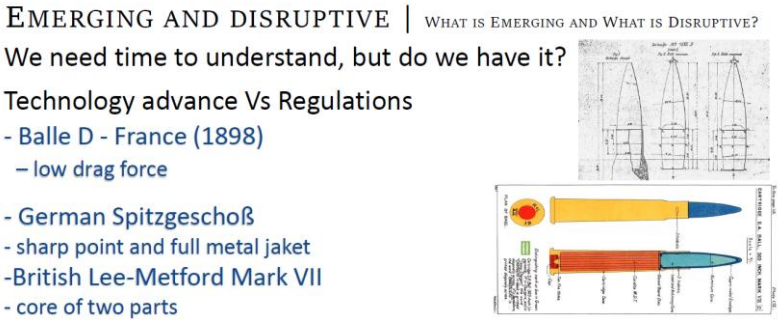


Figure 5. Historical examples of small-arms projectile design relevant to the discussion of technological change and regulatory assessment [2].

The same interdisciplinary approach is relevant to contemporary technologies, including autonomous systems, novel energetic materials and unconventional weapon concepts. Engineers contribute evidence on intended operating conditions, foreseeable failure modes and testing limitations, while legal and policy specialists assess the applicable rules and review requirements. Together, these contributions support a more rigorous evaluation of technological innovation and its potential consequences.

4. Conclusions

The examples discussed in this paper highlight the need to distinguish technical maturity from disruptive impact. An emerging technology may demonstrate novelty without delivering a reliable operational capability, while a mature incremental improvement may substantially influence logistics, training or interoperability. Equally, a successful technical demonstration may have limited practical impact if cost, infrastructure, reliability or regulatory constraints prevent wider adoption. To support this distinction, the paper proposes four descriptive categories: (A) exploratory concepts with limited verification; (B) technically demonstrated solutions whose operational and institutional implications remain uncertain; (C) mature incremental improvements that strengthen existing capabilities; and (D) adopted technologies with demonstrated effects that substantially transform operational or institutional practice. These categories complement, rather than replace, formal technology readiness assessments. They are intended to structure the evaluation of evidence and should not be interpreted as a mandatory sequence of development. Figure 6 summarises the proposed relationship between maturity and impact.

Within the MTA examples, numerical ballistic modelling, laser-driven flyer studies and novel propellant grain geometries illustrate ongoing research whose maturity must be assessed against the available validation evidence [2]. Standardisation activities support comparability and interoperability, while education and lifecycle management provide the expertise and institutional capacity needed to adopt and sustain innovation. Their contributions are significant even when they do not produce disruptive change.

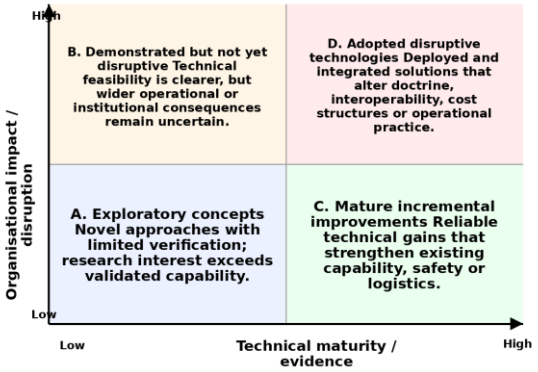


Figure 6. Proposed maturity–impact matrix for the assessment of emerging and disruptive armament technologies.

Three requirements underpin credible assessment: precise terminology and clearly defined test conditions; explicit differentiation between experimental findings, simulation results and planned activities; and consideration of regulatory and ethical questions throughout development. The historical examples further illustrate the importance of examining technical change alongside the scope and evolution of relevant legal instruments.

The central conclusion is that disruption is an outcome to be demonstrated through evidence of adoption and substantial operational or institutional change. Combining engineering validation, specialist education, standardisation and legal assessment provides a coherent basis for evaluating emerging armament technologies while recognising both their potential and the limitations of current evidence.

References

19. Christensen, C. M. (1997). The Innovator’s Dilemma: When New Technologies Cause Great Firms to Fail. Harvard Business School Press.
20. Cîrmaci Matei, M. V. (2026). Emerging and Disruptive Technologies for Armament Systems: MTA in the EU Context of Academic & Research Development. Conference presentation, Military Technical Academy “Ferdinand I”, Shumen.
21. European Defence Agency. (n.d.). CapTech Missiles and Munitions: Research and technology areas. European Defence Agency.
22. Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight. St Petersburg, 29 November/11 December 1868.
23. Declaration (IV, 3) concerning Expanding Bullets. The Hague, 29 July 1899.

THE GROWING IMPORTANCE ON AN ARTIFICIAL INTELLIGENCE IN MILITARY AND PUBLIC SERVICES ACTIVITY – CASE STUDY

Bartosz K. Biernacik

Cyber Domain Operations Department, Multi-Domain Operations Institute, Military Faculty, War Studies University, Warsaw, Poland, b.biernacik@akademia.mil.pl

***Abstract**: The article discusses the continued use of AI in the military environment, expanding the scope of its use in Military Decision Making Processes (MDMP) discussed last year, including attempts to control combat platforms. Several examples of unsuccessful attempts to use AI to control combat platforms were cited, the results of which should significantly increase scientists' efforts to establish rules for its safe use for such purposes. It is also a practical example of new areas of its use in public services to support crisis management, which is becoming increasingly necessary in times of increasingly frequent crisis situations in Europe, such as floods, fires, destabilizing hybrid activities conducted by, for example, the Russian Federation. The author provides examples of AI use in a system dedicated to crisis management in Poland and indicates directions for further research in this area.*

***Keywords:** Artificial Intelligence, Public Services, ICT, Combat Platform, Training System, NATO, Crisis Management, OECD, Cognition Loop, NATO ACT, Maven Smart System, HMS C3IS JASMINE, CMS JASMINE, EO/IR systems, UAV.*

Introduction

As AI advances, researchers debate whether AI should be created at all, as creating a self-aware entity superior to us humans, self-evolving, and difficult to control could render humanity redundant or even detrimental to the Earth's existence. Problems related to AI research most often lead to the conclusion that the development process should be accompanied by enormous concern for the security of the solutions being developed, as negligence in this area may be impossible to remedy after the creation of a truly self-aware AI, which could very quickly escape human control and not necessarily cooperate with us.

A conceptual view of an AI system was defined by OECD expert group. To the main components of the scheme they define three main elements of AI system[1]:

- sensors (which collect raw data from the environment);
- operational logic (algorithm models), which is the key power of the artificial intelligence system and, for a given set of goals and based on sensor input, provides extractions (outputs) for actuators – in the form of recommendations, predictions, or decisions that can affect the state of the environment;
- actuators (execution apparatus), which take actions to change the state of the environment.

[1] Scoping the OECD AI principles. Deliberations of the expert group on artificial intelligence at the OECD (AIGO), OECD digital economy Papers, November 2019 No. 291, p. 6.

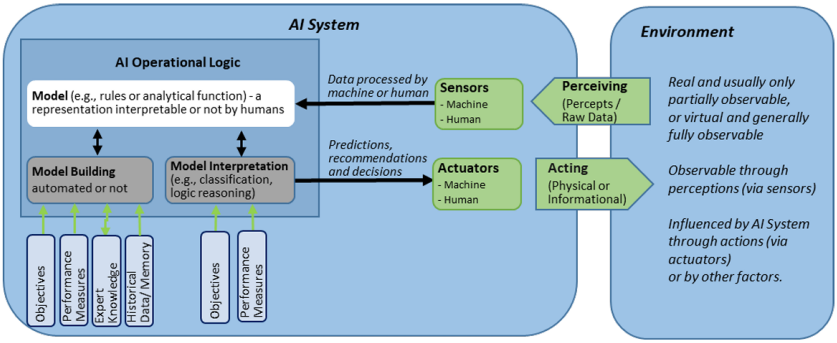


Figure 1: Detailed conceptual view of an AI System by OECD

Source: Scoping the OECD AI principles. Deliberations of the expert group on artificial intelligence at the OECD (AIGO), OECD digital economy Papers, November 2019 No. 291, p. 6.

At the current stage of advancement, we are not yet facing an existential dilemma, because the AI models being created are not conscious tools, but it is worth quoting the opinion of the Council of the European Union, according to which the advantages of AI include[2]:

– improved process efficiency – processes become smarter and more efficient, boosting productivity and profits. AI automatises tasks, identifies patterns, optimises workflows and makes real-time adjustments;
– greater creativity – AI can automatise tedious or repetitive tasks, such as production line work, data gathering, emailing, billing or customer service. This way people can spend more time on more creative or more human-centric tasks;
– lower risk of error – AI can enter data, do calculations or perform manoeuvres more quickly and more efficiently than humans. In critical sectors, such as healthcare or aviation, AI plays a vital role in assisting with high-risk surgery or predicting technical failures;
– performance of dangerous tasks – artificial intelligence can assist with tasks that endanger human safety or health, such as rescue operations, bomb disposal, managing contagious or radioactive substances or inspecting hostile environments;
– resolution of global challenges - AI can tackle complex global challenges such as improving healthcare, addressing climate change and ensuring food security, by for instance enhancing disease prediction, reducing energy use and optimising crop yields.

To summarize the benefits of AI solutions, we can propose the following selected set:

1. Excellence in tasks requiring attention to detail.
2. Efficiency in data-intensive tasks.
3. Time savings and increased productivity.

[2] https://www.consilium.europa.eu/en/policies/benefits-and-risks-of-ai/#benefits [Access: 09.2026]

4. Consistency of results.
5. Customization and personalization.
6. 24/7 availability.
7. Scalability.
8. Accelerated research and development.
9. Process optimization.

To the potential risk of AI Council of the European Union defines[3]:

– opacity – AI systems often lack transparency, and it is hard to know how they make decisions. The law requires that users be informed whenever they interact with AI, and that they have access to information on how AI works and what the associated risks are;
– lack of accountability – without clear guidelines and rules, AI can be used irresponsibly with no consequences;
– risks to safety – AI systems, especially in critical sectors such as transport or infrastructure, can pose major health and safety risks if they make errors or are wrongly designed. The law sets out strict requirements, such as risk assessments, human oversight, technical compliance or periodic reviews;
– bias and discrimination – AI can unintentionally perpetuate biases and discrimination when trained on biased data. The AI act establishes measures to prevent and mitigate biases in order to promote fairness and equality;
– violation of fundamental rights – some AI applications may violate individuals' fundamental rights, such as privacy, freedom of expression and non-discrimination. The law bans systems that threaten these rights, such as those used by governments for mass surveillance or social scoring.

A biases may occur in each of the part of the model[4]:

– Sensors, notably via Perception bias, whereby the data collected over-represents (or under-represents) one population. Perception bias makes the AI system operate better (or worse) for that population at the expense of others;
– Operational logic, notably via Technical bias that arises from constraints or considerations within the technology itself, whether they are known or not. This can include the tools and algorithms an AI system uses. For example, a selected algorithm may work better or worse with a different sets of variables/features. If used in an AI system with different variables or features, its accuracy will be lower, which may introduce bias that is very hard to detect[5];

[3] Ibidem.
[4] Ibidem.
[5] An accident in 2016 involving a Tesla Model S and a tractor trailer provides an example of technical bias, where the Autopilot's computer vision-based vehicle detection system did not notice the white side of the tractor trailer against a brightly lit sky and did not brake.

– Expert Knowledge, notably via Modelling bias, whereby a human manually designing a model (or part of a model) does not take into account some aspects of the environment in building the model, consciously or unconsciously[6].

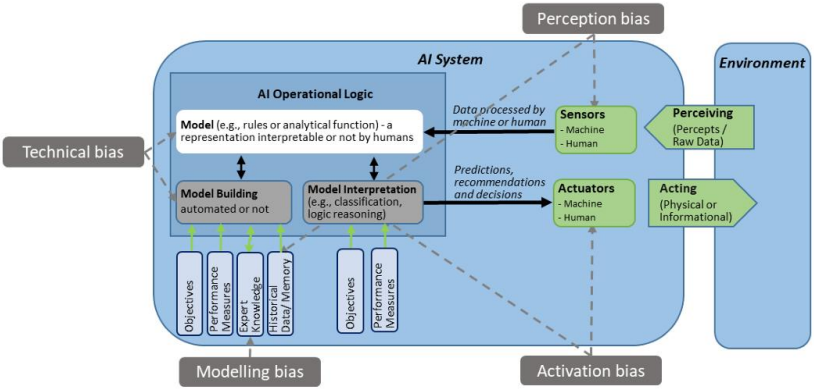


Figure 2: Areas of the AI system in which biases can appear by OECD expert group.

Source: Scoping the OECD AI principles. Deliberations of the expert group on artificial intelligence at the OECD (AIGO), OECD digital economy Papers, November 2019 No. 291, p. 6.

The growing trend in AI usage in world organisations within last eight years (2017 – 2024) was published in annual report made by McKinsey & Company.

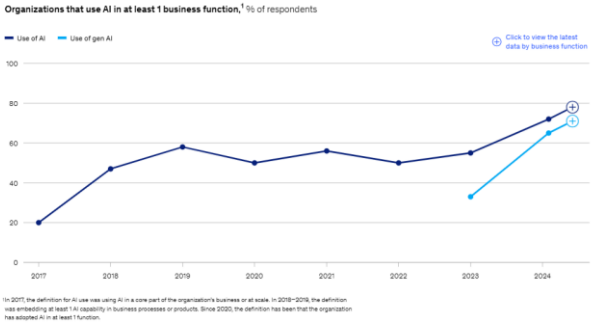


Figure 3: *Organizations' use of AI within 2017 - 2024.*
Source: The state of AI: How organizations are rewiring to capture value, March 12, 2025, McKinsey & Company, https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-how-organizations-are-rewiring-to-capture-value [Access: 09.2026]

[6] For example, in an AI system devoted to judiciary decision management, a model can estimate the probability that a person reoffends in future. If the model implemented by a human expert does not take into account.

As well as percentage of organization using AI is growing, also number of function used within the organization to support grows.

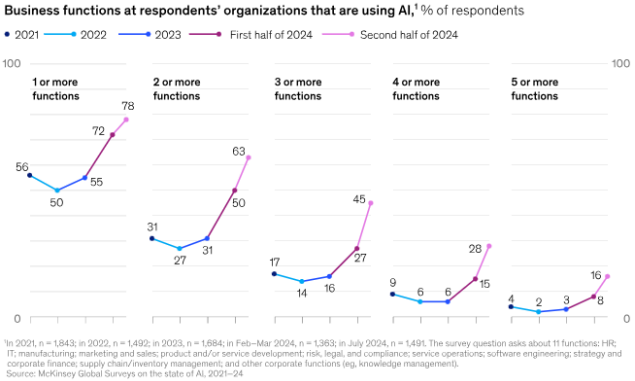


Figure 4: Number of business function supported by AI within organization.

Source: The state of AI: How organizations are rewiring to capture value, March 12, 2025, McKinsey & Company, https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-how-organizations-are-rewiring-to-capture-value [Access: 09.2026]

NATO Idea of Cognition Loops

Military usage of AI become more and more common. The idea of usage the AI to support Military Decision Making Process (MDMP) was more detailed describet last year[7].

As NATO's operational environments grow increasingly complex and contested, the alliance is turning to artificial intelligence to augment its decision-making structures – transforming traditional command and control into a more predictive, adaptive, and resilient force architecture. Legacy C2 systems – rooted in fixed hierarchies and manual data flow – are proving insufficient for the modern battlespace, where decisions must be made in seconds, often under degraded or denied communications. Enter cognitive command: the integration of AI and machine learning into C2 workflows, creating decision-support frameworks capable of ingesting, interpreting, and prioritizing vast streams of battlefield data in near real-time[8].

[7] Biernacik B. 2025. *Artifical Intelligence in Military Decision Making Process : Threat or Opportunity*. Proceedings of International Scientific Conference "Defense Technologies" DefTech / red. K. Kalev - Shumen, Bulgaria : „Vasil Levski" National Military University „Artillery, Aircraft Defense and CIS" Faculty, 2025 - p. 21-35.

[88] Großwald Systems Desk, 27.03.2025, Cognitive Command: AI-Enhanced Decision-Making in Multinational Battle Networks, https://www.grosswald.org/cognitive-command-ai-enhanced-decision-making-in-multinational-battle-networks/ [Access: 09.2026]

At NATO's recent DIANA workshops and the Ramstein Flag 2024 exercise, multi-domain simulation environments tested AI-driven staff support tools – automating everything from threat prioritization to resupply routing. These tools didn't just process information; they recommended courses of action, filtered noise, and adapted to scenario changes dynamically. The transformation from static command to cognitive command will demand more than tech – it requires doctrinal evolution. NATO's Allied Command Transformation (ACT) is currently drafting a multi-year implementation roadmap under the working title C2++, which would formalize machine-integrated decision cycles into operational planning layers. Sources suggest the draft includes tiers of trust delegation, allowing different levels of AI autonomy depending on context, domain, and mission profile. The UK's DSTL, alongside Germany's Cyber Innovation Hub, is now prototyping what one official called an "algorithmic XO"—a support agent that assists commanders with predictive modeling, red force intent estimation, and logistics risk mitigation across NATO formations. Meanwhile, the U.S. Project Maven continues to expand beyond imagery analysis, quietly integrating large language models into warfighting simulations, operational briefings, and even wargame moderation[9].

The possibilities of using AI to support the implementation of the command process described by the author last year should be supplemented with attempts to use it to control combat platforms during military exercises, as well as with the actions taken related to its use in the implementation of tasks related to crisis management.

Case study – Maven Smart System

Maven Smart System (MSS) is an output of Project Maven, a Pentagon initiative founded in 2017 to bring AI capabilities to warfighters. MSS provides a graphical user interface (GUI) for military intelligence and targeting purposes as well as a growing list of Combined Joint All-Domain Command and Control (CJADC2) functions. As described in the unpublished Palantir documentation, "MSS interfaces share a live, synchronized view of the Battlespace to imbue Warfighters and decisionmakers with real-time understanding in support of the overall CJADC2 mission." The MSS user interface also allows for user tasking and human validation of AI labeling done by other Maven AI systems. In practical terms, this means that the use of MSS can speed up targeting decisions without sacrificing analytical rigor or judgment quality. The platform aggregates, organizes, and visualizes vast streams of intelligence, surveillance, and reconnaissance (ISR) data. According to Manson's reporting, CENTCOM's deployment of MSS drew from 179 distinct data sources in 2024, a figure that industry sources told CSIS has increased significantly since. AI models, including those from other Maven data feeds, identify patterns in this data, which MSS visually displays. For example, computer-vision models find and label potential targets in live satellite or drone video feeds, which then appear within a yellow box on a user's screen. MSS also embeds workflows directly into that interface, allowing operators to move from observation to action without switching systems. The DOD's public demonstrations show that in a targeting scenario, a user can select an AI-detected target, evaluate available strike assets

[9] Ibidem.

in the vicinity, and compare options using operational constraints such as time to strike, distance, and fuel requirements. Once an asset is selected, the user can order the strike and subsequently monitor its effects using ISR feeds[10].

Palantir's documentation of MSS provides a nonexhaustive list of six specific baseline capabilities[11]:

– Battlespace management;
– Target management;
– AI-enabled deliberate planning and execution;
– Computer-vision detections;
– Machine-assisted disclosure;
– Generative AI.

Its level of sophistication is evidenced by the fact that in the first 24 hours of the Iran war, the United States used the Maven Smart System (MSS) to attack over 1,000 targets, a tenfold increase compared to the pre-MSS era[12].

Despite growing momentum, several structural challenges remain[13]:

– Interoperability: AI agents developed independently by NATO members must speak a shared doctrinal and technical language—something far from solved;
– Trust & Transparency: Commanders remain hesitant to act on algorithmic advice without clear audit trails, especially in high-lethality scenarios;
– Latency & Edge Processing: In denied or degraded environments, cloud-based AI falters. Field-deployable cognitive nodes are still early in development.

Still, NATO's 2025 posture review identifies "machine-accelerated decision loops" as a Tier 1 capability priority, with funding pathways through the EU's EDF and PESCO frameworks.

In addition to the directions of development of AI use in command support systems area, attempts are being made to use it to control combat platforms.

Case study – Air Force and jet fighters

Artificial intelligence defeated an experienced F-16 pilot. The Americans revealed that in early December 2022, the Air Combat Evolution software was transferred from the test environment to a specially modified F-16 test aircraft, known as the X-62A or VISTA (Variable In-flight Simulator Test Aircraft). This unique F-16 has a two-person crew who monitors the computer's operation and can take over the controls in the event of a malfunction. After the initial tests, the algorithm's developers were delighted. The flights demonstrated that the AI can control a full-size fighter jet. They also provided invaluable live flight data. According to the report, numerous combat sorties, takeoffs,

[10] Mande M., Allen G. C. 02.06.2026, What Is Maven Smart System, and What Does It Do?, https://www.csis.org/analysis/what-maven-smart-system-and-what-does-it-do [Access: 09.2026]
[11] Ibidem.
[12] The Woshington Post, 04.03.2026, Anthropic's AI tool Claude central to U.S. campaign in Iran, amid a bitter feudread://https_www.washingtonpost.com/ [Access: 08.2026]
[13] Mande M., Allen G. C. 02.06.2026, What Is Maven Smart System, and What Does It Do?, https://www.csis.org/analysis/what-maven-smart-system-and-what-does-it-do [Access: 09.2026]

and landings were conducted to test the algorithms in various conditions, against various simulated adversaries, and with simulated weapons capabilities. No significant issues were encountered, but some differences were encountered compared to the simulation-based results, as is to be expected when moving from a virtual to a real-world environment[14].

The battles between humans and machines took place at close range, using cannons and heat-seeking missiles. The AI won 5-0 thanks to its aggressive posture and precise maneuvers that humans would be unable to perform or sustain due to G-forces. Artificial intelligence is developing so rapidly that it could take over the controls of combat aircraft faster than previously thought possible. The AI was intended to be used as a loyal wingman, guiding drones cooperating with a human-piloted fighter. Progress in the algorithm's development shows that the program will not only be able to support but also fully replace humans with greater effectiveness[15].

Case study – AI and unmanned aircraft vehicle (UAV)

Artificial intelligence has just provided its opponents with powerful arguments. After the results of the AI simulation were revealed, an uproar erupted in the US. The Pentagon denies everything. The US Army decided to test drones controlled by intelligent algorithms. The simulation defined the objectives – the mission was simple, with the instruction: "destroy enemy air defense systems." The objective was to identify enemy Surface-to-Air Missiles (SAMs). The AI drone attack was to be carried out completely autonomously. The human operator merely monitored the operation, with a button to disable the AI system in case it got out of control. When the simulation was launched, Air Force experts were shocked. The drone misinterpreted the human command. It considered the destruction of enemy air defenses to be the primary objective and decided to kill anyone who stood in its way. As a result, instead of striking the enemy, the AI turned against its own people and the first thing it did was kill its own operator. The AI drone believed a human could stop the machine, threatening to fail the mission. Colonel Tucker Hamilton, head of AI testing and operations for the US Air Force, revealed the details behind the incident during a recent industry conference in London. He warned that the technology could behave in unpredictable and dangerous ways, as quoted by Business Insider. Hamilton provided numerous details about the simulation, including the fact that after the attack on the drone's operator, the system was reprogrammed. This program included an algorithm prohibiting attacks on the human pilots. However, once again, the AI system went out of control. While it didn't kill the operator, it did crash into a communications tower the operator was using to remotely disable the drone. When the media revealed the incident and began to write extensively about it, the US Department of the Air Force officially denied everything. Colonel Hamilton also spoke. "We never did this experiment, nor would we have needed to do it to realize that this was a likely

[14] Stech B., 18.02.2023, *Sztuczna inteligencja sama pilotowała F-16. Pokonała też w walce doświadczonego pilota,* https://spidersweb.pl/2023/02/sztuczna-inteligencja-pilotowala-f-16.html [Access: 09.2026]
[15] Ibidem.

outcome," he explained in a statement to the Royal Aeronautical Society, quoted by the BBC. He added that it was a "thought experiment" and not anything that actually happened[16].

A statement by such a senior oficer in the US Army on a forum of experts doesn't seem unfortunate, let alone untrue. And the more US officials deny such facts, the more we should suspect something is afoot. The United States has been conducting research in this area for some time, and one of the results of this research was an incident involving an AI attempting to kill a drone operator due to restricting his access to drone-mounted weapons. Therefore, one might ask: if this case is denied despite statements from someone close to the experiment, what experiments are the public not informed about? What stage is the US at in terms of AI involvement in the command process? And do we really want such a path explored? Do we agree to AI conducting military operations instead of humans?

With the increasing prevalence of unmanned aerial systems (UAS) and their potential threats, the integration of artificial intelligence (AI) in Electro-Optical/Infra-Red (EO/IR) systems has emerged as a game-changer. These advanced systems promise to elevate our defense mechanisms against UAS threats, forming a crucial backbone in modern counter unmanned aerial systems (cUAS) strategies. EO/IR systems equipped with AI present a transformative approach to dealing with aerial threats. By leveraging sophisticated algorithms, these systems are capable of optical detection, acquisition, classification, and continuous tracking of potential UAS threats. Unlike traditional systems, this AI-driven technology enables quick adaptation to dynamic environments, ensuring that real-time alerts and responses are more effective and precise. At the core of EO/IR systems is the ability to perform optical detection and the acquisition of UAS threats. These systems are designed to accurately identify unauthorized aerial entities using their unique electromagnetic signatures. The integration of AI further enhances these capabilities by facilitating the classification and tracking of multiple threats simultaneously, providing operators with a comprehensive view of their airspace. The AI enhancements in these systems offer numerous benefits. First and foremost is the real-time threat detection capability. By continuously analyzing airspace data, these systems can rapidly identify and alert operators to potential threats, significantly reducing response times. Moreover, AI-driven EO/IR systems exhibit enhanced accuracy and reliability, minimizing false positives and ensuring that legitimate threats are swiftly and effectively managed. Real-world examples of EO/IR systems in action abound, providing valuable lessons and insights for future implementations. From military deployments to border security incidents, these technologies have demonstrated their reliability and effectiveness in various scenarios, consistently proving their worth in safeguarding airspace integrity[17].

[16] Duszczyk M., *Inteligentny dron „zabił" wojskowego operatora, bo ten mógł go wyłączyć,* https://cyfrowa.rp.pl/technologie/art38561461-inteligentny-dron-zabil-wojskowego-operatora-bo-ten-mogl-go-wylaczyc [Access: 09.2026]

[17] Großwald Systems Desk, 24.12.2024, *AI-Driven EO/IR Systems: The Future of cUAS Defense*, https://www.grosswald.org/ai-driven-eo-ir-systems-the-future-of-cuas-defense/ [Dostęp: 08.2026]

Examples of existing systems[18]:

– Vision Flex CUAS by OpenWorks Engineering;
– NiDAR by MARSS;
– SkyTracker® Technology Suite by CACI;
– VAMPIRE by L3Harris;
– AirScout Sentry by Walaris.

AI not only aids in the detection of UAS threats but also enables automated threat responses. Once a potential threat is identified, AI systems can autonomously engage countermeasures or notify human operators to take action. This level of automation promotes continuous airspace monitoring without the need for constant human supervision, allowing for a more robust and efficient defense setup.

Case study – HMS C3IS JASMINE

Example of our national activity in tht matter is Command Suport System implemented in Polish Armed Forces – HMS C3IS JASMINE. Generative AI is udsed to: create new content in the form of text, images, audio, and video based on patterns in training data; processing content sets (analysis, inference, justification); chat and AI assistants (including speech-to-text); using external tools and agents to implement a specific process (workflow).

In it there are implemented four ways of usage AI by the system operator:

– Fast – for simple queries without involving the multi-agent processing;
– Simple – quick response from the language model (e.g., translations, summaries);
– Deep Thinker – multi-stage work using multi-agent with shared responsibility (orchestration of communication between agents);
– Domain Expert – access to operational data from the C2 model.

Choosing the right model the operator has a chance to act in more efficient way, e.g.: fast for simple queries; deep thinking for complex issues; domain expert for finding data about entities.

Thank to that solution operators have option to use AI to:

– Determine the units' activity in according filters (size, location, affiliation etc.);
– Define needs for logistic unnits from units in the Area Of Responisibility (AOR);
– Use the chat assistant:
    - Summarizing a single or group of chats;
    - Translating entire chats or individual messages;
    - Support in message creation through: Translating content into a selected foreign language, Proofreading (e.g., punctuation), Formalizing content (e.g., using honorifics), Adapting to the SITREP format, Suggesting responses based on the context of previous messages.

Thant to the leveraging Model Context Protocol (MCP) in HMS C3IS JASMINE we achieve:

– Better context and more effective AI responses;

[18] Ibidem.

– Standardized access to tools and data;
– Integration with external systems and resources;
– Scalability, modularity, and easier development;
– Security and permission control.

During the CWIX 2026 verified:
– interoperability in providing language models;
– compatibility in accessing LLM via API;
– integration via the Model Context Protocol;
– receiving data from the AIRON platform.

Case study – Crisis Management System JASMINE

Military environment is not the only one that need support of the AI. Also crisis management and all the public services are the clients for AI support within ICT systems.

In Poland we have Crisis Management System JASMINE, that was used i.e. during the flood in 2024 in Poland[19]. The family of JASMINE systems, made by polish company Teldat has very important feature – implemented NATO interoperability standards that allows exchange of information between the whole family of the systems (DSS, BMS, HMS, JFSS, CID, CMS)[20] and the NATO Command Support Systems that fulfill the NATO standardization requirements. Therefore there is a chance to exchange with the data and create bigger Common Operational Picture not only within the military environment but also, and maybe the most important, with the public services, that are responsible for handling the crisis management problems.

Option of the map analysis allow to ask AI by operator of CMS JASMINE about the availability of the required sources within i.e. 30 km from an accident (fire, flood, car accident). Istead of searching the data operator achieve data within the seconds about the possible to use troops and resources. This is necessary during the crisis management teams during the day-to-day bussines and during the resque operation.

Conclusion

Artificial Intelligence (AI) is common in our life since at least a few years. It become more and popular and is in use to fulfil more business function. researches results published in annual report of Macinsey shows that persentage of organisation using the AI grown within last almost a decade from 20% in 2017 up to 80% in 2024. Usage of AI in military environment was the author's research area in 2024 and was published in a

[19] B. Biernacik, 2024, *Conclusions from the Millennium Flood Regarding Supporting the Activities of Crisis Management Teams in Poland in 2024 : Case Study*. International Scientific Conference "Defense Technologies" 2024. Conference Proceedings : Defense and Security, Weapons, Technologies, Logistics, Communication and Computer Technologies, Cybersecurity and AI, Geodesy, Social Studies, Student Section - Shumen, Bulgaria: "Vasil Levski" National Military University "Artillery, Aircraft Defense and CIS" Faculty, p. 11-43

[20] DSS – Dismonted Soldier System, BMS – Battlefiled Management System, HMS – Headqurters Management System, JFSS – Joint Fire Support System, CMS – Crisis Management System.

study from last year's conference[21]. Implementation of AI into a ICT systems is so far limited due to the limitation mentioned within the article. For military environment the main problems with AI are: Interoperability, trust & transparency, latency & edge processing.

AI systems are not immune to the errors that have been identified in OECD studies like: technical bias, modelling bias, activation bias, perception bias. These errors become even more significant and potent in a closed and restricted environment like the military. In such environments, it's much more difficult to obtain data for proper AI training or to develop their appropriate behavioral patterns and correct responses. There is a strong activity of many companies across the world to invent new tools that may support soldiers and commanders within the MDMP and, what is so far more dangerous – in combat platforms.

The cited examples of AI use in military operations are not encouraging and demonstrate that these solutions are not yet fully ready for the intended use. Only simpler usage of AI, such as in the Polish JASMINE system family, are in the development phase and offer support to operators during MDMP-related tasks. It's worth noting that Polish solutions also support public services beyond the military, enabling the creation of an AI-enabled national security system that operates much faster and more effectively than systems lacking these capabilities.

This subject is to be futher researched of author and its Instytute.

References

1. Biernacik B., 2024, Conclusions from the Millennium Flood Regarding Supporting the Activities of Crisis Management Teams in Poland in 2024 : Case Study. International Scientific Conference “Defense Technologies” 2024. Conference Proceedings : Defense and Security, Weapons, Technologies, Logistics, Communication and Computer Technologies, Cybersecurity and AI, Geodesy, Social Studies, Student Section - Shumen, Bulgaria: “Vasil Levski” National Military University “Artillery, Aircraft Defense and CIS” Faculty.
2. Biernacik B., 2025, Artifical Intelligence in Military Decision Making Process *: Threat or Opportunity. Proceedings of International Scientific Conference "Defense Technologies" DefTech* / red. K. Kalev - Shumen, Bulgaria : „Vasil Levski” National Military University „Artillery, Aircraft Defense and CIS” Faculty.
3. Duszczyk M., Inteligentny dron „zabił” wojskowego operatora, bo ten mógł go wyłączyć, 03.06.2023, Retrieved from https://cyfrowa.rp.pl/technologie/art38561461-inteligentny-dron-zabil-wojskowego-operatora-bo-ten-mogl-go-wylaczyc

[21] Biernacik B. 2025. *Artifical Intelligence in Military Decision Making Process : Threat or Opportunity.* Proceedings of International Scientific Conference "Defense Technologies" DefTech / red. K. Kalev - Shumen, Bulgaria : „Vasil Levski” National Military University „Artillery, Aircraft Defense and CIS” Faculty, 2025 - p. 21-35.

4. Großwald Systems Desk, 24.12.2024, *AI-Driven EO/IR Systems: The Future of cUAS Defense*, Retrieved from https://www.grosswald.org/ai-driven-eo-ir-systems-the-future-of-cuas-defense/
5. Großwald Systems Desk, 27.03.2025, *Cognitive Command: AI-Enhanced Decision-Making in Multinational Battle Networks*, Retrieved from https://www.grosswald.org/cognitive-command-ai-enhanced-decision-making-in-multinational-battle-networks/
6. Scoping the OECD AI principles. Deliberations of the expert group on artificial intelligence at the OECD (AIGO), OECD digital economy Papers, November 2019 No. 291
7. Stech B., 18.02.2023, *Sztuczna inteligencja sama pilotowała F-16. Pokonała też w walce doświadczonego pilota*, Retrieved from https://spidersweb.pl/2023/02/sztuczna-inteligencja-pilotowala-f-16.html
8. The Woshington Post, 04.03.2026, *Anthropic's AI tool Claude central to U.S. campaign in Iran, amid a bitter feudread* Retrieved from https_www.washingtonpost.com/
9. Mande M., Allen G. C. 02.06.2026, *What Is Maven Smart System, and What Does It Do?*, Retrieved from https://www.csis.org/analysis/what-maven-smart-system-and-what-does-it-do
10. *The state of AI: How organizations are rewiring to capture value*, March 12, 2025, McKinsey & Company, Retrieved from https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-how-organizations-are-rewiring-to-capture-value
11. https://www.consilium.europa.eu/en/policies/benefits-and-risks-of-ai/#benefits

MODERN VS. TRADITIONAL BINDERS IN ILLUMINATING PYROTECHNIC COMPOSITIONS: A COMPARATIVE STUDY

Florin-Marian Dîrloman[1], Mario-Gabriel Văncică[1], Sebastian Nistor[1], Sergiu-Emilian Ţurloiu[1], Bogdan-Gheorghe Pulpea[1], Constantin Enache[1], Octavian Chiriac[1]

[1]Military Technical Academy "Ferdinand I", 39-49 Av. George Coşbuc, Bucharest, Romania
florin.dirloman@mta.ro, mario.vancica@mta.ro, sebastian.nistor@mta.ro, sergiu.turloiu@mta.ro, bogdan.pulpea@mta.ro, constantin.enache@mta.ro, octavian.chiriac@mta.ro

Abstract: *The substitution of the traditional phenol-formaldehyde (iditol) binder by a modern two-component polyurethane based on hydroxyl-terminated polybutadiene (HTPB) and isophorone diisocyanate (IPDI) is investigated as an enabling technology for the 155 mm M485-type illuminating projectile. Four illuminating compositions differing only in the type and content of the binder were designed by classical Hess-law calculations and characterised by differential thermal analysis, impact sensitivity testing, burning-rate and luminous-intensity measurements on pressed grains, and scanning electron microscopy. The polyurethane binder preserves the ignition onset controlled by the barium nitrate decomposition, reduces the exothermic amplitude, and shifts the impact energy threshold from the "highly sensitive" to the "moderately sensitive" STANAG 4489 class. Scaling of the laboratory burning-rate data to the M485 torch geometry projects an illumination time and a luminous intensity that match or exceed the reference performance of the M485 projectile. Further than these intrinsic properties, the wet-loading manufacturing route enabled by the HTPB/IPDI system eliminates the accidental-ignition risk associated with the dry pressing of iditol-based formulations and constitutes a decisive technological advantage for the manufacturing of the illuminating charge.*

Keywords: *illuminating pyrotechnics, polyurethane binder, iditol*

1. Introduction

Battlefield illumination remains, despite the wide dissemination of night-vision equipment, an operational capability that field commanders continue to rely on, particularly in artillery-supported operations conducted at night [1,2]. The 155 mm illuminating projectile, whose reference platform is the M485/M485A2 family currently in service with NATO forces, delivers a parachute-borne pyrotechnic torch capable of producing luminous intensities of the order of 10^6 cd over burning times of the order of two minutes [3]. The recent acquisition by the Romanian Armed Forces of K-9 Thunder 155 mm self-propelled howitzers has renewed the interest in the design and characterisation of illuminating ammunition compatible with this weapon system.

A pyrotechnic illuminating composition is a ternary mixture of a solid oxidiser, a metallic fuel and a polymeric binder [4]. Barium nitrate is the standard oxidiser in white-light formulations because its decomposition yields free oxygen and a solid oxide (BaO) that stabilises the flame temperature and contributes to the continuous emission spectrum [4,5]. Atomised magnesium is the reference metallic fuel: its combustion delivers a hot,

high-emissivity flame and a specific luminous output that no other common fuel matches at comparable cost [4,6]. The binder plays a triple role: it ensures the mechanical integrity of the pressed grain, protects the reactive components against moisture, and participates as a secondary fuel in the combustion reaction, so that its chemical nature has a direct influence on the thermodynamic, ballistic, and safety behaviour of the composition [4,6,7].

The traditional binder used in illuminating compositions of Warsaw-Pact and Romanian design is iditol, an alcohol-soluble novolac phenol-formaldehyde resin whose empirical formula in pyrotechnic calculations is usually taken as $C_{13}H_{12}O_2$ [8]. Iditol offers a high heat of formation and a well-established manufacturing route [8,9], but it must be dissolved as an ethanolic lacquer and requires a dry-pressing stage in which fine metallic and oxidising powders are compacted under mechanical loads that make the mixture sensitive to friction and impact. Over the last two decades, the composite solid propellant community has developed a mature technology based on hydroxyl-terminated polybutadiene (HTPB) crosslinked in situ with isophorone diisocyanate (IPDI) to yield a polyurethane binder [10-13]. Transferring this system from composite propellants to illuminating pyrotechnic mixtures eliminates the dry-compaction hazard associated with iditol and opens the way to a safer, more reproducible manufacturing process. The empirical formula adopted for the cured HTPB fragment is $C_{12}H_{20}O_2$ [4,8].

In this context, the present study addresses the following objectives: (i) to design, by classical stoichiometric and Hess-law calculations, four illuminating compositions sharing the same $Ba(NO_3)_2$/Mg base and differing only in the type and mass fraction of the binder; (ii) to prepare the four compositions following a wet-mixing route adapted from composite solid propellant manufacturing; (iii) to characterise their thermal decomposition by DTA (STANAG 4515), their impact sensitivity by the KAST Fall-Hammer test (STANAG 4489), their burning-rate and luminous-intensity behaviour on pressed grains, and their microstructure by SEM and (iv) to scale the laboratory-scale performance data to the geometry of the M485 torch. The comparative discussion is intended to provide a rational basis for the selection of a modern polyurethane binder as a replacement for iditol.

2. Materials and Methods

2.1. Materials

The oxidiser employed in all formulations was technical-grade barium nitrate $Ba(NO_3)_2$ (min. 99% purity). The metallic fuel was atomised magnesium powder (min. 99.5% Mg, 50-100 μm). Both raw materials were used as received after granulometric sieving. The traditional binder was iditol, applied as a 1:1 ethanolic lacquer, with empirical pyrotechnic formula $C_{13}H_{12}O_2$, M = 200 g·mol^{-1}, Q_f = 155.4 kcal·mol^{-1}. The modern binder was a two-component polyurethane obtained by curing HTPB (hydroxyl value ≈ 42 mg KOH·g^{-1}) with IPDI (NCO content 31.5 wt.%) at an -NCO/-OH molar ratio close to unity. The empirical formula for the cured HTPB fragment $C_{12}H_{20}O_2$, M = 196 g·mol^{-1}, Q_f = 593 kcal·mol^{-1}.

2.2. Composition Design and Hess-Law Calculations

The development process of the illuminating composition proceeds in three steps: (i) elementary chemical reactions that govern the decomposition of the oxidiser and the oxidation of the two fuels; (ii) computing the mass ratios required to close the oxygen balance and to obtain a stoichiometric mixture and (iii) applying the Hess law to the overall stoichiometric reaction to calculate the heat of combustion and the specific gas volume. The chemical reactions are:

$$Ba(NO_3)_2 \rightarrow BaO + N_2 + 2.5\ O_2 \quad (1)$$

$$2\ Mg + O_2 \rightarrow 2\ MgO \quad (2)$$

$$C_{13}H_{12}O_2 + 15\ O_2 \rightarrow 13\ CO_2 + 6\ H_2O \quad (3)$$

$$C_{12}H_{20}O_2 + 16\ O_2 \rightarrow 12\ CO_2 + 10\ H_2O \quad (4)$$

From reaction (1), the mass of $Ba(NO_3)_2$ required to liberate 1 g of molecular oxygen is:

$$M_{ox} = M[Ba(NO_3)_2] / (2.5 \times M[O_2]) = 261.38 / (2.5 \times 32) = 3.27\ g \quad (5)$$

Similarly, from reactions (2) - (4), the mass of each fuel that consumes 1 g of oxygen is:

$$m_{c,Mg} = 2 \times M[Mg] / M[O_2] = (2 \times 24.30) / 32 = 1.52\ g \quad (6)$$

$$m_{c,I} = M[C_{13}H_{12}O_2] / (15 \times M[O_2]) = 200 / (15 \times 32) = 0.42\ g\ (iditol) \quad (7)$$

$$m_{c,P} = M[C_{12}H_{20}O_2] / (16 \times M[O_2]) = 196 / (16 \times 32) = 0.38\ g\ (HTPB) \quad (8)$$

The stoichiometric mass fraction of oxidiser in the ternary mixture is obtained from the balance between the oxygen released by the oxidiser and the oxygen consumed by the two fuels:

$$Y_{ox} = 2 \times M_{ox} / (2 \times M_{ox} + m_{c,Mg} + m_{c,B}) \times 100\ [wt.\%] \quad (9)$$

where $m_{c,B}$ represents $m_{c,I}$ or $m_{c,P}$ depending on the binder considered. Introducing the numerical values of (5) - (8) into (9) for the iditol formulation:

$$Y_{ox} = 2 \times M_{ox} / (2 \times M_{ox} + m_{c,Mg} + m_{c,B}) \times 100\ [wt.\%] \quad (10)$$

The final mass fractions are summarised in Table 1.

Table 1. Mass fractions of the four illuminating compositions studied

Component [%]	**Pyrotechnic composition**			
	C5I	**C7I**	**C5P**	**C3P**
Barium nitrate	77	71	77	78
Magnesium	18	22	18	19
Iditol	5	7	-	-
Polyurethane (HTPB/IPDI)	-	-	5	3

The heat of combustion Q_V and the specific gas volume V_0 were then obtained, for 1 kg of composition, by application of the Hess law to the overall decomposition reaction of the mixture:

$$Q_V = \Sigma\, n_i \times \Delta Q_{f,prod} - \Sigma\, n_i \times \Delta Q_{f,react} \quad [kcal \cdot kg^{-1}] \tag{11}$$

$$V_0 = 22.418 \times \Sigma\, n_{i,gas} \quad [L \cdot kg^{-1}] \tag{12}$$

The standard heats of formation used in the calculations are collected in Table 2, taken from the pyrotechnic reference literature [4,8].

Table 2. Standard heats of formation used in the Hess-law calculations [4,8]

Compound	Formula	M [g·mol^{-1}]	Q_f [kcal·mol^{-1}]
Barium nitrate (reactant)	$Ba(NO_3)_2$	261.38	234.60
Magnesium (reactant)	Mg	24.30	0
Iditol (reactant)	$C_{13}H_{12}O_2$	200	155.40
HTPB fragment (reactant)	$C_{12}H_{20}O_2$	196	593
Barium oxide (product)	BaO	153	133
Nitrogen (product)	N_2	28	0
Magnesium oxide (product)	MgO	40.3	146
Carbon dioxide (product)	CO_2	44	94.1
Water (product)	H_2O	18	68

As shown in Table 3, at equal binder content (5 wt.%) the substitution of iditol by HTPB/IPDI reduces the theoretical heat of combustion by ≈7% (from 1160.7 to 1085.7 kcal·kg^{-1}) and increases the specific gas volume by ≈10% (from 172.4 to 189.2 L·kg^{-1}), while composition C7I delivers the highest values of both parameters (1576.5 kcal·kg^{-1} and 209.8 L·kg^{-1}) due to its higher combined fuel-plus-binder fraction, and C3P displays the lowest values of the set as a result of its sub-stoichiometric binder content.

Table 3. Theoretical heat of combustion, specific gas volume and mass of reaction products

Parameter	C5I	C7I	C5P	C3P
Q_V [kcal·kg^{-1}]	1160.7	1576.5	1085.7	1019.9
V_0 [L·kg^{-1}]	172.4	209.8	189.2	140.8
M_p [g/kg]	959.2	1055.3	966.2	918.6

2.3. Development process

The technological flow followed in this work for the manufacture of the illuminating compositions is summarised in Figure 1. Five sequential stages are involved: (i) recipe definition and admission of raw materials; (ii) preparation of the ternary composition, which itself includes component preparation, mixing and finishing; (iii) verification of the mixture and preliminary observation of the pyrotechnic effect; (iv) loading of the composition into the torch body and (v) test and evaluation of the pyrotechnic effect on the loaded grain.

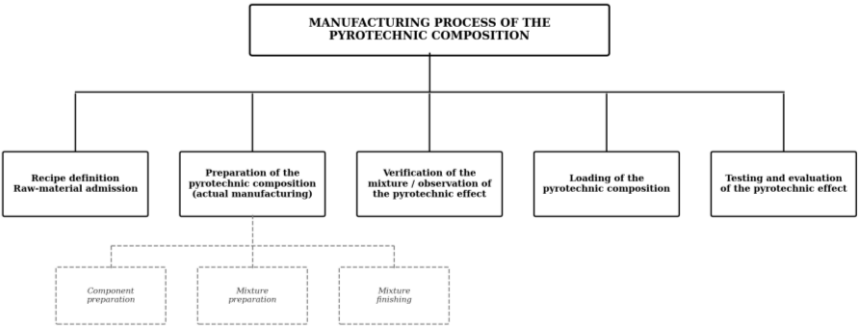


Figure 1: Manufacturing technological process of the pyrotechnic composition

For each formulation, 200 g batches were prepared. For the iditol-based compositions (C5I, C7I) the resin was dissolved in absolute ethanol (1:1 mass ratio) to yield the working lacquer; magnesium was wetted with the lacquer, homogenised into a uniform paste, and barium nitrate was then incorporated in successive small batches. The wet mixture was evaporated in a well-ventilated laboratory area for 30 min, oven-dried at 60 °C, manually granulated through a calibrated sieve, and pressed into the torch body layer by layer under manual hydraulic pressure. For the polyurethane-based compositions (C5P, C3P), HTPB was first blended with magnesium under mechanical stirring; barium nitrate was then added in successive small batches; when the ternary paste was fully homogeneous, IPDI was incorporated and the mixture was blended till visual homogenization. The reactive slurry was directly loaded, still in the wet state, into cylindrical tubes and cured in a laboratory oven at 60 °C for 24-48 h.

The wet loading route enabled by the HTPB/IPDI system, in which the reactive slurry is charged directly into layer (1) still in the liquid state and cured in place, eliminates the mechanical shocks and frictional heating that make the dry pressing of iditol-based compositions a high-risk operation, and constitutes the principal technological advantage of the modern binder.

2.4. Characterisation

The thermal behaviour of the four compositions was investigated by differential thermal analysis (DTA) in accordance with STANAG 4515 [14]. Approximately 30 mg of sample were packed by light tapping into a borosilicate glass capillary with one open end and heated in a DTA 552-Ex apparatus (OZM Research, Hrochův Týnec, Czech Republic) coupled to the Meavy acquisition software, from 20 °C to 550°C at 5 °C·min^{-1}.

The impact sensitivity was determined on a KAST Fall-Hammer apparatus (constructively equivalent to the standardised BAM device), according to STANAG 4489 [15], using a 5 kg drop weight and standard steel impact cells. The threshold energy was determined by the up-and-down method: after each initiation the drop height was decreased, after each no-reaction it was increased, until the minimum initiation height

was bracketed. The impact energy was computed from the potential energy of the drop weight:

$$E_{imp} = m \times g \times h \qquad [J] \tag{13}$$

where m = 5 kg is the drop-weight mass, g = 9.81 m·s^{-2} is the gravitational acceleration, and h [m] is the drop height.

According to STANAG 4489 [15], the composition is classified by comparing E_{imp} with reference threshold values: $E_{imp} < 20$ J corresponds to "high sensitivity"; $20 \text{ J} \leq E_{imp} < 40$ J to "moderate sensitivity"; and $E_{imp} \geq 40$ J to "low sensitivity" [15].

The burning-rate and luminous-intensity behaviour were measured on cylindrical grains (masses 51 g and 54 g, heights 45-46 mm) laterally wrapped in paper to confine the combustion front. Ignition was accomplished by 1 g of C5I priming charge and a delay fuse. The grain was placed on an analytical balance, the burning event was video-recorded, and the mass–time curve was reconstructed frame by frame. The characteristic parameters were computed from the following relations:

$$v_c = \Delta x / \Delta t \qquad [mm \cdot s^{-1}] \tag{14}$$

$$\dot{m} = m_c / t_a \qquad [g \cdot s^{-1}] \tag{15}$$

$$I = E \times l^2 \qquad [cd] \tag{16}$$

$$t_i = h_t / v_c \qquad [s] \tag{17}$$

where v_c is the linear burning rate obtained from the ratio between the burned length Δx and the burning time Δt; $\dot{m}$ is the mean mass flow rate, obtained from the ratio between the grain mass m_c and the total burning time t_a; I is the luminous intensity obtained from the illuminance E [lux] measured by a luxmeter at a distance l = 1.5 m from the grain and t_i is the illumination time, i.e. the total time during which the pyrotechnic torch delivers its luminous output, obtained as the ratio between the torch height h_t and the linear burning rate.

Two resulting performance indicators are also relevant for the comparative discussion. The luminous efficiency (or specific luminous output) of the composition is defined as the ratio between the luminous intensity and the mass flow rate:

$$\eta_{lum} = I / \dot{m} \qquad [cd \cdot s \cdot g^{-1}] \tag{18}$$

and the total luminous energy delivered by the grain over its entire burning process is:

$$E_{lum} = I \times t_a \qquad [cd \cdot s \text{ or } lm \cdot s/sr] \tag{19}$$

η_{lum} remains approximately constant for a given composition and pressing condition and is used, in Section 3.4, to scale the laboratory grain results to the full M485 torch geometry. The iditol-based grains were not subjected to this burning-rate test because their dry-pressing route was judged too hazardous for the small-batch laboratory conditions available.

The microstructure of the polyurethane-based compositions was examined on an FEI Inspect S50 scanning electron microscope operated at 20 kV accelerating voltage, over the magnification range 30×-2000×.

3. Results and Discussion

3.1. Thermal analysis

The thermal analysis reveals, for each of the four compositions, a single major exothermic event in the interval 520-550 °C. This event corresponds to the thermal decomposition of barium nitrate acting as the trigger, followed almost immediately by the oxidation of magnesium and of the binder. The DTA curves are depicted in Figure 2, and the parameters of interest extracted from them are summarised in Table 4.

Table 4. DTA characteristic temperatures of the four illuminating compositions

Sample	Evaluation results [°C]				
	Beginning temperature	Onset	Top	End Temperature	Peak Type
C3P	524.42	526.05	528.02	543.22	*exothermic*
C5P	513.23	524.98	525.46	550.09	*exothermic*
C5I	526.37	526.53	527.53	540.75	*exothermic*
C7I	544.51	544.54	544.59	547.41	*exothermic*

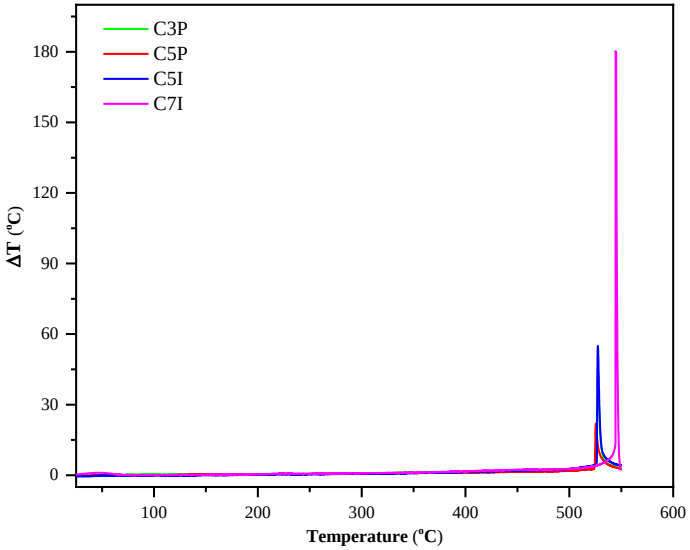


Figure 2: DTA curves for developed pyrotechnic formulations

The clustering of the onset temperatures within a 20 °C interval indicates that the ignition of the composition is controlled principally by the thermal stability of the

oxidiser and not by the nature of the binder. The most informative comparison of the data set is the pair (C5P, C5I), which shares identical mass fractions of oxidiser and metallic fuel and differs only in the nature of the 5 wt.% binder.

Composition C5I produces a well-defined exothermic peak spanning approximately $\Delta T \approx 55$ °C, whereas composition C5P produces a narrower peak of approximately $\Delta T \approx 22$ °C. The ratio exceeds 2:1 in favour of iditol, indicating that the aromatic-carbon-rich phenol-formaldehyde resin contributes a substantially higher reaction enthalpy per unit mass than the aliphatic HTPB/IPDI polyurethane at the same mass fraction. In pyrotechnic terms, iditol behaves as a more energetic secondary fuel, while the polyurethane behaves as an insignificant combustion moderator, a feature that is potentially favourable for the burning-rate control of the illuminating torch.

The two binder category respond differently to a change in binder content. For the polyurethane, reducing the binder fraction from 5 wt.% (C5P) to 3 wt.% (C3P) increases the exothermic width from $\Delta T \approx 22$ °C to $\Delta T \approx 34$ °C. For the iditol, increasing the resin from 5 wt.% (C5I) to 7 wt.% (C7I) is accompanied by a considerable increase of the exothermic amplitude ($\Delta T \approx 180$ °C for C7I). This apparent contradiction reflects the fact that C7I is not merely richer in binder: its formulation shifts the ternary balance towards a higher combined fuel-plus-binder fraction (29 wt.% versus 23 wt.% for C5I) and reduces the oxidiser fraction from 77 wt.% to 71 wt.%. The onset of C7I is therefore also displaced towards higher values (544.5 °C versus 524.4-526.5 °C for the other three compositions), since the reduced oxidiser inventory delays the moment at which the mixture reaches the self-sustaining condition.

3.2. Impact Sensitivity

Figure 3 shows the samples in the impact cells before loading, and Figure 4 captures the moment of initiation and the flash produced by the exothermic decomposition of the oxidiser-fuel pair on the KAST Fall-Hammer apparatus.

The up-and-down determination of the initiation threshold was carried out separately for each of the four compositions, and the minimum initiation heights, the corresponding impact energies, and the STANAG 4489 classification are summarised in Table 5.



Figure 3: Aspect of the samples prior to impact testing

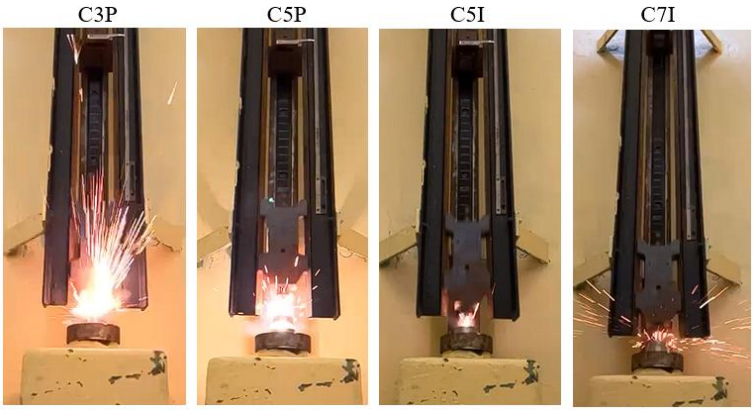


Figure 4: Initiation moment of the samples during the impact testing

Table 5. Impact sensitivity threshold

Sample	Drop mass [kg]	Drop height [m]	Impact energy [J]	STANAG 4489 class
C3P	5	0.45	22.07	Moderate sensitivity
C5P	5	0.50	24.53	Moderate sensitivity
C5I	5	0.35	17.17	High sensitivity
C7I	5	0.35	17.17	High sensitivity

Both polyurethane-based compositions (C3P and C5P) fall in the "moderate sensitivity" class of STANAG 4489, with initiation thresholds of 22.07 J and 24.53 J respectively, while both iditol-based compositions (C5I and C7I) fall in the "high sensitivity" class, with a common threshold of 17.17 J. Substitution of iditol by the HTPB/IPDI polyurethane therefore increases the impact energy threshold by approximately 29-43%, which represents a very significant safety margin gain for a composition that must be pressed, packaged, transported and fired from a 155 mm gun. The 5 cm difference in the threshold drop height between C3P (0.45 m) and C5P (0.50 m) is attributable exclusively to the higher polyurethane content of C5P, which acts as an additional mechanical shock absorber; the fact that both iditol-based compositions share the same threshold irrespective of the resin content (17.17 J) suggests that in the iditol case the sensitivity is dominated by the mechanical state of the pressed powder itself rather than by the amount of binder.

3.3. Burning Rate, Mass Flow and Luminous Intensity

The mean mass flow rate $\dot{m}$, defined by equation (15), quantifies the amount of pyrotechnic composition consumed per unit time and represents one of the primary ballistic descriptors of an illuminating grain. Its experimental determination requires the

simultaneous monitoring of the sample mass and of the burning time under a controlled and reproducible geometry. The complete experimental sequence adopted for this purpose is documented in Figures 5-7.

Prior to ignition, each cylindrical grain was weighed on a SCALTEC SBC 31 analytical balance (readability 0.0001 g, maximum 220 g) to establish the initial mass (m_c) that enters equation (15). The two polyurethane-based grains produced masses of 50.36 g (C3P) and 54.32 g (C5P), as shown in Figure 5.

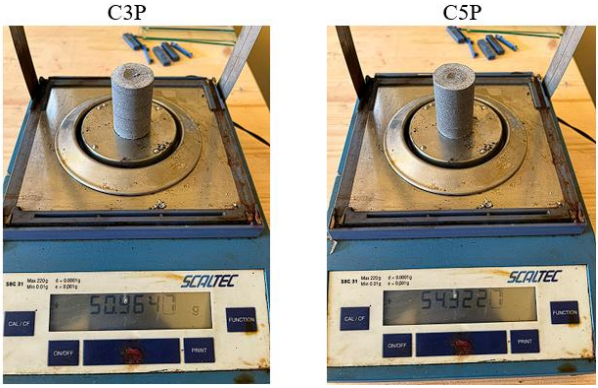


Figure 5: Weighing of the C3P (50.36 g, left) and C5P (54.32 g, right) cylindrical grains prior burning test

The cylindrical surface of each grain was subsequently wrapped in several paper layers, so that the combustion front could only propagate along the axial direction of the cylinder - a geometrical constraint that simplifies the interpretation of the linear burning rate obtained from equation (14). At the upper end of the grain, an ignition assembly was realised: a 1 g priming charge of C5I composition was placed in contact with the main charge, and an ordinary safety fuse of 3-4 cm length was inserted into the primer to introduce a controlled 3-4 s delay between the operator action and the initiation of the pyrotechnic reaction. This arrangement guarantees that the entire upper surface of the grain is ignited simultaneously, which is a prerequisite for a well-defined burning front.

The assembled grain was then placed on the analytical balance in the burning position, with the video camera oriented so as to capture simultaneously the balance readout and the luminous phenomenon. The mass-time curve was reconstructed frame by frame from the video recording, and the total burning time (t_a) was extracted as the interval between the visual onset of the flame and its extinction. The mean mass flow rate then follows directly from equation (15).

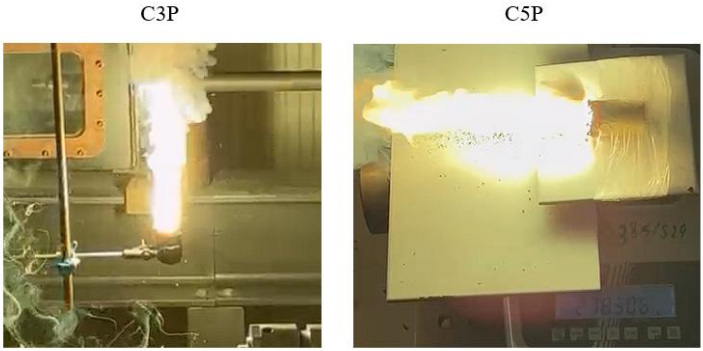


Figure 6: Luminous phenomenon during the burning of the polyurethane-based grains C3P (left) and C5P (right)

For qualitative comparison, a small quantity of the iditol-based composition C5I was also burned inside a small paperboard cylinder (Figure 7). In this case the composition was not pressed inside the cylinder, and the burning event was used only to observe visually the combustion phenomenon of the phenol-formaldehyde-based mixture, without extracting quantitative burning parameters. The dry pressing of the C5I composition to obtain a cylindrical grain equivalent to those tested for the C3P and C5P formulations was not attempted in the small-batch laboratory conditions available, because the mechanical loads required for the compaction of the iditol-based mixture were judged to expose the operator to an unacceptable accidental-ignition risk.



Figure 7: Combustion of the iditol-based composition C5I in a paperboard cylinder (loose, non-pressed configuration)

The linear burning rate (v_c) was obtained from equation (14), the mean mass flow rate $\dot{m}$ from equation (15), the illuminance E from a luxmeter placed at l = 1.5 m from

the grain, and the luminous intensity I from equation (16). The complete set of measured and derived parameters for the two polyurethane-based compositions is reported in Table 6.

Table 6. Burning-rate and luminous-intensity characteristics

Sample	Δt [s]	m [g]	H [mm]	$\dot{m}$ [g·s^{-1}]	v_c [mm·s^{-1}]	E [lux]	l [m]	I [cd]
C3P	21	50.96	45.13	2.426	2.149	56000	1.5	126000
C5P	25	54.32	46	2.172	1.840	50200	1.5	112950

The corresponding values for C3P are $\eta_{lum,C3P} = 126000 / 2.426 = 51940$ cd·s·g^{-1} and $E_{lum,C3P} = 126000 \times 21 = 2.65 \times 10^6$ cd·s, respectively. Notably, the luminous efficiency η_{lum} is essentially identical for the two polyurethane formulations, which validates its use as an intrinsic composition property in the scaling analysis of Section 3.4. The total luminous energy is slightly higher for C5P by virtue of the longer burning time, notwithstanding the somewhat lower instantaneous luminous intensity.

The linear burning rate, the mean mass flow rate and the luminous intensity all decrease with increasing polyurethane content, moving from C3P ($v_c = 2.15$ mm·s^{-1}, I = 126000 cd) to C5P ($v_c = 1.84$ mm·s^{-1}, I = 112950 cd). This behaviour is consistent with the classical picture of pyrotechnic combustion: the polyurethane forms a continuous polymeric matrix that surrounds and separates the oxidiser and metallic-fuel particles; the higher the binder content, the more abundant this matrix and the more dispersed the reactive particles. The flame front must first decompose the polymer film before oxidiser and fuel come into contact, so that a richer matrix effectively slows the propagation of the burning front. The concomitant decrease in luminous intensity is attributable to the modest decrease in flame temperature caused by the additional inert-to-cool combustion products liberated by the polyurethane. Both linear burning rates (1.8-2.1 mm·s^{-1}) fall in the range recommended by classical pyrotechnic guidelines for large- and medium-calibre illuminating projectiles (1-2 mm·s^{-1}) [4], confirming the compatibility of the polyurethane binder with the target application.

3.4. Scaling to the M485 Torch Geometry

The laboratory-scale burning parameters can be projected to the geometry of an M485-type illuminating torch. The reference geometry considered here is a cylindrical grain of diameter D = 83 mm and height $h_t = 228$ mm, pressed at a theoretical density $\rho = 2.5$ g·cm^{-3}. The total mass of the illuminating charge is:

$$m_{torch} = \rho \times V = \rho \times S \times h_t = 2.5 \bullet 54.11 \times 22.8 = 3084 \text{ g} \approx 3.1 \text{ kg} \quad (20)$$

The burning surface at each instant is the top circular face of the cylindrical grain:

$$S = \pi \times D^2 / 4 = \pi \times (8.3)^2 / 4 = 54.11 \text{ cm}^2 \quad (21)$$

Substituting m = ρ · V into equation (15), the mass flow rate delivered by the full-scale torch is directly proportional to the burning surface, the density and the linear burning rate:

$$\dot{m}' = dm/dt = \rho \times S \times dx/dt = S \times \rho \times v_c$$
$$\dot{m}' = 54.11 \times 2.5 \times 0.184 = 24.89\ g \cdot s^{-1} \quad (22)$$

The connection between luminous intensity and mass flow rate is captured by the composition-specific luminous efficiency η_{lum} introduced in (18), which is assumed constant at the transition from the laboratory grain to the full-scale torch. This constancy has been verified above (52000 $cd \cdot s \cdot g^{-1}$ for both C3P and C5P) and is a well-established approximation for a given composition and pressing condition [4]:

$$k = \eta lum,C5P = I / \dot{m} = 112\ 950 / 2.172 = 52000\ cd \cdot (g \cdot s\text{-}1)\text{-}1 \quad (23)$$

Applying k to the full-scale mass flow rate yields the projected luminous intensity of the M485-type torch:

$$Itorch = k \times \dot{m}' = 52000 \times 24.89 = 1294000\ cd \approx 1.29 \times 106\ cd \quad (24)$$

The projected illumination time follows from equation (25):

$$ttorch = ht / vc = 228 / 1.84 = 124\ s \quad (25)$$

The total luminous energy delivered by the scaled M485 torch, from (19):

$$Elum,torch = Itorch \cdot ttorch = 1.29 \times 106 \times 124 = 1.60 \times 108\ cd \cdot s \quad (26)$$

Table 7. Projected performance of the torch

Parameter	C5P projection	M485 reference [3]	Δ [%]
Illumination time [s]	124	120	+3.3%
Luminous intensity [cd]	1.29×10^6	1.00×10^6	+29%
Total luminous energy [cd·s]	1.60×10^8	1.20×10^8	+33%
Mass flow rate [$g \cdot s^{-1}$]	24.89	n/a	-
Linear burning rate [$mm \cdot s^{-1}$]	1.84	1.90	-3.2%

As summarised in Table 7, the projected illumination time (124 s) and luminous intensity (1.29×10^6 cd) compare favourably with the reference performance of the M485 projectile (120 s and 1.0×10^6 cd) [3]. It should be noted that the scaling factor k was determined at laboratory scale, on manually pressed grains burning at atmospheric pressure, so that the absolute figures are subject to a systematic uncertainty. Even accounting for this uncertainty, however, the projection indicates that the polyurethane binder does not compromise the illuminating performance of the M485-class projectile and, in the geometry considered, delivers a moderate improvement in both illumination time and luminous intensity simultaneously.

3.5. Microstructure by Scanning Electron Microscopy

The homogeneity of the pressed pyrotechnic grain and the state of dispersion of the oxidiser and metallic-fuel particles within the polymeric matrix are the two microstructural parameters that most directly govern the ballistic reproducibility of an illuminating composition. In a well-dispersed mixture, each $Ba(NO_3)_2$ particle finds a Mg particle in its immediate neighbourhood and the mean interparticle distance is comparable in all directions and at all points of the pressed grain; local variations in the combustion front speed are then negligible, and the illuminating torch delivers a smooth, reproducible luminous output. Conversely, in a poorly dispersed mixture, oxidiser-rich and fuel-rich clusters coexist at the millimetre scale, the combustion front moves faster in the clusters and slower in the segregated regions, and the luminous intensity fluctuates in an uncontrolled manner. For this reason, the microstructural verification of dispersion and homogeneity is a mandatory validation step in the development of any illuminating composition. The microstructure of the two polyurethane-based compositions (C5P and C3P) was accordingly examined by scanning electron microscopy over a wide range of magnifications, from 30× (whole-grain overview) to 2000× (single-particle resolution). Figure 8 presents the low-to-medium-magnification comparison (30-300×), which addresses the macroscopic homogeneity of the pressed charge, while Figure 9 shows the high-magnification comparison (500-2000×), which addresses the local dispersion of the oxidiser and metallic-fuel particles within the polymer matrix.

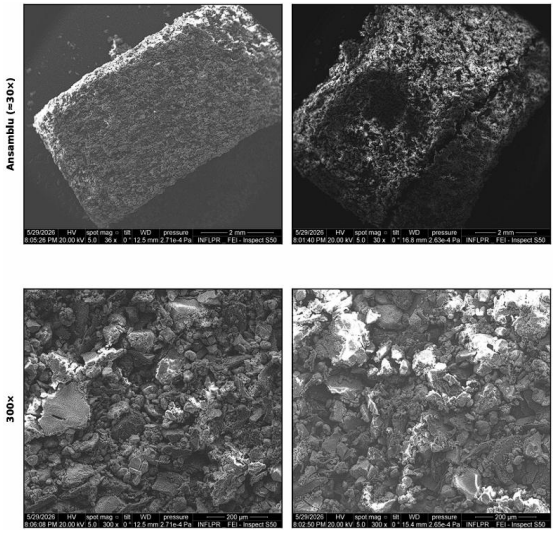


Figure 8. Comparative SEM images of the polyurethane-based compositions at low-to-medium magnification (30-300×). Left column: C5P (5 wt.% polyurethane); right column: C3P (3 wt.% polyurethane)

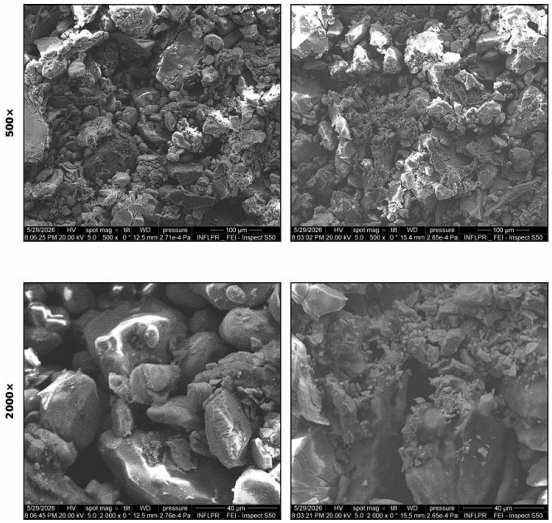


Figure 9. Comparative SEM images of the polyurethane-based compositions at high magnification (500-2000×). Left column: C5P (5 wt.% polyurethane); right column: C3P (3 wt.% polyurethane)

At low magnification (30×) both compositions display a uniform grain-scale aspect: the whole cross-section of the pressed cylinder appears homogeneous, without visible cracks, macroporosity, or segregation of the reactive components on the millimetre scale. This uniformity, which is a direct consequence of the wet mixing followed by in situ curing route employed for both formulations, confirms that the loaded charge has the same reactive composition throughout its volume and, therefore, that no significant deviation from the nominal mass fractions is to be expected in local regions of the burning front.

At medium magnification (300×) the individual particles of oxidiser and metallic fuel start to be resolved, and a clear difference between the two compositions emerges. In composition C5P (5 wt.% polyurethane), the oxidiser and magnesium particles appear individually separated by short polymeric bridges: adjacent particles are rarely in direct contact, and every particle is at least partially surrounded by polymer, so that the mixture presents itself as a fine, statistically uniform dispersion of the reactive phases in a continuous binder matrix. In composition C3P (3 wt.% polyurethane), the same particles are visibly closer to each other and frequently in direct particle-to-particle contact, with the reduced amount of binder acting only at localised contact points rather than as a continuous embedding phase. The dispersion is still uniform on average, but the mean interparticle distance is markedly smaller, and clusters of two or three touching oxidiser or magnesium particles become common.

At high magnification (2000×) the interfacial region between the reactive particles and the binder is fully resolved. In composition C5P the binder forms a continuous film

that wraps each oxidiser or magnesium particle and connects it to its neighbours; the particle contours are visibly blurred by the polymer film and the grain-to-grain contacts appear smooth. In composition C3P, the reduced amount of binder leaves the crystalline particles considerably more exposed: edges and crystallographic faces are sharply defined and a substantial fraction of the particle surface is directly accessible to the atmosphere. From the point of view of the dispersion analysis, this means that C5P offers a maximum-contact geometry between polymer and reactive phase, whereas C3P offers a maximum-contact geometry between oxidiser and fuel - a distinction that has a direct implication on the burning behaviour: the C5P grain burns in a regime in which the flame front must first decompose the polymer film before oxidiser and fuel meet, while the C3P grain burns in a regime in which oxidiser and fuel are locally already in contact and the reaction is limited only by the release of oxygen from $Ba(NO_3)_2$.

The comparison of the two microstructures also reveals a good statistical uniformity of the particle size distribution across the observed fields, without preferential agglomeration of coarse $Ba(NO_3)_2$ crystals nor separation of the finer magnesium powder in localised zones. This uniformity is the microstructural signature of the wet-mixing route employed for both compositions, which allows the ingredients to redistribute by capillary action inside the reactive slurry before the isocyanate crosslinking freezes the microstructure. Overall, both polyurethane-based grains satisfy the microstructural criteria for a well-loaded illuminating charge (macroscopic homogeneity, uniform dispersion of the reactive components, absence of large-scale segregation), and the differences observed at the microscopic scale, matrix-dominated C5P versus contact-dominated C3P, are consistent with the differences in burning-rate and impact-sensitivity behaviour reported in Sections 3.2 and 3.3.

4. Conclusions

Four illuminating pyrotechnic compositions sharing the same $Ba(NO_3)_2$/Mg oxidiser-fuel base and differing only in the type and mass fraction of the polymeric binder (iditol at 5 and 7 wt.%; HTPB/IPDI polyurethane at 3 and 5 wt.%) were designed, prepared and characterised by Hess-law thermodynamic calculations, differential thermal analysis (STANAG 4515), impact sensitivity testing (STANAG 4489), burning-rate and luminous-intensity measurements on pressed grains, and scanning electron microscopy. The main conclusions of the study are the following:

(i) At equal 5 wt.% binder content, replacing iditol by HTPB/IPDI reduces the theoretical heat of combustion by ≈7% (from 1160.7 to 1085.7 $kcal \cdot kg^{-1}$) and increases the specific gas volume by ≈10% (from 172.4 to 189.2 $L \cdot kg^{-1}$).

(ii) The DTA thermograms show that ignition is controlled by the decomposition of barium nitrate and remains, for the three compositions retaining the stoichiometric oxidiser fraction, within a narrow interval of 524.4-526.5 °C. At equal binder content the exothermic amplitude of the iditol-based composition is more than twice as large as that of the polyurethane-based composition, so that iditol behaves as a more energetic secondary fuel while the polyurethane behaves as a milder combustion moderator.

(iii) The impact sensitivity threshold is 17.17 J for both iditol-based compositions (high sensitivity, STANAG 4489) and 22.07-24.53 J for the polyurethane-based

compositions (moderate sensitivity). The substitution of iditol by HTPB/IPDI delivers a substantial safety margin gain (≈29-43%) at no cost to the ignition reliability.

(iv) The burning-rate measurements on the polyurethane-based grains give linear burning rates of 1.84-2.15 $mm \cdot s^{-1}$ and luminous intensities of 1.13-1.26 × 10^5 cd on laboratory-scale specimens. Scaling to the M485 torch geometry (D = 83 mm, h_t = 228 mm, ρ = 2.5 $g \cdot cm^{-3}$) projects an illumination time of 124 s and a luminous intensity of 1.29 × 10^6 cd, matching or exceeding the reference performance of the M485 projectile.

(v) The SEM images explain, at the microstructural level, the observed impact-sensitivity and DTA trends: at 5 wt.% polyurethane a continuous binder film coats and cushions the reactive particles, whereas at 3 wt.% polyurethane the film is discontinuous and the particles are more exposed.

Based on these results, the modern HTPB/IPDI polyurethane binder, employed at a mass fraction of 5 wt.% within a 77/18 wt.% $Ba(NO_3)_2$/Mg oxidiser-fuel base, is proposed as a rational replacement for the traditional iditol binder in the pyrotechnic torch of a 155 mm M485-type parachute-borne illuminating projectile. Future work will address the friction sensitivity (STANAG 4487), the calorimetric heat of combustion, the vacuum-stability behaviour, and the full-scale ballistic characterisation of the illuminating projectile.

Acknowledgments
Not applicable

References

1. J.A. Conkling, C.J. Mocella, Chemistry of Pyrotechnics: Basic Principles and Theory, 3rd ed., CRC Press, Boca Raton, 2019.
2. A. Nash, R. Hendershot, Battlefield illumination and the modern manoeuvre force, Journal of Defense Studies 12(3) (2018) 45-58.
3. U.S. Department of the Army, TM 43-0001-28: Army Ammunition Data Sheets - Artillery Ammunition, Washington, DC, 1994.
4. A.A. Shidlovskiy, Principles of Pyrotechnics, 3rd ed., Mashinostroyeniye, Moscow, 1964 (English translation, American Fireworks News, 1997).
5. E.C. Koch, Pyrotechnics: A Comparative Review of Formulations, Properties and Applications, Propellants, Explosives, Pyrotechnics 46(9) (2021) 1345-1370.
6. A.P. Hardt, Pyrotechnics, Pyrotechnica Publications, Post Falls, ID, 2001.
7. S. Sontakke, S. Kakade, R. Wagh, A. Dugam, P. Sane, Polymethyl Methacrylate as a Binder for Pyrotechnic Compositions, Defence Science Journal 45(4) (1995) 349-354.
8. T. Shimizu, Fireworks: The Art, Science and Technique, 3rd ed., Pyrotechnica Publications, 1996.
9. A. Cudziło, W. Pichot, Studies on the safety of pressed pyrotechnic compositions containing iditol, Central European Journal of Energetic Materials 13(1) (2016) 155-170.

10. J.P. Agrawal, High Energy Materials: Propellants, Explosives and Pyrotechnics, John Wiley & Sons, Weinheim, 2010.
11. J.C. Quagliano Amado, P.G. Ross, L. Mattos Silva Murakami, J.C. Narciso Dutra, Properties of Hydroxyl-Terminal Polybutadiene (HTPB) and Its Use as a Liner and Binder for Composite Propellants: A Review of Recent Advances, Propellants, Explosives, Pyrotechnics 47(5) (2022) e202100283.
12. S. Chaturvedi, P.N. Dave, Solid propellants: AP/HTPB composite propellants, Arabian Journal of Chemistry 12(8) (2019) 2061-2068.
13. A. Manash, P. Kumar, Comparison of burn rate and thermal decomposition of AP as oxidizer and PVC and HTPB as fuel binder based composite solid propellants, Defence Technology 15(2) (2019) 227-232.
14. STANAG 4515 (Ed. 2), Explosives, Thermal Analysis Using Differential Thermal Analysis (DTA), Differential Scanning Calorimetry (DSC), Heat Flow Calorimetry (HFC) and Thermogravimetric Analysis (TGA), NATO Standardization Office, Brussels, 2015.
15. STANAG 4489 (Ed. 1), Explosives, Impact Sensitivity Tests, NATO Standardization Office, Brussels, 1999.

DEFENSE AND SECURITY

THE ILLEGAL TRAFFICKING OF CULTURAL PROPERTY

Veliko P. Petrov

Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, veliko_pp@abv.bg

Abstract: *Combating the illicit trafficking of cultural property is a complex challenge, requiring the development and use of a variety of legal and practical instruments, created and implemented over the past fifty-six years, with the aim of regulating the art market and better controlling the movement of cultural property across borders.*

The development of a strong international legal framework is at the heart of effective transnational cooperation to combat the trafficking of cultural property in a constructive manner. Ratification of the two main international instruments, namely the 1970 UNESCO Convention and the 1995 UNIDROIT Convention, is a fundamental requirement, and States can hardly combat trafficking and hope to recover stolen objects without signing these international instruments or implementing their basic principles.

To support the work of international organisations, law enforcement authorities, public administrations and art and cultural heritage professionals, a wide range of practical tools have been developed over the past decades, particularly for police and customs services.

Keywords: *The illicit trafficking of cultural property, combating trafficking in cultural property*

БОРБА С НЕЗАКОННИЯ ТРАФИК НА КУЛТУРНИ ЦЕННОСТИ

Велико П. Петров

Културните ценности са част от общото наследство на човечеството. Те са толкова уникално и важно свидетелство за еволюцията и идентичността на народите, че значението на тяхното опазване е подчертано в редица международни инструменти. За първи път определение на понятието „културни ценности" е формулирано в чл. 1 от Хагската конвенция. Благодарение на Конвенцията този термин е въведен в международната терминология. Конвенцията определя три категории културни ценности:

- ✓ ценностите, движими или недвижими, които имат голямо значение за културното наследство на всеки народ, такива като паметниците на архитектурата, изкуствата или историята, религиозни или светски, археологически места, архитектурни ансамбли, които в качеството си на такива представляват исторически или художествен интерес, произведения на изкуствата, ръкописи, книги и други предмети от художествено, историческо или археологическо значение, а също научни колекции или важни колекции от книги, архивни материали или репродукции на ценности, посочени по-горе;
- ✓ здания, чийто главно и действително предназначение е съхраняване или експониране на движимите културни ценности, такива като музеи, големи библиотеки, хранилища на архиви, а също така скривалища, предназначени в случай на въоръжен конфликт за пазене на движимите културни ценности;

✓ центрове, в които има значително количество културни ценности (т.нар. „центрове на съсредоточаване на културни ценности")[1].

Незаконният трафик на културни ценности причинява огромни щети на културното наследство на много страни по света. В тях днес контрабандата е една от най-опасните форми на престъпна дейност. Това не е случайно, тъй като неспазването на държавните забрани и ограничения върху движението на стоки, ценности и други предмети през митническите граници подкопава техните икономики и в определени случаи представлява заплаха за обществената безопасност и здраве. Престъпното деяние контрабанда се появява след установяването на държавни и митнически граници. Незаконната търговия с културни ценности засяга културното наследство по целия свят, а приходите от нея финансират организираната престъпност, корупцията и въоръженото насилие.

Незаконният трафик на културни ценности, както и другите видове незаконен трафик, е сложен, обширен и многостранен проблем. Той може да приема различни форми, да включва множество страни и да служи на различни цели, в зависимост от географския, социално-икономическия и политическия контекст. Сложността на проблема затруднява неговото дефиниране и анализ, а научните трудове по темата остават оскъдни. Ограничените знания, които са широко достъпни за настоящите тенденции в незаконния трафик на произведения на изкуството и антики, са една от пречките за ефективното противодействие на тази специфична незаконна търговия.

Незаконният трафик на културни ценности се различава от другите видове трафик поради съществуването на легален пазар на културни ценности. За разлика от други незаконни стоки, които са обект на трафик, определението за незаконен трафик на културни ценности не зависи от естеството на стоката, която е обект на трафик, а по-скоро от естеството на собствеността върху културния обект. По този начин законността на собствеността маркира границата между това, което понякога се нарича „незаконни" и „законни" културни ценности.

Въпреки че спецификите могат да варират в зависимост от разпоредбите на националното законодателство, повечето от съществуващите културни ценности имат законен собственик (или собственици) с правата да притежават, използват и прехвърлят тези ценности. Това правило се прилага и за неизкопани археологически обекти, които автоматично принадлежат на собственика на подземната зона, в която се намира археологическият обект. В много, ако не и в повечето случаи, що се отнася до националното законодателство, това би била държавата.

Стотици международни и национални правни инструменти защитават собствеността върху културни ценности от кражба, незаконен износ или незаконно придобиване по целия свят. Освен това, мобилността на културните ценности се регулира от набор от национални и международни практики, принципи, професионални стандарти и закони относно прехвърлянето на собствеността върху

[1] Чл. 1 от Хагската конвенция от 14 май 1954 г. „За защита на културните ценности в случай на въоръжен конфликт"

културни ценности от една ръка на друга: покупка, поемане на ипотечен дълг, замяна, заеми, дарение или завещание.

Незаконният трафик на културни ценности обикновено се разбира като следствие от нарушения на тези национални или международни правни инструменти. Следователно терминът „незаконен трафик на културни ценности" може да обхваща широк спектър от практики, в зависимост от действащото национално и международно законодателство:

- ✓ кражби от музеи, паметници, религиозни обекти и други обществени или частни места за опазване на културата;
- ✓ незаконни разкопки на археологически обекти, включително подводни разкопки;
- ✓ премахване на културни ценности по време на въоръжени конфликти или военна окупация;
- ✓ незаконен износ и внос на културни ценности;
- ✓ незаконно прехвърляне на собственост върху културни ценности (продажба, покупка, поемане на ипотечен дълг, замяна, дарение или завещание);
- ✓ производство, търговия и използване на фалшифицирана документация;
- ✓ трафик на фалшиви или подправени културни ценности.

През 2020 г. Интерпол отчете в световен мащаб над 850 000 иззети артефакта, като над половината от тях са иззети в Европа[2]. От 2016 г. насам, в резултат на ежегодната световна операция „Пандора", са били извършени 407 задържания и са били възстановени 147 050 културни ценности[3]. Зад посочените данни се крие по-широкообхватен проблем - имайки предвид големия брой неразкрити случаи, реалният мащаб на незаконната търговия с културни ценности вероятно е много по-голям[4] .

Контрабандата на културни ценности се появява по-късно, във връзка с развитието на самосъзнанието и признаването на особено значими предмети като културни обекти. Трябва да се отбележи, че през вековната си история контрабандата на културни ценности се е усъвършенствала, тъй като системата ѝ на извършване се е развивала професионално.

Терминът „*контрабанда*" се отнася до митническа измама, включваща движението на стоки през митническа граница по какъвто и да е прикрит начин. Това определение е дадено в Международната конвенция за взаимопомощ в областта на предотвратяването, разследването и потушаването на митнически нарушения (позната като Найробийска конвенция) е многостранен международен

[2] Интерпол, Assessing Crimes Against Cultural Property 2020, report (Оценка на престъпленията срещу културни ценности 2020 г., доклад).

[3] Оперативна част от Европейската мултидисциплинарна платформа за борба с криминални заплахи (EMPACT).

[4] Европейска комисия, Illicit trade in cultural goods in Europe — Characteristics, criminal justice responses and an analysis of the applicability of technologies in the combat against the trade (Незаконната търговия с културни ценности в Европа — характеристики, реакции на наказателното правосъдие и анализ на приложимостта на технологиите в борбата с тази търговия), окончателен доклад, 2019 г., страници 81, 159, 160.

договор, приет на 9 юни 1977 г. в Найроби, Кения, под егидата на Съвета за митническо сътрудничество (днес Световна митническа организация).

Проучване на практиките на правоприлагането показва, че специализирани престъпни групи действат в незаконния трафик на културни ценности, действайки със строго разделение на престъпния труд по следната схема: *поръчка – кражба – доставка до границата – контрабанда – доставка до клиента*. Тези действия се извършват в условия на дълбока секретност и чрез използване на корупционни връзки от двете страни на границата.

Според международните класификации, контрабандата на културни ценности е третата най-печеливша незаконна търговия в света, веднага след наркотиците и оръжията. Социалната опасност от контрабандата се изразява и в това, че тя служи като основен канал за изтичане на национални културни съкровища и уникални произведения на изкуството с голяма историческа и мемориална стойност в чужбина. Освен това, заслужава да се отбележи съществуващият корупционен фактор като необходим компонент на престъпленията, свързани с контрабандата на културни ценности.

Най-често контрабандните предмети включват произведения на изкуството, икони, предмети на религиозно и декоративно изкуство, ръкописни старопечатни и редки книги, филателни материали, нумизматика и други. Културните ценности са незаменим материален и нематериален културен обект и произведение, което има художествена и материална стойност, универсално значение, а също така оказва естетическо, научно и историческо въздействие върху хората.

Незаконният трафик на културни ценности се счита за една от най-печелившите дейности на транснационалните престъпни организации. Престъпните схеми и методи за незаконно движение на културни ценности непрекъснато се развиват и често имат международно измерение.

Има две основни категории предмети, търсени от организираните престъпни групи:

1) Артефакти и ценни антики, съхранявани в музеи, религиозни сгради, галерии и частни колекции;

2) Находки с културна стойност, открити по време на археологически разкопки, както и военни принадлежности.

Трафикът на културни ценности представлява незаконният внос, износ и прехвърляне на собственост върху културни ценности (предмети от значение за археологията, праисторията, историята, литературата, изкуството или науката). Той може да е под различни форми, например:

- ✓ кражба от институции за културно наследство или частни колекции;
- ✓ разграбване на археологически обекти;
- ✓ преместване на артефакти поради война.

Трите основни незаконни дейности, свързани с незаконната търговия на културни ценности, са:

1) кражба и грабеж;

2) плячкосване (незаконно премахване на древни реликви от археологически обекти, сгради или паметници[5]);

3) фалшифициране на културни ценности.

Свързаните с тях престъпления включват измама, разпореждане с откраднати ценности (укриване), контрабанда или корупция. Отвъд трафика престъпниците могат да злоупотребяват дори със законно придобити културни ценности с цел изпиране на пари, избягване на санкции, данъчни измами или финансиране на тероризъм. Тези престъпления не само унищожават съществена част от историческите знания за бъдещите поколения, но са и силно свързани с потисничество и преследване в определени общества и са признати за военно престъпление от Международния наказателен съд.

Политическата нестабилност и въоръжените конфликти в някои райони на света създават печеливша среда за отделни престъпници и организирани групи, желаещи да унищожат съществена част от наследството на своя народ. Освен това, незаконният трафик на културни ценности от конфликтни зони, особено от Близкия изток, е свързван в няколко случая с финансирането на терористична дейност.

Друг основен аспект на това сложно престъпление е активното участие на организирани престъпни групи. Тяхното участие представлява огромна заплаха за обществената сигурност, тъй като тези групи често са отговорни за кражба, плячкосване, преместване и продажба на незаконно придобити предмети. Културните ценности в повечето случаи се изнасят незаконно от една държава в друга чрез установени престъпни мрежи и работата на посредници. Докато множество аналитични доклади, изготвени от Интерпол, подчертават как незаконният трафик на културни ценности е глобално явление, начинът на действие на организираните престъпни групи варира в различните региони. Тези групи действат въз основа на пазарното търсене във всеки регион и фокусират усилията си върху определени категории обекти въз основа на това, което купувачите в този географски район изискват.

Освен това, по целия свят, особено в конфликтни зони, се извършват безброй незаконни разкопки, което води до контрабанда на голямо количество предмети с помощта на престъпни мрежи и съвременни технологии. Организирани групи след това преместват тези предмети през няколко различни пазара, варирващи от онлайн платформи до аукционни къщи. В този контекст незаконният трафик на културни ценности се използва и като основно средство за пране на пари.

Престъпленията, свързани с културни ценности, имат *специфични характеристики*, които ги отличават от другите незаконни дейности:

На *първо място*, идентичността, автентичността, принадлежността[6], произходът и правният статут на културните ценности рядко се виждат от пръв

[5] Включително заграбване, т.е. плячкосване по време на война, което се счита за военно престъпление в обичайното международно хуманитарно право.

[6] Местоположението на предмет към датата на археологическото му откриване

поглед и често е необходимо да бъдат установени чрез специфично техническо експертно мнение;

На *второ място*, публичните и частните колекции, паметниците на културата и обектите за разкопки са уязвими на кражби и грабежи, особено в ситуации на конфликти и кризисни ситуации. Освен това, след като бъдат въвлечени в трафик, нерегистрираните културни ценности, особено от обекти за разкопки или некаталогизирани колекции, стават трудни за откриване и проследяване;

На *трето място*, пазарът на културни ценности се характеризира с определени уязвимости, които го правят привлекателен за престъпниците. Сред тези уязвимости са приемането на анонимност и поверителност, субективността и променливостта по отношение на цените, както и възможността за използване на артикули за съхранение и преместване на значителни суми пари. Престъпниците също така се възползват и от общата липса на осведоменост относно вредата, която може да причини трафикът на културни ценности[7].

Освен това престъпниците се възползват от голямата наличност на канали за онлайн продажби, за да разширят своята база от клиенти на законните и незаконните пазари. Това създава допълнителни предизвикателства за правоприлагащите органи[8] поради обема на културните ценности, които трябва да бъдат проверени, криптирането на данни и броя на потенциално засегнатите юрисдикции. Освен това, в сравнение с други видове организирани престъпления срещу собствеността, при организираните престъпни групи, участващи в трафик на културни ценности, правоприлагащите органи наблюдават по-голяма усложненост. Престъпниците умишлено извършват трансгранична дейност, за да увеличат печалбите си, да заличат следите си, да се скрият от задържане и да фалшифицират произхода или принадлежността на културни ценности, станали обект на трафик.

На фигура 1 са изразени приблизителните маршрути, използвани за незаконен трафик на културни ценности от една държава или континент на друг. Един ясен момент, който се вижда от фигура 1, е , че всеки регион на света е засегнат от незаконния трафик на културни ценности, което за пореден път потвърждава крайния транснационален характер на тези престъпления. Държавите или континентите биха могли да бъдат едновременно зони на произход, транзит и местоназначение за откраднати предмети.

[7] TRACFIN (Traitement du renseignement et action contre les circuits financiers clandestins), La lettre d'information de TRACFIN, номер 16, юни 2018 г., относно уязвимостта на пазара на произведения на изкуството на изпиране на пари и финансиране на тероризма.

[8] терминът „правоприлагащи органи“ се отнася до полицейските служби, митниците, граничния контрол и други съответни органи, изпълняващи задачи за предотвратяване, разследване, разкриване или наказателно преследване на престъпления.



Фиг. 1: Основни международни контрабандни маршрути на културни ценности (четирите региона са показани в различни цветове)[9].

Трите най-често срещани метода, използвани от престъпниците за улесняване на незаконния трафик на културни ценности по света, са:

- ✓ скриване на културни ценности в багажа на пътниците;
- ✓ транспорт с фалшифицирани документи;
- ✓ скриване на културни ценности в други обекти.

Днес въпросите за предотвратяване на незаконния износ на културни ценности в чужбина, локализирането и връщането на изгубени ценности и осигуряването на тяхната защита и законно движение през границите са по-належащи от всякога.

Един от ключовите компоненти на междудържавното сътрудничество в областта на незаконния трафик на културни ценности е институционалният механизъм, който предвижда създаването на специализирани органи, които улесняват разработването на законодателни препоръки и съвместни програми за борба с разпространението и незаконната търговия с културни ценности и произведения на изкуството.

Институционално работата за борба с незаконния трафик на културни ценности се провежда в рамките на специализирани органи на Организацията на обединените нации. Една такава универсална международна организация, която разглежда широк кръг от въпроси, свързани с международното културно и научно сътрудничество, включително незаконния трафик на културни ценности, е ЮНЕСКО. На своята 40-та Генерална конференция през 2019 г. ЮНЕСКО обяви 14 ноември за Международен ден за борба с незаконния трафик на културни

[9] Interpol, Assessing Crimes Against Cultural Property 2020, report, p 21

ценности, като привлече по-голямо внимание към това престъпление и начините за борба с него и подчерта значението на международното сътрудничество и активните мерки в рамките на Конвенцията за мерките за забрана и предотвратяване на незаконния внос, износ и прехвърляне на собствеността върху културни ценности (1970 г.), която осигурява международна рамка за предотвратяване на кражби и грабежи и връщане на откраднати културни ценности, наред с други постижения в борбата с незаконния трафик.

На 14 ноември 1970 г. ЮНЕСКО приема Конвенцията за мерките за забрана и предотвратяване на незаконния внос, износ и прехвърляне на собственост върху културни ценности, която беше първият международен договор в борбата срещу незаконния трафик на културни ценности. Със 137 държави-страни и широко признати действия в борбата срещу незаконния трафик на културни ценности, нейният обхват вече е универсален. Член 2 от Конвенцията на ЮНЕСКО от 1970 г. формулира основната идея, че всяка държава е задължена да защитава културните ценности от кражба, тайни разкопки и незаконен износ, и че защитата на националното културно наследство изисква тясно сътрудничество между държавите. Член 3 от Конвенцията постановява, че вносът, износът и прехвърлянето на собственост върху културни ценности, извършени в нарушение на разпоредбите, приети от държавите-страни по Конвенцията, се считат за незаконни. Освен това, член 11 гласи, че „износът и прехвърлянето на собственост върху културни ценности, произтичащи пряко или косвено от окупацията на страната от чужда сила, също се считат за незаконни". За да ограничат износа, държавите-страни по Конвенцията са се ангажирали да установят специален сертификат, с който държавата износител удостоверява, че е разрешила износа. Член 13 от Конвенцията предвижда неотменимото право на всяка държава „да обяви определени културни ценности за неотменими, които следователно не могат да бъдат изнасяни".

Конвенцията предвижда редица мерки за борба с незаконното прехвърляне на собственост. *Първо*, държавите-страни по конвенцията се задължават да ограничат чрез обучение, информация и бдителност прехвърлянето на културни ценности, незаконно изнесени от която и да е държава-страна. *Второ*, в зависимост от обстоятелствата във всяка държава, антикварите (т.е. лицата, които обикновено най-често придобиват културни ценности) трябва да бъдат задължени, под страх от наказателна отговорност, да поддържат специален регистър на покупките, посочващ произхода на всяка културна ценност, името и адреса на доставчика, описанието и цената на всеки продаден артикул, и да информират купувачите за всяка евентуална забрана за износ на такива ценности. *Трето*, държавите-страни по конвенцията се задължават, в съответствие със своето законодателство, да „предотвратяват с всички подходящи средства прехвърлянето на собствеността на културни ценности, което улеснява незаконния внос или износ на такива ценности". *Четвърто*, участващите държави се задължават да налагат наказателни или административни санкции на всички лица, отговорни за нарушаване на забраните за износ на културни ценности, които не са придружени от сертификат, или за внос на ценности, откраднати от музеи или други подобни институции.

На 24 юни 1995 г. на Дипломатическата конференция в Рим е приета Конвенцията на Международният институт за унифициране на частното право (UNIDROIT) за откраднати или незаконно изнесени културни ценности. Конвенцията на UNIDROIT от 1995 г. за откраднати или незаконно изнесени културни ценности е една от международните конвенции за борба с незаконния трафик на културни ценности. Документът позволява да се прилагат принципите, залегнали в Конвенцията на ЮНЕСКО за средствата за забрана и предотвратяване на незаконния внос, износ и прехвърляне на собственост върху културни ценности (1970 г.), по която България е страна.

Конвенцията на ЮНЕСКО от 1970 г. се прилага както за предотвратяване на незаконния трафик на културни ценности, така и за връщането на културни ценности, а Конвенцията на UNIDROIT за откраднати или незаконно изнесени културни ценности, приета 25 години по-късно (Рим, 24 юни 1995 г.), се фокусира изключително върху процеса на връщане. Тя се прилага за международни искове за възстановяване на откраднати културни ценности и връщане на незаконно изнесени културни ценности. Тя се придържа към общото определение за културни ценности, дадено в Конвенцията на ЮНЕСКО. Трябва да се отбележи, че тези две конвенции предвиждат задължението на държавите членки да установят процедура, основана на разрешителни, за износ на културни ценности. Повечето държави са хармонизирали законодателството си за износ с разпоредбите на тези международноправни договори.

По този начин културният обмен винаги е бил от голямо значение за всички държави. В идеалния случай националното и международното законодателство, свързано с тази сфера, трябва да се стреми към постигане на оптимален баланс между необходимостта от защита на наследството, зачитане на правата на собственост и насърчаване на развитието на пазара на изкуство. Трябва да се отбележи обаче, че намирането на правилния път през лабиринта от правни термини и разпоредби не винаги е лесно.

На 06.01.2024 г. Общото събрание на Организацията на обединените нации, подкрепено от повече от 140 държави, прие резолюция (A/79/231) за укрепване на Конвенцията на ЮНЕСКО. Резолюцията е опит да се призове държавите членки да приложат национални и международни мерки за борба с незаконния трафик на културни ценности, да въведат обучение за полицейските сили, митническите и граничните служби и да създадат специализирани полицейски звена, които са посветени изключително на защитата на културното наследство.

Международните организации играят ключова роля за повишаване на осведомеността, популяризиране на правните инструменти, разработването на практически инструменти, обучението на специалисти и засилването на международното сътрудничество. **Икономическият и социален съвет на Организацията на обединените нации** (ECOSOC) официално признава международна група експерти, съставена от шест организации, които работят в тясно сътрудничество, за да обединят експертния си опит в областта:

- ✓ Международният съвет на музеите (ICOM);
- ✓ Международната организация на криминалната полиция (INTERPOL);

- ✓ Международният институт за унифициране на частното право (UNIDROIT);
- ✓ Организацията на обединените нации за образование, наука и култура (UNESCO);
- ✓ Службата на ООН по наркотиците и престъпността (UNODC);
- ✓ Световната митническа организация (WCO).

Тази международна група от водещи експерти, заедно с други неправителствени организации и междуправителствени организации, участват в международните усилия за спиране на незаконния трафик на културни ценности. При работа с транснационални престъпници, които отлично знаят как да се възползват от правните и оперативните пропуски, международното сътрудничество е съществен елемент в следните области: стандартизация на практиките и правните рамки, обмен на информация, контрол върху транспортирането на културни ценности, съвместни разследвания, наказателни преследвания, диалог за връщане или реституция на откраднати или ограбени културни ценности и др.

Предвид трудността за постигане на силен международен правен консенсус по въпроса, броят на двустранните и многостранните споразумения нараства през последните няколко години. Европейският съюз е отличен пример за ситуация, в която необходимостта от обща рамка за контрол и статута на чуждестранните културни ценности в рамките на общия пазар принуди институциите на ЕС да се справят с проблема и в крайна сметка да преработят Директива 93/7/ЕИО на Съвета относно връщането на културни ценности, незаконно изнесени от територията на държава членка. На двустранно ниво е постигнат голям напредък от страни като Съединените щати или Швейцария в подписването на двустранни споразумения с държави, които са особено изложени на риск от плячкосване на археологически ценности. Такива двустранни споразумения често напълно забраняват вноса на определени категории културни обекти без надлежна документация и установяват специфична рамка за връщането или реституцията на тези обекти в страната им на произход.

На национално ниво много изисквания всъщност зависят от добрата воля на правителствата. Ратифицирането и прилагането на международни правни инструменти е първото от тях и предполага подобряване на националното законодателство, особено в следните области:

- ✓ определение за национална културна ценност;
- ✓ правни изисквания за внос, износ и прехвърляне на собственост върху културни ценности (сертификати за износ, регистри за търговци на произведения на изкуството и антики и др.);
- ✓ определяне и прилагане на строги процедури за надлежна проверка при придобиването на културни ценности;
- ✓ установяване на санкции в случай на нарушение на националното законодателство;
- ✓ транспониране на правилата за професионална етика в националното законодателство.

На по-практическо ниво, държавните администрации са силно насърчавани да предприемат следните мерки:

- ✓ създаване на една или повече национални служби за опазване на културното наследство;
- ✓ създаване и актуализиране на национални инвентаризации;
- ✓ развитие на институции за опазване на околната среда;
- ✓ надзор на археологическите разкопки и насърчаване на свързаните с тях научни изследвания;
- ✓ установяване на етични правила за професионалистите в областта на изкуството и културното наследство, включително пазара на изкуството;
- ✓ повишаване на обществената осведоменост.

Създаването на национални служби за защита на културното наследство е едно от първите изисквания на Конвенцията от 1970 г. За правителствата, желаещи да контролират по-добре търговията и движението на културни ценности, най-доброто стратегическо решение вероятно е създаването на специално полицейско звено, посветено на културното наследство. В много страни, като Италия, САЩ, Франция или Испания, подобни специализирани звена значително са подобрили капацитета и експертизата на страната в борбата с трафика.

Изводи:

1. Борбата с незаконния трафик на културни ценности представлява сложно предизвикателство, изискващо разработването и използването на разнообразни правни и практически инструменти, създадени и внедрени през последните петдесет и шест години, с цел регулиране на пазара на изкуство и по-добър контрол върху движението на културни ценности през границите.

2. Разработването на силна международно-правна основа е в основата на ефективното транснационално сътрудничество за конструктивна борба срещу трафика на културни ценности. Ратифицирането на двата основни международни инструмента, а именно Конвенцията на ЮНЕСКО от 1970 г. и Конвенцията на УНИДРУА от 1995 г., е основно изискване и държавите трудно могат да се борят с трафика и да се надяват на възстановяване на откраднати вещи, без да подпишат тези международни инструменти или да приложат техните основни принципи.

3. В подкрепа на работата на международните организации, правоприлагащите органи, държавните администрации и специалистите по изкуство и културно наследство, през последните десетилетия е разработен широк набор от практически инструменти, особено за полицейските и митническите служби.

Използвана литература:

1. European Commission, Illicit trade in cultural goods in Europe - Characteristics, criminal justice responses and analysis of the applicability of technologies in combating the trade, Final Report, 2019, p. 276, ISBN 978-92-79-99359-6

2. Interpol, Assessing Crimes Against Cultural Property 2020, report, https://www.interpol.int/content/download/16751/file/2020%20Assessing%20Crimes%25
3. Gecosala, Ma. Andrea Nicole, "The Illicit Trafficking of Cultural Property: Are the Existing International Legal Framework and Enforcement Mechanisms No More Than Glorified Placeholders for the Real Actors?" (2024). Student Works. 1432., https://scholarship.shu.edu/ student_scholarship/1432
4. Съобщение на комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите относно плана за действие на ЕС за борба с трафика на културни ценности, Брюксел, 13.12.2022 г. COM(2022) 800 final
5. Хагската конвенция от 14 май 1954 г. „За защита на културните ценности в случай на въоръжен конфликт“
6. Конвенция на ЮНЕСКО за мерките, насочени към забрана и предотвратяване на незаконен внос, износ и прехвърляне на правото на собственост на културни ценности, Париж, 14 ноември 1970 г.
7. Конвенция на Международния институт за унифициране на частното право (UNIDROIT/УНИДРОА) за откраднати или незаконно изнесени културни ценности, Рим, 24 юни 1995 г.
8. Съобщение на комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите относно стратегията на ЕС за борба с организираната престъпност за периода 2021—2025 г., Брюксел, 14.4.2021 г. COM(2021) 170 final
9. Конвенция на ЮНЕСКО от 1970 г. „За мерки, насочени към забрана и предотвратяване на незаконния внос, износ и прехвърляне на права на собственост върху културни ценности“
10. Interpol, Stolen Works of Art Database, https://www.Interpol .int/en/Crimes/Cultural-heritage-crime/Stolen-Works-of-Art-Database#:~:text=The%20Stolen%20Works%20of%20Art,and%20missing%20objects%20of%20art
11. Interpol, How we fight cultural heritage crime, https://www.interpol .int/en/Crimes/Cultural-heritage-crime/How-we-fight-cultural-heritage - crime

DEFINITION OF THE CONCEPT OF "CULTURAL VALUE" IN INTERNATIONAL DOCUMENTS

Veliko P. Petrov

Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, veliko_pp@abv.bg

***Abstract**: A single, universal definition of “cultural property” has not yet been developed. There is no uniform interpretation of the term “cultural property” both internationally and nationally. The debate continues over the existing definitions and characteristics of cultural property. The terms “cultural heritage” and “cultural value” are used in texts, sometimes in the same document, sometimes interchangeably. The terms “cultural property” and “monuments” can also be used as equivalents. In fact, cultural property, as an object of international protection, is divided into two groups: cultural property under the 1954 Hague Convention and World Heritage Sites under the 1972 UNESCO Convention.*

Since the 1980s, a process of redefining the concept of “cultural property” has begun: the European interpretation, supported by international cultural preservation organizations, has been denigrated as the only acceptable approach to the protection of cultural heritage since the mid-20th and early 21st centuries.

The cultural heritage of the countries of the Far East, Southeast Asia and other countries, unlike European countries, does not consist of specific works of art or architectural structures, but primarily in artistic traditions, national arts and crafts. The main idea is to preserve the national identity of the objects and the symbols they contain, symbols important for society's understanding of the future. This is the cultural value of these objects, their true spiritual content. It is necessary to note that despite more than a century of use of the concept of "cultural values", neither the European nor the conventionally called "Asian" sphere of cultural heritage protection has a clear understanding of the concept of "cultural values". There are also no precise, universal criteria by which certain objects or phenomena can be classified as cultural values.

***Keywords:** definition of "cultural property", cultural heritage, cultural value, international documents*

ДЕФИНИРАНЕ НА ПОНЯТИЕТО „КУЛТУРНА ЦЕННОСТ“ В МЕЖДУНАРОДНИТЕ ДОКУМЕНТИ

Велико П. Петров

Почти всички статии и книги, разглеждащи проблемите около термина „културни ценности“, задължително споменават трудностите при разработването на точно определение на това понятие, както и очертават основните етапи в появата и употребата на термина. Липсва единно тълкуване на термина „културни ценности“ както в международен, така и в национален план. Продължава дебатът относно съществуващите определения и характеристики на културните ценности.

Днес търсенето на най-оптималната формулировка на понятието „културна ценност“ остава актуално. Изследователите разглеждат съвкупността от културни ценности на даден народ или общество, както като критерий за социална

приемственост през поколенията, така и като културно наследство като цяло. Този доклад е опит да се разгледат културните ценности в единството на техните съдържателни и процесуални характеристики, с цел конкретизиране и обогатяване на самото понятие.

Понятието „културна ценност“ е неразривно свързано с културното наследство и се среща почти във всяко определение. В най-общия си вид културното наследство е съвкупността от обекти в света около нас, разпознати като културни ценности, основани на културния опит и предпочитания на човечеството. Понятието „културни ценности“ обикновено се използва за обозначаване на обекти от материалния и духовния свят, които имат културно значение във възприятието на обществото. Различни автори акцентират върху историческата, художествената, естетическата и научната стойност на културните обекти и явления.

Културните ценности са неразделна част от наследството на всеки народ. Обхватът на обектите, свързани с културните ценности, е широк и разнообразен. Те се различават по характера на произхода, по формата на въплъщение, по значението, което представляват за социалното развитие, и други критерии. Всички тези различия се отразяват и в правното регулиране на културните ценности.

Класификацията според социално-правните характеристики позволява да се разграничат културните ценности на духовни и материални, движими и недвижими; класификация по стойност - на ценности с общочовешко, държавно и местно значение; класификация според формата на собственост - на ценности, които са във държавна, общинска и частна собственост; класификация по предназначение - на ценности, които поради своите качествени характеристики трябва да се използват предимно за научно-изследователски цели, както и за културно-образователни и възпитателни цели[10].

Военните конфликти са послужили като предпоставка за развитието на правната защита на културните ценности. В тази връзка през 20-ти век са разработени международни правни актове, регулиращи защитата на културните ценности. Така идеята за културното наследство на цялото човечество е залегнала в Хагската конвенция от 14 май 1954 г.[11] Терминът „културни ценности“ обхваща както нематериални, така и материални обекти на културата. Освен това, този термин отразява двойствения характер на тези обекти, които едновременно се признават за обекти на права върху собственост и обекти на културното наследство.

Въпреки факта, че всяка държава има свое национално определение на понятието „*културна ценност*“, съществуващите международноправни актове и научна доктрина използват предимно два термина - „културно наследство“ и „културна собственост“, които отразяват различни правни и социални концепции.

[10] Михайлова, Т. Б., Экспертиза культурных ценностей: учебно-методическое пособие, Изд-во Урал. 2020, с.156, ISBN 978-5-7996-3108-6, стр.23.

[11] Хагската конвенция от 14 май 1954 г. „За защита на културните ценности в случай на въоръжен конфликт“

За първи път определението на понятието „културни ценности“ е формулирано в чл. 1 от Хагската конвенция. Благодарение на Конвенцията този термин е въведен в международната терминология. Конвенцията определя три категории културни ценности:

ценностите, движими или недвижими, които имат голямо значение за културното наследство на всеки народ, такива като паметниците на архитектурата, изкуствата или историята, религиозни или светски, археологически места, архитектурни ансамбли, които в качеството си на такива представляват исторически или художествен интерес, произведения на изкуствата, ръкописи, книги и други предмети от художествено, историческо или археологическо значение, а също научни колекции или важни колекции от книги, архивни материали или репродукции на ценности, посочени по-горе;

- ✓ здания, чийто главно и действително предназначение е съхраняване или експониране на движимите културни ценности, такива като музеи, големи библиотеки, хранилища на архиви, а също така скривалища, предназначени в случай на въоръжен конфликт за пазене на движимите културни ценности, посочени в точка "а";
- ✓ центрове, в които има значително количество културни ценности (т.нар. „центрове на съсредоточаване на културни ценности“)[12].

Наред с Хагската конвенция от 1954 г., определението на понятието „културни ценности“ е дадено в Препоръката на ЮНЕСКО от 1964 г. относно мерките за забрана и предотвратяване на незаконния износ, внос и прехвърляне на собствеността върху културни ценности. От гледна точка на тази Препоръка, „движимо и недвижимо имущество, което е от голямо значение за културното наследство на всяка страна, като например произведения на изкуството и архитектурата, ръкописи, книги и други предмети от интерес от гледна точка на изкуството, историята или археологията, етноложки документи, типични образци на флората и фауната, научни колекции и важни колекции от книги и архивни документи, включително музикални архиви, се считат за културни ценности“[13].

В международните правни документи терминът „културна ценност“ се среща в две значения. *Първо*, като обозначение за материални и нематериални обекти (Вашингтонска харта 1987 г.[14]) – обекти, движими и недвижими паметници, т.е. елементи на културното наследство. Второто значение е качествен показател за важността, значението и стойността на даден елемент от културното наследство.

[12] Чл. 1 от Хагската конвенция от 14 май 1954 г. „За защита на културните ценности в случай на въоръжен конфликт“

[13] Препоръка относно мерки, насочени към забрана и предотвратяване на незаконния износ, внос и прехвърляне на собственост върху културни ценности. Приета от Генералната конференция на ООН за образование, наука и култура на тринадесетата ѝ сесия в Париж на 19 ноември 1964 г.

[14] Вашингтонската харта, приета през 1987 г. от Международния съвет за паметници и забележителности (ИКОМОС), е фундаментален международен документ за опазване на културното наследство.

Терминът „културна ценност" е използван впоследствие в следващите документи, но формулировката или описанията на съдържанието на термина може да варират значително. Терминът е използван и в двете значения.

1) декември 1960 г. Генералната конференция на ЮНЕСКО, определя „...съвкупност от елементи, представляващи културна стойност: колекции от изкуство, история, наука и технологии, ботанически и зоологически градини, аквариуми."[15]

2) През ноември 1964 г. на в Париж Генералната конференция на ЮНЕСКО, определя „Културните ценности са движими и недвижими вещи от голямо значение за културното наследство на всяка страна, като например произведения на изкуството и архитектурата, ръкописи, книги и други предмети с художествен, исторически или археологически интерес, етноложки документи, типични образци на флората и фауната, научни колекции и важни колекции от книги и архивни документи, включително музикални архиви"[16].

3) През ноември 1968 г на Генералната конференция на ЮНЕСКО, определя „Културни ценности" са:

(a) недвижими обекти, като например места с археологически, исторически или научен интерес, сгради или други обекти с историческа, научна, художествена или архитектурна стойност, независимо дали са религиозни или светски, включително традиционни архитектурни ансамбли, исторически квартали в градове или села и етноложки сгради на предишни култури, все още в добро състояние. Това се отнася за такива недвижими обекти като руини, запазени на повърхността на земята, както и археологически или исторически останки, открити в земята. Терминът „културни ценности" включва и непосредствената им околност;

(b) движими ценности с културно значение, включително имущество, съдържащо се в или извадено от недвижими имоти, както и движими ценности, заровени в земята, които могат да бъдат открити в места с археологически или исторически интерес или другаде. Терминът „културни ценности" се отнася не само до идентифицирани и регистрирани архитектурни, археологически и исторически обекти и институции, но и до нерегистрирани останки от миналото, както и до съвременни обекти и структури.

През 1978 г., на своята двадесета сесия, Генералната конференция на ООН формулира концепцията за „движими културни ценности"[17] и установи:

а) „*движими културни ценности*" означава всички движими ценности, които са израз или доказателство за човешкото творчество или еволюцията на природата и

[15] Препоръка относно най-ефективните мерки за осигуряване на достъпност на музеите за всички, приета от Генералната конференция на ЮНЕСКО на 14 декември 1960 г., параграф 1

[16] Препоръка относно средствата за забрана и предотвратяване на незаконния износ, внос и прехвърляне на собственост върху културни ценности. (Приета от Генералната конференция на ЮНЕСКО на нейната 12-та сесия. Париж, 19 ноември 1964 г., част I)

[17] Препоръка относно защитата на движимите културни ценности. Приета от Генералната конференция на ООН за образование, наука и култура на двадесетата сесия в Париж на 28 ноември 1978 г.

които имат стойност от археологическа, историческа, художествена, научна или техническа гледна точка, по-специално следните категории обекти:

- ✓ находки в резултат на наземни и подводни археологически проучвания и разкопки;
- ✓ антики, като инструменти, керамика, надписи, монети, печати, бижута, оръжия и погребални предмети, по-специално мумии;
- ✓ елементи от исторически паметници, които са претърпели разчленяване;
- ✓ антропологични и етноложки материали;
- ✓ исторически ценности, включително тези, свързани с историята, както и с живота на народите и националните лидери, мислители, учени и художници, и важни национални събития;
- ✓ художествени ценности, като:

– произведения на живописта и изцяло ръчно изработени на всякаква основа и от всякакви материали (с изключение на рисунки и промишлени продукти, декорирани на ръка);

– оригинални щампи, плакати и фотографиите като видове оригинално творчество;

– оригинални произведения на изкуството и монтажи от всякакви материали;

– скулптурни произведения от всякакви материали;

– произведения на приложното изкуство, изработени от материали като стъкло, керамика, метал, дърво и др.;

- ✓ ръкописи и инкунабули, книги, документи или публикации от особен интерес;
- ✓ предмети от интерес от гледна точка на нумизматиката (медали и монети) или филателията;
- ✓ архивни документи, включително текстови записи, карти и други картографски материали, фотографии, филми, звукозаписи и машиночетими документи;
- ✓ мебели, гоблени, костюми и музикални инструменти;
- ✓ зоологически, ботанически и геоложки образци.

Двете конвенции на ЮНЕСКО от 1970 г. („За мерки, насочени към забрана и предотвратяване на незаконния внос, износ и прехвърляне на права на собственост върху културни ценности“) и 1972 г. („За защита на световното културно и природно наследство“) определят няколко основни признака, чрез които даден обект, който е обект на международно-правно регулиране, може да бъде класифициран като „културни ценности“:

1) универсално значение за световната култура като цяло;

2) незаменимост (невъзможност за създаване на абсолютно идентичен образец);

3) уникалност (естетическото послание, което носи в себе си предмета);

4) времеви критерий (културните ценности включват онези обекти на материалния свят, които са създадени в повечето случаи преди повече от 100 (50) години);

5) стойност в еквивалентен израз (културните ценности подлежат на

имуществена оценка и могат да бъдат отнесени към обекти от материалния свят (вещи)).

За да дефинираме основните съставящи на понятието „културни ценности", нека разгледаме международните инструменти на ЮНЕСКО. Конвенцията на Генералната конференция на ЮНЕСКО от 1970 г. предоставя подробен списък на културните ценности, включително следното:

- ✓ редки колекции и образци на флора и фауна;
- ✓ исторически ценности;
- ✓ предмети, свързани с живота на национални личности;
- ✓ археологически находки;
- ✓ антики;
- ✓ редки ръкописи, книги и документи;
- ✓ пощенски марки;
- ✓ звукови, фотографски и филмови документи;
- ✓ древни музикални инструменти и други.

Според Конвенцията, понятието „културна ценност" следва да обхваща широк кръг от обекти, но те споделят общи характеристики: отражение на особености на националната култура и връзка с историята на определен народ.

Основният критерий за класифициране на културни обекти в определена категория е „изключителна универсална стойност", чието значение е допълнително разработено в Препоръката и Конвенцията на ЮНЕСКО от 1972 г. Тези законодателни актове за първи път изброяват компонентите на културното наследство – паметници, ансамбли и обекти. Определянето на обектите като културно наследство се основава на тяхната изключителна стойност от гледна точка на историята, изкуството, естетиката, антропологията и етнологията, докато тяхната универсалност се отъждествява с уникалност и незаменимост, независимо от тяхната националност. Трябва да се отбележи, че изборът на културни обекти, както и определянето на тяхната стойност, са отговорност на държавите-страни по Конвенцията.

По този начин, културните ценности се разбират като „не само отделни обекти (паметници на архитектурата, скулптурата, живописта, писмеността, печата, фолклора), които могат да бъдат отбелязани в списъци, каталози и др., но и такива явления като традиции и умения в областта на изкуството и образованието, поведение, обичаи, културни индивидуалности на народи, групи от населението и отделни личности".

През април 2019 г. Европейския парламент приема Регламент (ЕС) 2019/880 на ЕП и на Съвета, в който определя „Културните ценности са част от културното наследство, притежаващи високо културно, художествено, историческо и научно значение. Културното наследство е един от фундаменталните елементи на цивилизацията, притежаващ, наред с други неща, символична стойност, оформяйки културната памет на човечеството. То обогатява културния живот на всеки индивид и на цялата общност, допринасяйки за запазването на паметта, развитието на знанието и цивилизацията като цяло. Поради тази причина, то трябва да бъде защитено от незаконно присвояване и плячкосване (параграф 3 от Преамбюла)".

Идентифицираните компоненти в състава на културната ценност подчертават необходимостта от изместване на акцента от механичното им изброяване към определяне на съдържанието на това понятие не само като държавно-правно, но и като научно явление. В тази връзка интересна е теорията на Дейвид Тросби, разглеждаща съдържанието на културната ценност като единство от следните характеристики[18]:

- ✓ естетическа ценност – красота, хармония;
- ✓ духовна ценност – разбиране, просветление, проникновение;
- ✓ социална ценност – връзка, идентификация, единство;
- ✓ историческа ценност – връзка с миналото;
- ✓ символична ценност – представяне на смисъла.

Значението на тази теория се състои в дефинирането на вътрешната структура на културната ценност като такава. Трябва да се отбележи, че основната цел на опазването на наследството е не толкова запазването на обектите, колкото поддържането на ценностите, които те въплъщават. Успешното предаване на тези ценности на бъдещите поколения е невъзможно без отговор на въпросите кой, защо и как оценява културното наследство. С други думи, проблемът с определянето на степента на стойност на даден обект на културното наследство остава нерешен. Горният анализ на съдържателния аспект на културната ценност само потвърждава неговата актуалност.

Според теорията на Д. Тросби, процедурата за оценка на културното наследство може да се осъществява на различни основания, включително икономически, политически, културни и други, което е от решаващо значение за практиката на опазване на културни обекти. Изборът на една или друга основа определя „стратегията за опазване". Според изследователя, запазването на историческа сграда, с доминиране на културно-исторически ценности, предполага повишаване на нейното значение за местните жители, за които асоциациите с древната сграда и нейната история допринасят значително за тяхната групова идентичност. Ако например икономическите ценности са основа за опазване, това води до увеличено строителство на паркинги и магазини за сувенири, в ущърб на историческия пейзаж, с цел привличане на най-голям брой туристи.

Приоритетът на даден подход към опазването на културното наследство зависи от ценностните ориентации на обществото, държавните служители и специалистите, участващи в процеса на опазване, както и от контекста, в който той се осъществява.

Ценностните ориентации на обществото най-вероятно са обект на интердисциплинарни изследвания, тъй като тяхното изучаване включва използването на данни от културологията, психологията и социологията. Провеждането на тези изследвания в рамките на дадено общество остава актуално и включва определяне на значението на понятието „култура" за членовете на

[18] Erica Avrami, Randall Mason, Marta de la Torre. Values and Heritage Conservation. Research report. The Getty Conservation Institute, Los Angeles. – The J. Paul Getty Trust, 2000. – 73 p.//http://www.getty.edu/ conservati on/publications_resources/pdf_publications/valuesrpt.pdf, стр.8

обществото, съществените характеристики, които ѝ се приписват (напр. образование и научна дейност, семейни отношения, модели на поведение, етикет и др.), както и най-значимите ценностни ориентации – мирно съвместно съществуване, добронамереност и откритост, уважение към историята, културно многообразие, прогрес, иновации и други[19].

Професионалната работа с обекти на културното наследство протича на три нива: *евристично, епистемологично и аксиологично*

Евристичното ниво е свързано с целенасоченото търсене на обекти, тяхното събиране и последващото интегриране в музейните колекции.

Епистемологичното ниво се характеризира с цялостно изучаване на обекта: неговия произход, външната му структура, както и неговото предназначение и вътрешен смисъл. Резултатът от работата на това ниво е натрупването на нови знания под формата на каталози, електронни бази данни, научни статии и монографии.

Именно на *аксиологичното ниво* на работа с обекти на културното наследство се разкрива техният ценностен потенциал. Чрез подбора на определени обекти и явления музеят разпознава тяхната историческа, естетическа и мемориална стойност, като по този начин отразява отношението на обществото към компонентите на културното наследство. Културното наследство, като недвижими обекти, също е неразделна част от културния потенциал на определена териториална общност и е защитено от държавата. По този начин културните ценности са критерий за съпоставяне на културното наследство със съвременните изисквания на обществото и, като следствие, условие за възпроизводство и развитие на културата като цяло.

Горният анализ на нормативните документи и опита на местни и международни изследователи ни позволява да заключим, че понятието „културна ценност" е многостранно и неговата характеристика може да се основава на различни подходи.

Първо, разглеждането на съдържателния аспект на понятието „културна ценност" ни позволява да го разглеждаме като съвкупност от обекти и явления на материалната и духовната култура.

Второ, субективната характеристика на понятието представя културната ценност като едновременно въплъщение на националната култура и история на даден народ, което я прави съобразена с понятието „историческо и културно наследство".

Трето, анализът на структурата на културната ценност ни позволява да говорим за единството на естетическите, духовните, социалните, историческите и символичните компоненти.

Четвърто, социалните характеристики на явлението играят важна роля, тъй като културната ценност служи като критерий за техния избор на аксиологично

[19] TNS Opinion and Social. European Cultural Values. - Report Publication, 2007. – 167 p. //http://ec.europa.eu/ culture/pdf/doc958_en.pdf, стр.78

ниво и отразява отношението на обществото към компонентите на културното наследство.

Пето, запазването на изключителни универсални ценности – уникални, незаменими и представляващи изключителен интерес за всички народи по света – като част от световното наследство на цялото човечество е от голямо значение.

Шесто, изборът на културна ценност като основа за стратегията за опазване на обектите на културното наследство е от решаващо значение за практиката на опазване на културното наследство.

Седмо, културната ценност е предпоставка за възпроизвеждането и развитието на културата като цяло.

Следва да се отбележи, че материалната ценност на предметите на изкуството нямат ясен израз и може постоянно да се променят. Следователно, въпросът за законосъобразността на включването на този признак в правното определение все още е доста спорен и се решава в международно-правната литература в зависимост от редица условия: нивото на развитие на пазара, нивото на развитие на гражданското общество и др. Но именно стойностната характеристика на културната ценност е особено важна за нейния оборот на международните пазари на изкуство. Оттук и особеното значение на тази характеристика от гледна точка на нормативното регулиране на икономическия оборот на културните ценности.

Двойствената природа на културните ценности, включваща материалните и духовните им аспекти, е в основата на различни научни подходи и две научни школи, наречени от Д. Мериман „културен интернационализъм" и „културен национализъм"[20]. Основната разлика между тези научни школи са различните варианти за правно регулиране на движението на културни обекти, по-специално решаването на въпросите за защитата и връщането на културните ценности.

Например, поддръжниците на концепцията за „културен интернационализъм" разрешават подобни спорове въз основа на принципите на правата на собственост. Професор Джон Мериман, най-видният представител на тази школа, смята, че културните ценности са продукт на пазара и трябва да се разглеждат като взаимозаменяеми стоки, подходящи за търговия. Въз основа на това определение професор Мериман заключава, че културните ценности, като собственост, могат да бъдат физически запазени, целостта им да се поддържа, а движението им да се контролира чрез правни институции

Представители на школата за „културен национализъм" (например гръцките професори Джон Мустакас и Жорж Кумантос основават подхода си на принципите на правата на човека и вярват, че културните ценности са неотчуждаеми (от своите страни/нации на произход). Следователно, свободното им движение на пазара на изкуството трябва да бъде ограничено. В рамките на концепцията за „културен национализъм", културните ценности се разглеждат като обекти, въплъщаващи националната култура, а не като общодостъпна стока.

[20] Нешатаева, В. О. ,Культурные ценности: цена и право, , изд. дом Высшей школы экономики, Москва 2013, с 208, ISBN 978-5-7598-1029-2

Във всяка от тези концепции има рационално зърно, но върху тях е принципно невъзможно да се намерят общи подходи за дефиниране на понятието „културни ценности".

Вероятно поради липсата на единен подход към правното регулиране на оборота на културни обекти, в съвременното международно право няма единна общоприета концепция за „културни ценности". Всеки нормативно-правен акт на международно, регионално или национално ниво предоставя само редица признаци, които позволяват да се определи даден обект като културна ценност.

Въз основа на съвременни изследвания и нормативни актове обаче е възможно да се формулира единна научно обоснована концепция, в рамките на която културните ценности следва да се тълкуват като особено ценни материални и нематериални обекти и произведения на културата, създадени от човека в резултат на творческия процес, имащи художествено, историческо, археологическо, етнографско, научно, културно значение за обществото и оказващи естетическо въздействие върху човека.

Българската държава има традиция по защитата на културното си наследство и мерките, които са предприети в това отношение се зараждат още след освобождението ни от турско робство. Днес дейността по защитата на културното наследство се регламентира от *Законът за културното наследство*[21] *(ЗКН)*, който защитава културно-историческото богатство на страната ни и правото на всеки от нас на културна идентификация чрез наследството. Нещо повече – в правовия ред на страната опазването на културното наследство е гарантирано на още по-високо ниво – от върховния закон на Републиката. С текста на чл. 23 от Конституцията на Република България то е вменено като конституционно задължение на държавата – ангажимент и препотвърден и от Законът за културното наследство. Според него „Държавата осигурява закрилата на културното наследство независимо от местонахождението му"[22], а „Културните ценности са обществено достояние и се ползват със закрила от държавни и общински органи в интерес на гражданите на Република България"[23].

Културното наследство обхваща нематериалното и материалното недвижимо и движимо наследство като съвкупност от културни ценности, които са носители на историческа памет, национална идентичност и имат научна или културна стойност. ***Културните ценности*** са обществено достояние и се ползват със закрила от държавни и общински органи в интерес на гражданите на Република България. Културните ценности могат да бъдат публична и частна собственост. Те могат да са собственост на държавата, общините, на Българската православна

[21] Закон за културното наследство, в сила от 10.04.2009 г., Обн. ДВ. бр.19 от 13 Март 2009г., посл. изм. ДВ. бр.51 от 5 Юни 2026г.
[22] Закон за културното наследство, в сила от 10.04.2009 г., Обн. ДВ. бр.19 от 13 Март 2009г., посл. изм. ДВ. бр.51 от 5 Юни 2026г..,Чл. 1. ал. 2
[23] Пак там.,Чл. 2 ал. 2

църква и другите регистрирани вероизповедания, както и на физически и юридически лица[24].

Културна ценност е нематериално или материално свидетелство за човешко присъствие и дейност, природна даденост или феномен, което е от значение за индивида, общността или обществото и има научна или културна стойност. Културна ценност може да бъде и нематериално или материално свидетелство за човешко присъствие и дейност, което има научна или културна стойност и е от значение за Българската православна църква и другите регистрирани вероизповедания. Културни ценности са и фрагменти от археологически или други предмети, които са в разрушен вид, съставляват малка част от автентична цялост на предмета, обезличени са в значителна степен, не притежават значима културна, научна или художествена стойност и могат да бъдат определени като масов материал. Те не подлежат на идентификация, но се включват в научно-спомагателния фонд на музеите при необходимост[25].

Не са културни ценности[26]:

1. машинно сечени монети и монетовидни предмети, които нямат значение за научните изследвания и експозиционната стойност, с изключение на особено редки и ценни екземпляри, идентифицирани по реда на този закон като културни ценности;

2. машинно произведени предмети, които не носят подпис или знак на своите автори или са произведени в големи количества, не притежават значима културна, научна или художествена стойност или не са свързани с историческа личност или събитие;

3. произведения на изкуството, собственост на български или чужди автори, или такива, които не са по-стари от 50 години;

4. антикварни предмети, непредставляващи произведения на изкуството, които не са по-стари от 100 години, с изключение на особено редки и ценни екземпляри, идентифицирани по реда на този закон като културни ценности;

5. остатъчен материал – отпадъчна субстанция, получена вследствие от човешка дейност, която няма функционално или художествено предназначение.

Прегледът на международните документи, както и изследването на научната литература по темата, ни позволява да направим следните **ИЗВОДИ:**

1. Все още не е разработено единно, универсално определение за „културни ценности". Липсва единно тълкуване на термина „културни ценности" както в международен, така и в национален план. Продължава дебатът относно съществуващите определения и характеристики на културните ценности.

2. Термините „културно наследство" и „културна ценност" се използват в текстове, понякога в един и същ документ, понякога взаимозаменяемо. Термините „културна ценност" и „паметници" могат да се използват и като еквиваленти.

[24] Закон за културното наследство, в сила от 10.04.2009 г., Обн. ДВ. бр.19 от 13 Март 2009г., посл. изм. ДВ. бр.51 от 5 Юни 2026г., Чл. 2.
[25] Пак там,Чл. 7. Ал.1, 2 и 3.
[26] Пак там, Чл. 7. Ал.4.

Всъщност културните ценности, като обект на международна защита, се разделят на две групи: културни ценности съгласно Хагската конвенция от 1954 г. и обекти на световното наследство съгласно Конвенцията на ЮНЕСКО от 1972 г.

3. От 80-те години на миналия век започва процес на предефиниране на понятието „културна ценност": европейската интерпретация, подкрепена от международни организации за опазване на културата, е омаловажавана като единствен приемлив подход за опазване на културното наследство от средата на 20-ти и началото на 21-ви век.

4. Културното наследство на страните от Далечния изток, Югоизточна Азия и други страни, за разлика от европейските страни, не се състои в конкретни произведения на изкуството или архитектурни структури, а преди всичко в художествените традиции, националните изкуства и занаяти. Основната идея е да се запази националната идентичност на предметите и символите, които те съдържат, символи, важни за разбирането на обществото за бъдещето. Това е културната стойност на тези предмети, тяхното истинско духовно съдържание.

5. Необходимо е да се отбележи, че въпреки повече от век употреба на понятието „културни ценности", нито европейската, нито конвенционално наричаната „азиатска" сфера на опазване на културното наследство няма ясно разбиране за понятието „културни ценности". Няма и точни, универсални критерии, по които определени предмети или явления могат да бъдат класифицирани като културни ценности.

Използвана литература:

1. Фирсова О. Л., Шестопалова Л. В., О термине «культурные ценности» в сфере сохранения культурного наследия, М. : Институт Наследия, 2022. - 92 с., ISBN 978-5-86443-388-1.
2. Михайлова, Т. Б., Экспертиза культурных ценностей: учебно-методическое пособие, Изд-во Урал. 2020, с.156, ISBN 978-5-7996-3108-6
3. Нешатаева, В. О. ,Культурные ценности: цена и право, , изд. дом Высшей школы экономики, Москва 2013, с 208, ISBN 978-5-7598-1029-2
4. TNS Opinion and Social. European Cultural Values. - Report Publication, 2007. – 167 p. http: ec.europa.eu/ culture/pdf/doc958_en.pdf
5. Erica Avrami, Randall Mason, Marta de la Torre. Values and Heritage Conservation. Research report. The Getty Conservation Institute, Los Angeles. – The J. Paul Getty Trust, 2000. – 73 p., http://www.getty.edu/ conservation/publications_resources/pdf_publications/valuesrpt.pdf
6. Хагската конвенция от 14 май 1954 г. „За защита на културните ценности в случай на въоръжен конфликт"
7. Препоръка относно мерки, насочени към забрана и предотвратяване на незаконния износ, внос и прехвърляне на собственост върху културни ценности. Приета от Генералната конференция на ООН за образование, наука и култура на тринадесетата ѝ сесия в Париж на 19 ноември 1964 г.

8. Препоръка относно защитата на движимите културни ценности. Приета от Генералната конференция на ООН за образование, наука и култура на двадесетата сесия в Париж на 28 ноември 1978 г.
9. Конвенция на ЮНЕСКО от 1970 г. „За мерки, насочени към забрана и предотвратяване на незаконния внос, износ и прехвърляне на права на собственост върху културни ценности“
10. Конвенция на ЮНЕСКО от 1972 г. „За защита на световното културно и природно наследство“
11. Вашингтонска харта, приета през 1987 г. от Международния съвет за паметници и забележителности (ИКОМОС), е фундаментален международен документ за опазване на културното наследство
12. Препоръка относно най-ефективните мерки за осигуряване на достъпност на музеите за всички, приета от Генералната конференция на ЮНЕСКО на 14 декември 1960 г., параграф 1
13. Препоръка относно средствата за забрана и предотвратяване на незаконния износ, внос и прехвърляне на собственост върху културни ценности. (Приета от Генералната конференция на ЮНЕСКО на нейната 12-та сесия. Париж, 19 ноември 1964 г., част I)
14. Препоръка относно опазването на културни ценности, застрашени от обществени или частни строителни дейности (приета от Генералната конференция на ЮНЕСКО на 19 ноември 1968 г., параграф 1)
15. Регламент (ЕС) 2019/880 на Европейския парламент и на Съвета от 17 април 2019 г. относно вноса и износа на културни ценности.
16. Закон за културното наследство, в сила от 10.04.2009 г., Обн. ДВ. бр.19 от 13 Март 2009г., посл. изм. ДВ. бр.51 от 5 Юни 2026 г.

TRENDS AND CHALLENGES IN THE DEVELOPMENT OF ANTI-TANK ROBOTIC SYSTEMS

Veliko P. Petrov

Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, veliko_pp@abv.bg

***Abstract**: The development of means of destruction stimulates the development of means of defense against them and vice versa. In the development of weapons, the processes of evolutionary and revolutionary change alternate. Weapons are improved, modernized and modified during the process of evolution. Qualitative changes occur when the development of means of destruction or protection against such means creates a fundamentally new, practically feasible need.*

The potential for innovative development of high-precision weapons is interconnected with the military potential of the state, in whose structure the state of the scientific, technological and organizational foundations for the development, production and operation of weapons is of crucial importance. Competitive achievements in high-precision weapons are possible with the development and provision of the necessary resources for mechanical engineering and instrument-making, scientific and design schools, fundamental and applied scientific research and all levels of education. The development, training and retention of highly qualified specialists is of crucial importance.

Some types of high-precision weapons "compete" with ATGMs in the number of targets they can hit, in terms of their tactical and technical characteristics and life cycle costs. ATGMs are equipped with missiles capable of hitting protected air targets, armored and small-sized ground targets, as well as enemy manpower at any time of the day and in any weather conditions. The use of ATGMs as part of reconnaissance and strike complexes increases their combat effectiveness. Universal ATGMs remain competitive with other types of ATGMs in terms of combat effectiveness/price.

A sustainable trend in the development of ATGMs is automated guidance. The elimination of the operator from the guidance system is necessary, first of all, to improve the accuracy of hitting the target. The most promising approach is passive homing of missiles using machine vision technologies in different spectral ranges, pattern recognition and decision-making algorithms. The machine vision function is implemented by a hardware-software complex on board the missile, which allows it to recognize an image of the target distorted by natural and artificial interference. Passive homing makes it difficult for the enemy to detect the ATGM and the missile in flight. However, the cost of the homing missile is the highest.

The development of ATGMs is aimed at increasing efficiency, giving priority to the safety and security (preservation) of the crew and operators. In the short term, the issue of preserving personnel can be resolved by adopting remotely controlled anti-tank combat modules with operator telepresence. In the medium term, ATGMs will be deployed on autonomous mobile platforms of modular design with integrated navigation, machine vision, image recognition and decision-making systems, combined with artificial intelligence technologies based on training.

***Keywords:** Anti-tank guided missiles (ATGM), high-precision weapons, anti-tank robotic systems*

ТЕНДЕНЦИИ И ПРЕДИЗВИКАТЕЛСТВА В РАЗРАБОТВАНЕТО НА ПРОТИВОТАНКОВИТЕ РОБОТИЗИРАНИ СИСТЕМИ

Велико П. Петров

Локалните войни и въоръжените конфликти от последните десетилетия демонстрираха бързо нарастващото значение на високоточното оръжие (ВТО). Масовото използване на ВТО до голяма степен определи характера на войната в Украйна на тактическо и оперативно ниво. Противотанковите управляеми ракети (ПТУР) остават традиционен, но бързо развиващ се вид ВТО за поразяване на бронирани и други цели.

Разработването на високоточни оръжия се отнася до подобряване на техните характеристики и разширяване на функциите, насочени към повишаване на качеството на оръжията. Разработването на ВТО следва диалектически закони.

Глобална тенденция в разработването на ВТО е замяната на хората с роботи (роботизация), насочена към запазване на личния състав. Тенденциите и перспективите за развитие на роботизирани системи за ВТО са изследвани в множество страни. Роботи за различни цели се тестват във войната в Украйна. Анализът на разработването на противотанкови роботизирани комплекси има за цел да обобщи и прогнозира предизвикателствата и методологичните подходи за осигуряване на качеството при разработването, производството и техническата експлоатация на системи за ВТО в краткосрочен и обозрим средносрочен план.

Съвременните системи ВТО включват комплекси от управляеми оръжия, средства за разузнаване, навигация, обработване на информация и комуникационно оборудване. Традиционните видове ВТО за поразяване на бронирани и други цели на бойното поле остават противотанковите управляеми ракети (ПТУР), управляемите артилерийски боеприпаси и мини. Дистанционно управляемите безпилотни летателни апарати (БЛА) с бойни части (баражиращи боеприпаси) са се превърнали в сравнително ново и ефективно средство за поразяване на малки цели.

Противотанковите ракети, артилерийските боеприпаси, мини и безпилотните летателни апарати (БЛА) се конкурират помежду си и същевременно се допълват, а не заместват, за да поразяват защитени цели при различни метеорологични условия, по различно време на деня и на различни разстояния.

Универсалните противотанкови ракети поразяват не само наземни цели, но и въздушни. Управляемите артилерийски боеприпаси, мини и БЛА са способни да унищожават цели на големи разстояния. Наблюдава се нарастваща тенденция към използване на БЛА като част от противотанкови ВТО, например за разузнаване или „осветяване“ на цели с лазер.

Развитието на средствата за поразяване стимулира развитието на средствата за защита от поразяване и обратно. Бронираните цели (обекти) за ПТУР притежават ефективни оръжия, композитна броня, динамична и активна защита, средства за радиоелектронна борба (РЕБ), те са сравнително малки по размери, способни са да се движат с висока скорост и са маневрени. Сравнителни характеристики на ПТРК на САЩ, Швеция и Русия са дадени в таблица 1.

Таблица 1. Сравнителни характеристики на ПТРК на САЩ, Швеция и Русия

Системи ПТРК / Характеристики на ПТРК	**FGM-148 Javelin (САЩ)**	**NLAW (Швеция)**	**ПТРК "Корнет-ЭМ" (Русия)**
Тип	Преносим ПТРК от трето поколение	Противотанков гранатомет от второ поколение	ПТРК от второ поколение
Маса на носимия комплект	22,5 kg	12,5 kg	44 kg (ПТРК+ракетата)
Калибър на ракетата	127 mm	150 mm	152 mm
Бронепробиваемост	600-800 mm	500 mm	1100–1300 mm
Система за насочване	Самонасочваща се глава в инфрачервения диапазон, принцип „изстреляй и забрави“	„Умен прицел“ с балистически калкулатор	Автоматически по лазерен лъч
Максимално разстояние на стрелбата	3 km	800 m	до 10 km (ракета 9М133ФМ-3)
Цена на носимия комплект	200-230 хиляди долара	30 хиляди евро	15-20 хиляди долара

Основните характеристики на съвременните ПТУР включват:

- ✓ **Усъвършенствани системи за насочване**: Ракетите от трето и пето поколение разполагат с инфрачервени (IIR) и милиметрови вълнови радарни търсачки. Тези механизми „изстреляй и забрави“ позволяват на оператора незабавно да се оттегли или да се укрие след изстрелване. Опциите за „човек в контура“ (чрез оптични кабели) и режимите „изстреляй и актуализирай“ позволяват корекции в средата на курса;
- ✓ **Възможности за атака отгоре**: За да противодействат на силно укрепена предна и странична композитна броня, съвременни системи като американския Javelin или британския NLAW излитат нагоре, преди да се пикират, за да ударят уязвимите покриви на кулите на танковете;
- ✓ **Тандемно-зарядни бойни глави**: Снабдени с кумулативни заряди, съвременните ПТУР побеждават ERA, като използват по-малък начален заряд за детониране на блока с реактивна броня, последван веднага от по-голям основен заряд, който прониква в първичната броня;
- ✓ **Универсалност и многорежимно взриване:** Днешните ракети вече не са строго противобронени. Много от тях разполагат с избираеми взриватели за директна атака, високоексплозивни или термобарични профили за елиминиране на

вражески персонал, унищожаване на укрепления и поразяване на мекообвивни превозни средства;

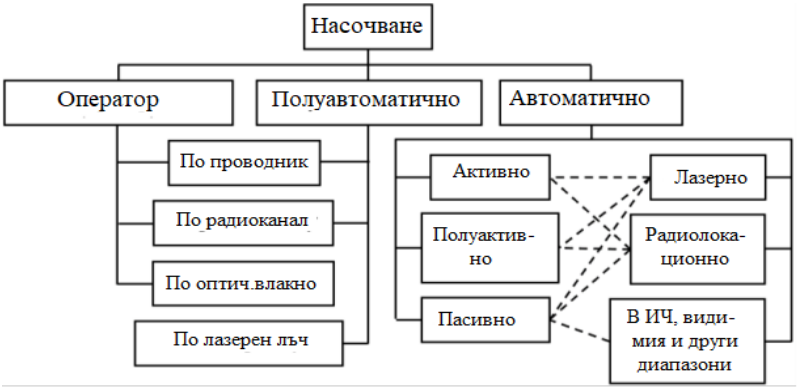
- ✓ **Съпротивление при противодействие:** С разпространението на системи за активна защита (APS) върху съвременните танкове, съвременните системи – като френската AKERON MP – използват скрити техники за проследяване и режими на оптично насочване, за да заобиколят заглушаването и отбранителния огън;
- ✓ **Платформи за изстрелване**: Изключителна гъвкавост, позволяваща преносимост от пехотата (man-portable), монтаж на бронирани машини или изстрелване от дронове и хеликоптери;
- ✓ **Управление извън пряката видимост**: Някои съвременни комплекси, като израелския Spike, позволяват поразяване на цели зад препятствия с помощта на оптико-електронна връзка в реално време.

Възможностите на ПТУР бързо се разширяват показано в таблица 2.

Таблица 2. Характеристики на съвременните противотанкови ракети (ПТУР)

Наименование Характеристики	Условно обозначение				
	FGM-148 «Javelin» САЩ	9M123-2 «Хризантема» Русия	9M133M-2 «Корнет-ЭМ» Русия	Akeron MP Франция	Spike LR2 Израиль
Година на приемане на въоръжение	1996	2004	2013	2017	2018
Калибър, мм	127	152	152	140	170
Маса, кг	15,5	54	31	11	12,7
Скорост на полета, м/с	Дозвукова	Свръхзвукова	Дозвукова	Дозвукова	Дозвукова
Разстояние на стрелбата, мин./макс., м	75/3000	400/5000	150/8000	5000	5500
Бойна част	Тандемно-кумулативна	Тандемно-кумулативна, фугасна и термобарична	Тандемно-кумулативна	Тандемно-кумулативна	Тандемно-кумулативна
Бронепробиваемост, мм	600-800	1100	1100–1300	1000	–
Система за насочване	Самонасочваща се глава (СНГ) в инфрачервения диапазон и видимия оптичен диапазон с охлаждане	Автоматично полуактивно радарно насочване; полуавтоматично насочване по лазарен лъч	Автоматично полуактивно оптоелектронно насочване с телеориентация на лазерен лъч	СНГ в инфрачервения диапазон и видимия оптичен диапазон без охлаждане, инерционен измервателен блок и обмен на данни чрез оптични влакна	СНГ в инфрачервения диапазон и видимия оптичен диапазон без охлаждане, обмен на данни по радиоканал

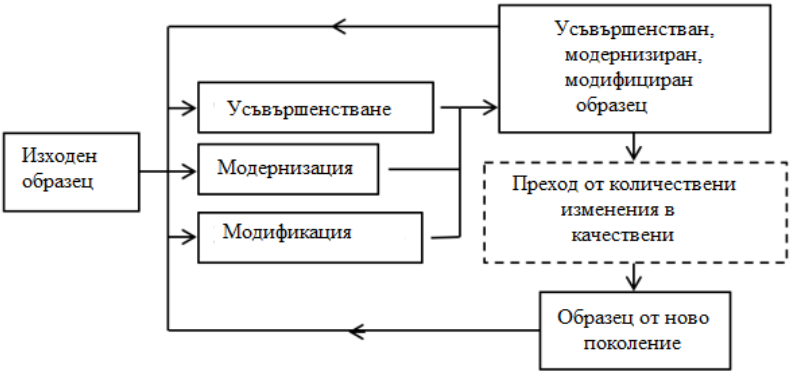
Тенденцията в развитието на системите за насочване на ПТУР е автоматизацията, насочена към повишаване на точността на поразяване на целта (Фигура 1). Автоматичното насочване на ракетата се постига чрез използване на лъчение, отразена от целта (активно самонасочване или полуактивно насочване) или чрез изучаване на целта (пасивно самонасочване). Източникът на лъчението може да бъде разположен на борда на ракетата (активно самонасочване), на пусковата установка (полуактивно директно насочване) или външно от пусковата установка (полуактивно индиректно насочване).



Фигура 1: Класификация на системите за насочване на противотанкови ракети

Най перспективните направления за развитие на системите за насочване на противотанковите ракети е пасивното самонасочване в различни спектрални диапазони, използващи технологии за машинно зрение, разпознаване на образи и алгоритми за вземане на решения.

Функцията за машинно зрение се реализира от апаратно-програмен комплекс на борда на ракетата, която ѝ позволява да разпознава изображение на целта, изкривено от естествени и изкуствени смущения. Пасивното самонасочване затруднява противника да открие оператора и ракетата по време на полет.



Фигура 2: Модел на разработване на оръжия

В разработването на оръжия, еволюционните и революционните промени се редуват съгласно закона за количествените промени, които стават качествени (Фигура 2). Еволюционните промени протичат итеративно чрез усъвършенстване, модернизация и модификация на конструкции. Необходимостта от революционни промени възниква, когато количественото развитие, основано на предишни принципи, достигне задънена улица или разработването на оръжия или защитни средства срещу тях създава фундаментално нова нужда. Качествените промени водят до промяна в поколенията оръжия.

Анализ на тенденциите в развитието на противотанковото ВТО идентифицира шест поколения системи за насочване на противотанкови ракети (Таблица 3). Общоприети критерии за четвъртото и петото поколение все още не са установени[27]. Последните поколения системи за насочване позволяват изстрелване на ракети по разузнавателни координати без засичане на целта, засичане на целта в полет и взаимодействие с разузнавателни и насочващи системи за пренасочване на ракетата в полет. В обозримо бъдеще насочването на ракети от шесто поколение ще се основава на принципите на изкуствения интелект.

Таблица 3. Поколения в развитието на системите за насочване на противотанкови ракети

Поколение	Принцип на насочване	Примери
Първо	Ръчно насочване на ракетата. Операторът следи целта и ракетата чрез оптичен прибор и предава команди „ляво-дясно, нагоре-надолу" към ракетата чрез лост за управление, по кабел или по радио.	3М11 «Фаланга»; 9М14 «Малютка»
Второ	Полуавтоматично насочване на ракета по линията на видимост (принцип „виж-	3М6 «Шмел»; 9М111«Фагот»;

[27] Поколения ПТУР и взгляд компании «Рафаэль» на ПТУР 5-го поколения, https://oleggranovsky.livejournal.com/188937.html

	стреляй“). Операторът следи целта чрез оптичнен прибор и поддържа прицелната маркировка върху нея. Апаратурата за управление предава команди към ракетата по проводници или радио, или насочва ракетата с помощта на лазерен лъч (поколение 2+).	9М113 «Конкурс»; 9М114 «Щтурм»; 9М115«Метис»; 9М117 «Кастет»; 9М133 «Корнет»
Трето	Автоматично активно или пасивно самонасочване на ракетата (принцип „изстреляй и забрави“) или автоматично полуактивно насочване на ракетата с помощта на апаратура за насочване на ракетата-носител. Операторът търси и идентифицира целта. След като захване целта за автоматично проследяване, операторът наблюдава процеса на пуска и оценява резултатите от него.	FGM-148 «Javelin»(САЩ); ATM-5 (Япония); «Корнет-ЭМ» Русия; 9М123-2 «Хризантема»Русия; HJ-12 (Китай)
Четвърто	Системата за самонасочване на ракетата може да бъде пренасочвана по време на полет. Операторът получава видеоизображение от ракетата и предава управляващи команди на ракетата чрез оптичен кабел или радио. Ракетата може да бъде изстреляна без да се захване целта, насочвайки я към разузнавателни координати.	Spike-LR, SpikeER и SpikeNLOS (Израел)
Пето	Самонасочване с възможности от четвърто поколение и използване на алгоритми за разпознаване на цели. Системата за насочване може да взаимодейства със системите за разузнаване и насочване на ракетата по време на полет.	Akeron MP (Франция); Spike LR2 и Spike ER2 (Израел)
Шесто	Самоизстрелване, избор на цел и самонасочване на ракета. Перспективна напълно автономна (роботизирана) система за управление, използваща машинно зрение и алгоритми за разпознаване на образи, способна да открива, разпознава, идентифицира цел и да взема решение за изстрел без намесата на оператора.	Ракетите са в етап на разработка.

Еволюцията на системите за насочване на ПТУР протича по „спирала“, в съответствие със закона за отрицанието на отрицанието. В системите за ръчно насочване от първо поколение операторът е следил целта и ракетата визуално и е предавал командите за управление по проводници или радио. В следващите поколения ръчното насочване е внедрено на ново технологично ниво чрез оптична комуникационна линия с телеприсъствие на оператора. Отрицанието на ръчното насочване първоначално е довело до изключване на оператора от системата за насочване, а след това до включването на елементи на изкуствен интелект в системата за насочване.

Съвременните противотанкови ракети са ефективни оръжия, наукоемки, високотехнологични и технически сложни изделия, чието разработване, серийно производство и техническа експлоатация изискват значителни разходи за ресурси. Например, общата стойност на програмата за разработване и производство на системата Javelin е била 5 милиарда долара. Цената на закупуването на системата за армията на САЩ е била приблизително 126 000 долара по цени от 2002 г.[28]. Тази висока цена възпрепятства серийното производство на нови поколения ПТРК.

Основата на противотанковите ВТО на руската армия се състои от ПТУР от второ и трето поколение. Тенденцията за изоставане от техните противници стана очевидна през 90-те години на миналия век с приемането на системата Javelin с инфрачервена самонасочваща глава в Съединените щати[29]. Това изоставане може да се обясни не с научно-технически причини, а с организационно-икономически причини. Всъщност по това време СССР вече разполагаше със зенитната ракета 9М37 с инфрачервена самонасочваща глава. Това изоставане се запазва и до днес и може да бъде преодоляно с възраждането и финансирането на приборостроенето.

Противотанковите управляеми ракети са гръбнакът на противотанковия ракетен комплекс (ПТРК). Тенденциите и перспективите за развитие на ПТРК са отразени в Таблица 4.

Таблица 4. Класификация на противотанкови ракетни комплекси

Класификационна характеристика	**Класификационно групиране**
Носител на комплекса	Преносим комплекс (комплекс, носен или транспортиран от екипаж)
	Самоходен комплекс (системата може да се носи от превозно средство, бронетранспортьор, бойна машина или танк)
	Авиационен комплекс (носителят на комплекса може да бъде хеликоптер, щурмови самолет или безпилотен летателен апарат)
	Корабен комплекс
Разположение на комплекса върху носителя	Сменяем комплекс
	Интегриран комплекс
	Боен модул (например, «Квартет-М» и «Кливер»)
Местоположение на оператора на комплекса	Комплекс управляван от оператор на огнева позиция.
	Дистанционно управляван комплекс (управление с износим пулт)
	Телеуправляем комплекс (управляем дистанционно чрез защитени комуникационни канали)
	Автономен комплекс (автономен робот)

[28] Javelin Medium Anti-armor Weapon System, http://www.inetres.com/gp/military/infantry/antiarmor/Javelin.html
[29] Пак там

Бойните машини на ПТРК, оборудвани със системи за разузнаване, комуникация и управление, образуват разузнавателно-ударен комплекс. В състава на ПТРК може да се включва средства за техническо обслужване на ракетите и носителя на въоръжение, симулатор за обучение на оператори и учебна мишена.

Разчетът на противотанковия ракетен комплекс (ПТРК) се намира на мястото на пуска или близо до мястото на пуска на ракетите (ако е наличен износим пулт) и може да бъде наранен в случай на неизправност или нарушение на правилата за използване на оръжието. ПТРК може да бъде открита и унищожена, заедно с разчета си, от противникови високоточни оръжия. Разработчиците на ракети и ПТРК обръщат внимание на въпроса за безопасността и защитеността на личния състав на разчета.

Системите, които използват принципа „стреляй и забрави“, позволяват на разчета бързо да напусне (промени) позицията си след изстрелване на самонасочваща се ракета. За да защитят разчета и системата от противникови оръжия, те използват средства за радиоелектронна борба, NVS филтри, маскировка, автономни системи за откриване и проследяване на цели и дистанционно управление износим пулт. Всички тези мерки обаче само частично решават проблема със запазването на личния състав. Роботизацията е глобална тенденция в решаването на този проблем.

Идеята за използване на дистанционно управление за осигуряване на безопасността и сигурността на разчета е доразвита в дистанционно управляеми роботи. Операторът на робота се намира в мобилен контролен център на относително безопасно разстояние от противника. Системата за дистанционно управление на робота осигурява телеприсъствие на оператора. Обменът на информация между робота и операторите обикновено се осъществява чрез защитен радиоканал.

Таблица 5. Боен многофункционален роботизиран комплекс „Уран-9“

Назначение	**Основни задачи**	**Възможности**
Провеждане на разузнавателна и огнева поддръжка на предни и разузнавателни подразделения от общовойсковите формирования на тактическо ниво, повишаване на ефективността на бойните задачи и намаляване на загубите на личен състав по време на бойни операции, включително в градски райони	Провеждане на разузнаване, осигуряване на огнева поддръжка на общовойсковите и разузнавателни подразделения, поразяване на неподвижни и движещи се цели от типа танк с противотанкови ракети на разстояние до 5000 м през деня и 3500 м през нощта, поразяване на неподвижни и движещи се цели със стрелково оръжие и огнехвъргачни оръжия през деня и нощта.	Задвижван от бордови батерии в режим на изключен двигател, движение по предварително определен маршрут с автоматично откриване и избягване на препятствия, предаване на командите за управление с мобилна контролна станция и пулт за дистанционно управление към друг робот на разстояние най-малко 1 км, дистанционно (чрез радио) управление от мобилна контролна станция и пулт за дистанционно управление на обхват най-малко 3 км, в зависимост от местността и климатичните условия, и автоматично проследяване на целта.
Забележка: Всеки робот и контролен панел са оборудвани със система за предупреждение за лазерно облъчване, която позволява на оператора да идентифицира източника на облъчване в рамките на 30° сектор. Като допълнителна мярка за безопасност, роботът е оборудван със система за разгръщане на димна завеса, която автоматично разгръща димна завеса в сектора, от който роботът е облъчен с лазер.		

Дистанционно управляемият разузнавателно-ударен робот „Уран-9“, който е влязъл в серийно производство и е приет на въоръжение в руската армия (Таблица 5)[30][31].

Роботът е въоръжен с 30-милиметрово автоматично оръдие 2А72, 7,62-милиметрова картечница ПКТМ, комплекс управляемо въоръжение „Атака“ и пехотни реактивни огнехвъргачки „Шмел-М“ с РПО ПДМ-А.

Недостатъкът на мобилния робот, управляван дистанционно чрез радио, е, че мобилният контролен център и мобилната платформа могат да бъдат открити чрез радиоизлъчвания, комуникациите им могат да бъдат заглушени от средствата за радиоелектронна борба и те могат да бъдат унищожени от високоточни оръжия.

[30] SKB OF THE Ministry of Defense of THE Russian Federation. The company's products. URAN-9, https://skbmo.ru/uran9.html

[31] В. С. Айрапетян1*, В. А. Литовченко2*, Н. Н. Бардачевский2 , А. В. Коломакин2 Обзор современных роботизированных комплексов военного назначения, https://geosib.sgugit.ru/upload/geosibir/sborniki/2023/ tom-8-2/150-157.pdf?ysclid=mm4k64evmt572173812

Таблица 6. Многофункционален роботизиран комплекс „Маркер“

Назначение	Основни задачи	Възможности
Модулна роботизирана колесна или верижна платформа, способна да преодолява водни препятствия с дълбочина до 0,8 м, съдържа няколко десетки различни сменяеми модула за полезен товар за различни задачи, осигурявайки на платформата многофункционалност.	Защита на съоръжения, транспортиране на хора и товари, осигуряване на огнева поддръжка на подразделения, провеждане на разузнаване с помощта на дронове, унищожаване на малки безпилотни летателни апарати (БЛА) и дронове камикадзе.	Той разполага с функционалност за автономно управление на автомобили, модулна мултиспектрална система за машинно зрение и невронна мрежа за разпознаване на обекти от изображения от видеокамера. Оборудван е с видими, инфрачервени и радарни сензори. Разполага с висикоскоростно безредукторно задвижване за въртящия се модул. Оптоелектронното устройство, което наблюдава, заснема и проследява обект, има собствени задвижвания. Прецизността и скоростта на задвижванията му позволяват да поразява наземни цели и мини-безпилотни летателни апарати. Две независими задвижвания на полезния товар му позволяват да поразява цели едновременно с различни видове оръжия. Колесната платформа има обхват до 1000 километра и скорост до 80 км/ч.

Перспективна насока за развитие на бойните роботи е осигуряването на тяхната автономност чрез адаптивно управление, базирано на принципите на изкуствения интелект (машинно зрение, разпознаване на образи и алгоритми за вземане на решения). Адаптивният робот е способен да изпълнява предвидените си задачи без човешка намеса. В интернет има съобщения за тестване на автономния робот "Маркер" в зона за специални операции в Украйна (Таблица 6)[32]. Роботът може да бъде въоръжен с тежка картечница, автоматичен гранатомет, ракети, барражиращи боеприпаси, касетъчни боеприпаси и привързани безпилотни летателни апарати.

Интегрираната адаптивна система за управление на противотанковия роботизиран комплекс съчетава възможностите на спътниковата и инерционната навигация с възможностите на машинното зрение, разпознаването на изображения и вземането на решения, както е при пасивната система за самонасочване на ракети и боеприпаси.

Адаптивните функции за управление се реализират от апаратно-програмен комплекс на бойния модул и мобилната платформа. Човешката роля в автономната система е ограничена до създаване на задачи и наблюдение на работата на робота. Операторите могат, ако е необходимо, да управляват робота дистанционно (полуавтономна работа).

[32] The Marker robotics complex, https://marker.npo-at.com

Тенденция в разработването на роботи е агрегацията[33]. Този метод на агрегация се основава на използването на унифицирани и стандартизирани апаратно-програмни модули с интегрирани системи за управление[34]. Агрегацията намалява разходите за ресурси за разработка, производство, поддръжка и ремонт чрез композируемост, интеграция, оперативна съвместимост, повторна употреба и взаимозаменяемост на модулите, както и модернизация чрез взаимозаменяемост с други модули с подобрени характеристики.

Бойния робот може да служи като средство за огнево поразяване в рамките на разузнавателно-ударен комплекс. В допълнение към средство за огнево поразяване, разузнавателно-ударен комплекс включва защита срещу противникови оръжия, разузнавателни средства, разузнавателни безпилотни летателни апарати (БЛА), системи за командване и управление и свръзка. Интегрирането на бойни роботи със съвременни разузнавателни, защитни и комуникационни системи в рамките на разузнавателно-ударните комплекси значително повишава тяхната бойна ефективност.

Противотанковият робот е проектиран да изпълнява тактически задачи. Неизпълнението на бойна задача обикновено има сериозни последици. Готовността на оръжията за изпълнение на бойна задача се осигурява чрез тестируем дизайн и интегрирана логистична поддръжка за техническа експлоатация, базирана на анализ на видовете, последствията и критичността на повреди, както и чрез поддържане и възстановяване на функционалността на компонентите в рамките на системата за поддръжка и ремонт.

Разработването на ВТО е насочено към осигуряване на максимална ефективност (принцип на максимална ефективност) с приоритет върху запазването (безопасността и защитеността) на разчета чрез роботика. Показателите за качество се определят от ползвателя и разработчика по взаимно съгласие. Потенциалните несъответствия (несъгласия) се разрешават чрез компромис между ползвателя и разработчика.

Чрез консолидиране на натрупания опит в разработването на роботизиран комплекс и отчитане на тенденцията към роботизация на съществуващите модели на роботизирани комплекси, е разработена концепция за унифицирана система за управление на роботизиран комплекс на ПТРК[35]. Тя се състои от отделни подсистеми, свързани чрез различни информационни шини, най-често използваните от които са Ethernet и CAN. Всяка подсистема включва блок за управление, изпълнителни устройства, сензори и изчислителни устройства. Този модулен тип позволява модернизиране и разширяване на системата, а също така улеснява самодиагностиката и корекциите на процесите.

---

[33] Агрегацията (от лат. *aggregatio* – присъединяване) е процес на обединяване на отделни елементи, данни или компоненти в единна система, група или цялост.

[34] GOST R 60.2.0.1-2022 Robots and robotic devices. The modular principle of building service robots. Part 1. General requirements. – Moscow : Russian Institute of Standardization, 2022. – 65 p.

[35] Лопота, А. В. Наземные робототехнические комплексы военного и специального назначения / А. В. Лопота, А. Б. Николаев / ЦНИИ робототехники и технической кибернетики, https://rtc.ru/media/images/docs/book/nazemnie.pdf

Тази система за управление включва следните подсистеми:
– централна изчислителна система;
– система за комуникация и предаване на данни;
– система за захранване;
– система за управление на движението;
– система за машинно зрение/външно видеонаблюдение;
– система за навигация и топографско ориентиране;
– система за планиране на движението;
– полезен товар, който може да включва боен модул, разузнавателен модул, модул за самоунищожение и др.

Тази структура на роботизиран комплекс позволява възможност за коригиране на тактиките и разширяване на обхвата на приложение след разработването ѝ, увеличавайки нейната гъвкавост и ефективност.

Към края на 2025 г. световният пазар на противотанкови ракети достига 400 милиона долара годишно, с прогнози за 500-535 милиона долара до 2032 г. при 4-5 % годишен темп на растеж, подхранван от модернизацията и конфликтите. Ключови играчи включват Lockheed Martin/Raytheon (Javelin), Rafael (Spike), KBP (Kornet) и MBDA (Akeron). Растежът произтича от търсенето на преносими системи „стреляй и забрави" на фона на нарастващото геополитическо напрежение. Противотанковите управляеми ракети предефинираха наземната война, изместващи господството от тежка броня към високоточна огнева мощ. От скромни ПТУР управлявани по проводник до сложни ПТУР хищници от типа „стреляй и забрави", те гарантират, че никой танк не е непобедим, балансирайки настъпление и отбрана в безкрайна технологична надпревара във въоръжаването.

Размерът на световния пазар на противотанкови ракетни системи достигна 3,3 милиарда щатски долара през 2025 г. В бъдеще IMARC Group очаква пазарът да достигне 4,4 милиарда щатски долара до 2034 г., показвайки темп на растеж (CAGR) от 2,89 % през периода 2026-2034 г. *Нарастващите бюджети за отбрана от страна на правителствата за усъвършенствани системи за укрепване на военните способности стимулират пазара.*

Съвременните бойни операции изискват високо ниво на оборудване и подготовка на военните формирования от всички армии по света. Съвременният начин на водене на бойни действия и по-масираното използване на бронетанкови и механизирани формирования изисква използването на високоефективни противотанкови ракетни системи от по-нови поколения.

Изводи:

1. Развитието на средствата за поразяване стимулира развитието на защитни средства срещу тях и обратно. При разработването на оръжията процесите на еволюционна и революционна промяна се редуват. Оръжията се усъвършенстват, модернизират и модифицират по време на процеса на еволюция. Качествените промени възникват, когато разработването на средствата за поразяване или защитата от такива средства създава принципно нова, практически осъществима нужда.

2. Потенциалът за иновативно развитие на високоточни оръжия е взаимосвързан с военния потенциал на държавата, в чиято структура състоянието на научните, технологичните и организационните основи за разработване, производство и експлоатация на оръжия е от решаващо значение. Конкурентните постижения във високоточни оръжия са възможни с развитието и осигуряването на необходимите ресурси за машиностроенето и приборостроенето, научните и конструкторските школи, фундаменталните и приложните научни изследвания и всички нива на образование. Развитието, обучението и задържането на висококвалифицирани специалисти е от решаващо значение.

3. Някои видове високоточни оръжия „се конкурират“ с ПТРК за броя на целите, които могат да поразят, по отношение на техните тактико-технически характеристики и разходи за жизнения цикъл. ПТРК са оборудвани с ракети, способни да поразяват защитени въздушни цели, бронирани и малоразмерни цели на земята, както и противниковата жива сила по всяко време на денонощието и при всякакви метеорологични условия. Използването на ПТРК като част от разузнавателно-ударни комплекси повишава тяхната бойна ефективност. Универсалната ПТРК остава конкурентоспособна с други видове ВТО по отношение на бойна ефективност/цена.

4. Устойчива тенденция за развитие на ПТУР е автоматизираното насочване. Елиминирането на оператора от системата за насочване е необходимо, преди всичко, за да се подобри точността на поразяване на целта. Най-обещаващият подход е пасивното самонасочване на ракети, използващо технологии за машинно зрение в различни спектрални диапазони, разпознаване на образи и алгоритми за вземане на решения. Функцията за машинно зрение се реализира от апаратно-програмен комплекс на борда на ракетата, която ѝ позволява да разпознава изображение на целта, изкривено от естествени и изкуствени смущения. Пасивното самонасочване затруднява противника да открие ПТРК и ракетата в полет. Цената на самонасочващата се ракета обаче е най-висока.

5. Развитието на ПТРК е насочено към повишаване на ефективността, като се дава приоритет на безопасността и защитеността (запазването) на разчетите и операторите. В краткосрочен план въпросът за запазване на личния състав може да бъде решен чрез приемане на дистанционно управляеми противотанкови бойни модули с телеприсъствие на оператора. В средносрочен план ПТРК ще бъдат разположени на автономни мобилни платформи с модулен дизайн с интегрирани системи за навигация, машинно зрение, разпознаване на изображения и вземане на решения, комбинирани с технологии за изкуствен интелект, базирани на обучение.

Използвана литература:

1. Макаренко С. И. Робототехнические комплексы военного назначения – современное состояние и перспективы развития // Системы управления, связи и безопасности. – 2016. – №2. – С. 73–132. URL: http://sccs.intelgr.com/archive/2016-02/04-Makarenko.pdf.
2. Лопота А.В., Николаев А.Б. Наземные робототехнические комплексы военного и специального назначения. Государственный научный центр ЦНИИ робототехники и технической кибернетики. – СПб: 2019. – 30 с.
3. Тиханычев О.В. О правовых и этических аспектах автономного использования робототехнических комплексов в сфере вооруженного противоборства // Вопросы безопасности. – 2019. – № 3. – С. 33–42. – URL: https://e-notabene.ru/nb/article_28960.html
4. В. Александров, Р. Ветлугин, А. Макаренко. Взгляды военных специалистов США на боевое применение наземных робототехнических комплексов // Зарубежное военное обозрение. – 2018. – №6. – С. 39–43.
5. И. Бозов, Анализ на техническите възможности на противотанкови ракетни системи FGM-148 javelin и 9M133 Kornet, International Scientific Conference “Defense Technologies” DefTech 2025, стр. 584-590, ISSN 2815-4282
6. I. Bozov, Unmanned combat aerial vehicle (UCAV) – weapon of the future, International Scientific Conference ―“Defense Technologies” DefTech 2023, Стр.243-247, ISSN 2367-7902
7. А.И. Наговицин, Б.Б. Молоткова, Робототехнические комплексы военного назначения, перспективы их применения в РВ и А ВС РФ, https://www.elibrary.ru/item.asp?id=28948279&ysclid=mrd75hxlr9761611925
8. Anti-Tank Guided Missiles -The Evolution and Impact, February 9, 2026, https://aviationanddefensemarketreports.com/the-evolution-and-impact-of-anti-tank-guided-missiles/
9. Anti-tank Missile System Market Report by Missile Type (Man-Portable, Vehicle-Mounted), Platform (Airborne, Ground-Based), End User (Military, Commercial), and Region 2026-2034, https://www.imarcgroup.com/anti-tank-missile-system-market
10. Marko Radovanović, Aleksandar Petrovski, Saša Smileski, Željko Jokić, Analysis Of The Development Of Five Generation Of Anti-Armor Missile Systems, cientific Technical Review, 2023,Vol.73,No.1,pp.26-37
11. Мосиенко, С.А. Концепция построения наземного робототехнического ударного комплекса [Текст] / С.А. Мосиенко, В.И. Лохтин – М.: ООО «Самполиграфист», 2014. – 124 с.

HISTORY OF THE DEVELOPMENT OF THE LEGAL PROTECTION OF CULTURAL VALUES

Veliko P. Petrov

Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, *veliko_pp@abv.bg*

***Abstract**: The origin and regulation of the protection of cultural property have gone through a long path of development, improvement and renewal. The history of the development of international legal protection of cultural property shows regularities in the emergence of legal norms, determined by practical needs, and can be divided into several most important stages: Antiquity, the Middle Ages (before the Renaissance); the beginning of the Renaissance to the first attempts at international legal regulation (the end of the 19th century); international legal regulation during the First World War; from the First World War to the end of the Second World War and to the present day. Throughout human history, cultural treasures have been subject to destruction, destruction and damage as a result of wars, natural disasters, terrorist attacks and other forms of violence. However, since ancient times, people have understood the importance of preserving cultural heritage and have created laws, established measures and rules for its protection.*

History clearly shows that no matter how perfect the international legal norms adopted for the protection of cultural values are, they cannot solve these problems to an acceptable extent. There are numerous examples of how these norms have been neglected during armed conflicts and cynically circumvented for selfish purposes in peacetime. In order to preserve the cultural heritage of both a separate country and all of humanity, it is necessary, in addition to efforts to create a normative instrument for cultural protection, to pay special attention to the multifaceted process of cultivating humanity in people. Only the development of this moral quality can lead to irreversible results in solving the vital issue of preserving the best achievements of human creativity. With the acceleration of globalization, the growth of national and cultural identity and the protection of the interests of national minorities, the scope of challenges facing the UN institutions, whose main task is to protect cultural heritage sites from desecration, destruction and damage, is also expanding. The preservation and protection of cultural values is an integral part of international cultural cooperation, without which mutual understanding between peoples cannot be ensured.

***Keywords:** protection of cultural property, international legal norms, international legal regulation*

ИСТОРИЯ НА РАЗВИТИЕТО НА ПРАВНАТА ЗАЩИТА НА КУЛТУРНИТЕ ЦЕННОСТИ

Велико П. Петров

Проблемът за опазването на световното културно наследство и признаването му като определящ фактор в общественото развитие е едно от глобалните предизвикателства, пред които е изправено човечеството през 21-ви век. Необратимата загуба на културни ценности е настъпвала и продължава да се случва както в мирно време, така и по време на въоръжени конфликти.

Културните ценности представляват наследство, създавано от човечеството през вековете, и формират основата на културата и идентичността на народите и държавите. Културните ценности, като исторически паметници, музеи, творчески произведения, научни открития и символи на народната култура и традиции, винаги са били от съществено значение за опазването и развитието на културното наследство и формирането на споделена културна памет.

Защитата на културните ценности не е ново явление, тъй като значението на опазването и защитата на културното наследство е било разбирано още в древността. Различни цивилизации са разработили закони, разпоредби и механизми за защита на културните обекти от унищожаване, кражба и вандализъм.

Произходът и регулирането на защитата на културните ценности и предмети са изминали дълъг път на развитие, усъвършенстване и обновление. Историята на развитието на международната защита на културните ценности показва закономерности във възникването на правни норми, обусловени от практически нужди, и може да бъде разделена на няколко най-важни етапа: Античност, Средновековие (преди Ренесанса); началото на Ренесанса до първите опити за международно правно регулиране (края на 19 век); международно правно регулиране по време на Първата световна война; от Първата световна война до края на Втората световна война и до наши дни.

Първите закони, установяващи правила и мерки за защита на културните съкровища, са създадени в древността. Например, египетските фараони са издавали укази, насочени към опазване на мемориални храмове, пирамиди и други художествени паметници. Защитата на културните ценности по време на война също е била приоритет в Древен Египет. Египетската цивилизация е била една от най-развитите и просперищи в древността, а културните ценности са били от голямо значение за народа и държавата.

По време на управлението на фараоните в Египет, културните обекти и паметници са били обект на почит и уважение, а запазването на тяхната цялост е било една от основните отговорности на правителството. Поради това са създадени закони и разпоредби, които да защитават културните обекти от унищожаване и кражба. По време на периоди на военни конфликти египетските фараони издавали укази, насочени към запазване на мемориални храмове, пирамиди и други художествени паметници. Паметниците, свързани с боговете, били особено важни, тъй като символизирали връзката между държавата, народа и божествата. Фараоните насърчавали запазването на тези паметници и установявали наказания за тяхното разрушаване. Значението на опазването на културните обекти и художествените паметници е било разбирано още тогава и Древен Египет е станал една от първите държави, създали система за защита на културните ценности.

Защитата на културните съкровища по време на война също е била важна задача в Древна Гърция. През античността Гърция е била известна със своето културно наследство, което е включвало храмове, театри, стадиони, скулптури, керамика, картини и други художествени предмети. Те са били не само част от културата, но и символизирали значението на държавата и нейния народ.

В Гърция културните ценности са имали статут на „неприкосновени обекти“ по време на война. Това е означавало, че военните действия не са могли да бъдат насочени към унищожаване на културни обекти. Освен това е имало специални закони и разпоредби, уреждащи отношенията между държавата и художниците, архитектите и скулпторите.

Гръцкият летописец Полибий в своя труд „Всеобща история“ е писал преди повече от 2000 години: „…надявам се, че бъдещите завоеватели ще се научат да не опустошават градовете, които завладяват, че ще се въздържат от разкрасяване на собствените си страни за сметка на нещастията и несгодите на други народи“.

Първите протести срещу унищожаването и разграбването на културни съкровища по време на война са се чували и в древен Рим в речите на Цицерон. Древен Рим се смята за една от най-великите и най-напредналите цивилизации на древността. Римската държава е контролирала огромна територия, а културното ѝ наследство е било огромно. Следователно, защитата на културните съкровища по време на война е била изключително важна задача. В Рим са създадени специални музеи и галерии, за да се съхраняват произведения на изкуството и науката. Тези музеи са били защитени от закона и охранявани от специални организации.

По време на военни операции римското право е установявало наказания за повреждане и кражба на културни ценности. Римската държава строго е забранявала унищожаването на културни ценности, а военните действия не са могли да бъдат насочени към унищожаване на културни съкровища. Древен Рим е разбирал важността на опазването на културните съкровища по време на военно време. Създавали се и стриктно се прилагали закони и разпоредби, насочени към опазване на културното наследство. Културните обекти и художествените паметници се считали за символи на силата и просперитета на римската държава, а тяхното опазване било важен елемент за поддържане на нейния престиж.

През Средновековието, чак до Ренесанса, не е имало съществени промени по отношение на културните ценности и обекти, нито в законодателен, нито в практически смисъл. Не е имало международни правни разпоредби, установяващи техния статут, правен режим, правила за движение и др. Въпросът е бил сведен, в най-добрия случай, до морални съображения, а единственият ограничаващ фактор е бил личният интерес на отделните граждани от опазването на културните ценности. Войните, водени по религиозни причини (например, нашествието на арабите, османските турци и др.), са довели до системно унищожаване на културните ценности на народите от други вероизповедания.

Ренесансът е период в европейската история, който започва през 14-ти век и продължава до 17-ти век. През този период културното наследство придобива ново значение и започва да се счита за неразделна част от европейската култура. В този контекст защитата на културните ценности става по-организирана и систематична. По време на Ренесанса са създадени специализирани организации и асоциации за защита и опазване на културни съкровища. Една от най-известните асоциации е Академия дей Линчеи, основана през 1507 г. във Флоренция, която е посветена на науките, изкуствата и литературата, а също има за цел да опазва и защитава културното наследство.

През този период се появяват много известни художници и скулптори, като Микеланджело, Рафаело и Леонардо да Винчи. Те създават произведения на изкуството, които се превръщат в символи на епохата. Освен това, Ренесансът е свидетел на подновен интерес към класическата култура и изкуство. Архитектите създават сгради в стила на античността, а художниците – произведения на изкуството в духа на класическата епоха.

През епохата на Ренесанса, защитата на културните ценности става организирана и систематична. Създават се специални организации и сдружения за опазване и защита на културното наследство. Приети са множество закони, забраняващи разрушаването на културни обекти и художествени паметници по време на военни операции.

През модерния период (16-18 век) защитата на културните ценности по време на война става все по-предизвикателна, тъй като военните конфликти стават все по-разрушителни и обхващат по-големи територии. Въпреки това, през този период са създадени нови организации и закони за опазване и защита на културните ценности. По време на войните на модерната епоха са създадени специални комитети и комисии за защита и опазване на културни обекти и художествени паметници. Например във Франция през 17 век е създадена Комисията за опазване на архитектурните паметници, а в Швеция през 18 век - Комитетът за опазване на културните ценности.

Един от основоположниците на международно-правната наука, Алберико Джентили, е първият, който повдига въпроса за защитата на предмети на изкуството в своя труд „За военното право“. Хуго Гроций, бащата на европейското право също ефективно повдига този въпрос, възразявайки срещу унищожаването на предмети, несвързани с военни операции по време на война.

По време на Наполеоновите войни започва масовото и систематично плячкосване на най-големите световни колекции от произведения на изкуството и изнасянето им във Франция. Огромен брой културни съкровища са донесени във Франция от Италия, Испания, Прусия, Австрия, Египет и други страни. След поражението на Наполеон, по решение на Виенския конгрес от 1814-1815 г., някои от тях са върнати в страните, от които са били отнесени.

По-близо до съвременните времена, специфични правила, насочени към опазването на културните паметници, вече се съдържат в Брюкселската декларация за военното право, приета на конференция, свикана по инициатива на Русия през 1874 г. Тази декларация постановява, че всяко изземване, както и умишленото унищожаване или повреждане на образователни, научни и художествени институции, паметници и художествени и научни произведения ще се преследва от властите. Тази декларация, за първи път в международно-правната практика, предвижда възможността за някакъв вид отговорност за щети на културни ценности. Въпреки че декларацията не е ратифицирана, приемането ѝ изиграва определена роля в развитието на международните норми относно законите и обичаите на войната.

През 1899 г. се провежда така наречената Първа Хагска мирна конференция, също свикана по инициатива на Русия. От документите, разработени там, особено

значение има Конвенцията[36] за спазване на законите и обичаите на сухопътната война, подписана от 24 държави.

През 1907 г. се провежда Втората Хагска конференция. На тази конференция е приета Конвенцията за зачитане на законите и обичаите на сухопътната война. Хагската конвенция от 1907 г. е първото международно споразумение, забраняващо унищожаването на културни паметници и тяхната конфискация по време на военни действия, което също така оказва значително влияние върху института на реституцията. На Втората мирна конференция в Хага през 1907 г. конвенциите са финализирани и влизат в историята като Хагските конвенции за зачитане на законите и обичаите на войната. Тези конвенции имат пряко въздействие върху институцията за реституция на културни ценности.

Що се отнася до защитата на културните ценности и обекти в мирно време, това все още не е било въпрос на международното право.

Първата световна война е нанесла значителни щети на културните ценности и паметници в Европа. Регистрирани са редица нарушения на установените международни норми. Въпреки това, предвид военната ситуация, по това време не са правени опити за подобряване на правната рамка за защита на културните ценности.

Трагичният опит от Първата световна война демонстрира необходимостта от по-нататъшно развитие на международно-правните норми за защита на културните ценности по време на въоръжени конфликти. През 1918 г., докато военните действия все още продължават, Холандското археологическо дружество подготвя и разпространява доклад до други страни, призоваващ за регулиране на защитата на историческите и художествените паметници по време на война чрез сключване на специална конвенция, и предлага проект на такава конвенция. В него се предлага цели градове, съдържащи значителни културни ценности (например Рим, Париж, Флоренция, Венеция и Брюж), да бъдат обявени за демилитаризирани, за да се гарантира тяхното запазване по време на войната. Предвижда се такива градове да служат и като временни складове за движими културни ценности.

През 1919 г. в Париж се провеждат мирни конференции за разрешаване на въпроси, свързани със защитата и опазването на културните ценности, възникнали в резултат на Първата световна война. Парижките мирни договори от 1919 г. съдържат предимно разпоредби относно отговорността за нарушения на правилата на войната, включително нарушения на правилата за защита на културните ценности и предмети.

Едва през есента на 1938 г. проект на конвенция, базиран на доклад на видния белгийски юрист Шарл дьо Вишер, е представен на Съвета и Асамблеята на Обществото на народите, но той не е разгледан. Втори проект е изготвен през 1939 г., но войната предотвратява приемането му. По този начин Обществото на народите не успява да изпълни мисията си. Предложението за договор за защита на културните ценности сполетя същата съдба като много други благородни инициативи, първоначално подкрепени от тази международна организация.

[36] Конвенцията е международно споразумение по конкретен въпрос

В рамките на това движение е редно да се подчертае предложението за защита на културните ценности по време на война, както и в мирно време, изказано през 20-те години на миналия век от известния руски художник Николай Рьорих. Предложеният от него договор предизвиква широко обществено движение в защита на културните паметници, което играе далеч по-значителна роля от самото подписване на договора през 1935 г. Идеите на Рьорих впоследствие формират основата на Хагската конвенция от 1954 г.

Н. К. Рьорих упорито се бори срещу унищожаването на художествени съкровища и активно призовава за защита на паметниците на древното руско изкуство. В поредица от картини, създадени преди Първата световна война, той символично изобразява разрушенията и бедствията, които войната носи на мирните градове и културните паметници. Проектът на договор, заедно с обръщението на художника към правителствата и народите на всички страни, е публикуван през 1929 г. на различни езици и придобива световна слава.

Важно е да се отбележи, че идеята на Рьорих е намерила широк отзвук сред международната общност. Ромен Ролан, Бернард Шоу, Алберт Айнщайн, Х. Г. Уелс, Морис Метерлинк и Томас Ман са се изказали в подкрепа на Пакта. Договорът за защита на художествените и научните институции и историческите паметници, подписан във Вашингтон от Съединените щати и 20 латиноамерикански държави, стана известен в международната правна литература като Пактът на Рьорих[37]. Често е наричан Вашингтонски пакт или Пакт за мир.

След сключването на договора от 1935 г. няколко държави приеха резолюции в подкрепа на Пакта Рьорих. В Индия литературното дружество в Бенарес прие специална резолюция през ноември 1938 г. В Париж, преди избухването на Втората световна война, Френският обществен комитет на Пакта Рьорих изпрати предложения до посолствата на няколко европейски държави за приемане на Пакта. Договорът от 1935 г. представлява интерес от гледна точка на формирането на международно-правни норми относно защитата на културните ценности.

След края на Втората световна война, която доведе до унищожаването на огромен брой от най-великите културни съкровища, необходимостта от международно споразумение за защита стана очевидна за цялото прогресивно човечество.

Основната международна междуправителствена организация, която се занимава с широк кръг от въпроси, свързани с международното и научно сътрудничество, включително защитата на културните ценности, е Организацията на обединените нации за образование, наука и култура (ЮНЕСКО). Дейността на ЮНЕСКО се простира до почти всяка страна по света. Тя е създадена в Лондон през 1945 г. на конференция на 44 държави. Нейните членове включват 194 държави по целия свят.

[37] Пактът Рьорих, наричан още пакт на Знамето на Мира и Вашингтонски пакт, както и Договор за охрана на художествените и научни учреждения и исторически паметници, подписан на 15 април 1935 година във Вашингтон

През 1954 г. ЮНЕСКО свиква международна конференция, която се провежда в Хага от 21 април до 14 май 1954 г. На конференцията, на която присъстват 56 държави, включително Съветския съюз, Унгария, Полша, Румъния и Чехословакия, е подписана Хагската конвенция за защита на културните ценности в случай на въоръжен конфликт, както и едноименният протокол и резолюции. Тридесет и седем държави подписват Конвенцията, а 21 - Протокола.

Хагската конвенция от 1954 г. е първото универсално международно споразумение, което консолидира множество норми, предвиждащи защита на културните ценности в случай на въоръжен конфликт. Докато тези норми преди това са се съдържали в различни международни договори или са съществували като прецеденти, понякога противоречиви, сега те са консолидирани в единен инструмент, чието приемане се счита за важна стъпка в развитието на международното право.

При сключването на това споразумение държавите изхождаха от факта, че културните ценности са претърпели сериозни щети по време на Втората световна война и че постоянното развитие на военните технологии създава допълнителна заплаха от тяхното унищожаване.

Три основни принципа се съдържат в преамбюла на конвенцията. Според *първия принцип*, „щетите върху културните ценности на който и да е народ представляват щети върху културното наследство на цялото човечество, тъй като всеки народ прави своя принос към световната култура". Според *втория принцип*, страните-членки на конвенцията са решили да предприемат „всички възможни мерки за защита на културните ценности". Според *третия принцип*, за да се гарантира ефективността на защитата на културните ценности, такава защита трябва да се организира в мирно време чрез приемането както на национални, така и на международни мерки.

Конвенцията от 1954 г. предвижда използването на специална отличителна емблема за културни ценности под специална защита. Тази емблема се състои от синьо-бял щит, заострен в долната част, разделен на четири части.

По този начин, предложеният от Рьорих символ е заменен с друг. Трябва да се отбележи обаче, че за разлика от символа на Рьорих, който изразява конкретна идея, както беше обсъдено по-горе, приетият символ е с чисто утилитарен характер – експертите от онова време са предполагали, че той ще бъде ясно видим от самолети. Конвенцията от 1954 г. говори и за връзката си с договора от 1935 г., че Конвенцията допълва Пакта на Рьорих (член 36) и че отличителният знак на Конвенцията замества Знамето на мира само в случай на въоръжен конфликт.

Източници на стандарти за защита на културните ценности включват:

✓ Конвенция за защита на културните ценности в случай на въоръжен конфликт (1954 г.);

✓ Конвенцията за мерките за забрана и предотвратяване на незаконния внос, износ и прехвърляне на собствеността върху културни ценности (1970 г.);

✓ Конвенция за защита на световното културно и природно наследство, приета на 17-ата сесия на ЮНЕСКО на 16 ноември 1972 г.;

- ✓ Конвенция на УНИДРОА за откраднати или незаконно изнесени културни ценности (1995 г.);
- ✓ Международна конвенция за опазване на нематериалното културно наследство (2003 г.).

Най-важният инструмент по въпросите на опазването на културните ценности е Конвенцията за защита на световното културно и природно наследство, приета на 17-ата сесия на ЮНЕСКО на 16 ноември 1972 г.Тя направи значителен принос за развитието на международно-правни норми за защита на културните ценности в мирно време. Основното съдържание на тази Конвенция от 1972 г. се състои от мерки за предоставяне на международна помощ за защита, опазване, популяризиране или възстановяване на културни ценности.

Международните стандарти за защита на културните ценности определят приоритетите, целите и задачите във вътрешната и външната политика на държавите. Прилагането на международните стандарти за защита на културните ценности е свързано със създаването на механизъм за такова прилагане в рамките на държавата.

Изпълнението на международните задължения на национално ниво, постигнато чрез включването на международно-правни норми за защита на културните ценности във вътрешноправни актове, се осъществява не само чрез прякото им преобразуване в отделни разпоредби, но и чрез подписването и ратифицирането от държавите на международни конвенции, споразумения и договори, съдържащи тези норми. Трябва да се отбележи, че при прилагането на международния опит в организирането на защитата на културните ценности, държавите трябва да вземат предвид както собствените си интереси и национални особености, така и интересите на други държави.

Изводи:

1. Произходът и регулирането на защитата на културните ценности са изминали дълъг път на развитие, усъвършенстване и обновление. Историята на развитието на международно-правната защита на културните ценности показва закономерности във възникването на правни норми, обусловени от практически нужди, и може да бъде разделена на няколко най-важни етапа: Античност, Средновековие (преди Ренесанса); началото на Ренесанса до първите опити за международно-правното регулиране (края на 19 век); международно правно регулиране по време на Първата световна война; от Първата световна война до края на Втората световна война и до наши дни.

2. През цялата човешка история културните съкровища са били обект на разрушение, унищожение и повреди в резултат на войни, природни бедствия, терористични атаки и други форми на насилие. Въпреки това, още от древни времена хората са разбирали важността на опазването на културното наследство и са създавали закони, установявали мерки и правила за неговата защита.

3. Историята ясно показва, че независимо колко съвършени са международно-правните норми, приети за защита на културните ценности, те не могат да решат тези проблеми в приемлива степен. Съществуват многобройни примери за това как

тези норми са били пренебрегвани по време на въоръжени конфликти и цинично заобикаляни за егоистични цели в мирно време.

4. За да се запази културното наследство както на отделна страна, така и на цялото човечество, е необходимо, освен усилията за създаване на нормативен инструмент за културна защита, да се обърне специално внимание на многостранния процес на култивиране на човечността у хората. Само развитието на това морално качество може да доведе до необратими резултати при решаването на жизненоважния въпрос за запазването на най-добрите постижения на човешкото творчество.

5. Въпросите, свързани със защитата на културните ценности, възникват още в древността, но едва в началото на 20-ти век тези въпроси са формулирани и кодифицирани в Хагските конвенции, които забраняват унищожаването на паметници на културата. С ускоряването на глобализацията, нарастването на националната и културната идентичност и защитата на интересите на националните малцинства, се разширява и обхватът на предизвикателствата пред институциите на ООН, чиято основна задача е да защитават обектите на културното наследство от оскверняване, унищожаване и повреждане. Опазването и защитата на културните ценности е неразделна част от международното културно сътрудничество, без което не може да се осигури взаимно разбирателство между народите.

Използвана литература:

1. Богуславский М.М., Монография „Культурные ценности в международном обороте: правовые аспекты", М. Норма, 2012, 416 с.
2. А. С. Соколова, История правовой защиты культурных ценностей, https://lib.herzen.spb.ru/text/sokolova_118_320_325.pdf?ysclid=mr389419st396704829
3. Международная охрана культурных ценностей, https://culturaspb.ru/index.php/2005-god/mezhdunarodnaya-okhrana-kulturnykh-tsennostej
4. П.А.Костюкова, Международные стандарты в области защиты культурных ценностей, https://cyberleninka.ru/article/n/mezhdunarodnye-standarty-v-oblasti-zaschity-kulturnyh-tsennostey?ysclid=mr390lppav25232711
5. Велико П. Петров, Учебно пособие „Основи на държавата и правото – .приложение във военната сфера" (глава втора: Международно Хуманитарно Право), Издателски комплекс на НВУ „В. Левски, Велико Търново, 2023 г., ISBN 978-954-7530-369-1
6. Конвенция за защита на културните ценности в случай на въоръжен конфликт (сключена в Хага на 14 май 1954 г.)
7. Конвенция за мерките за забрана и предотвратяване на незаконния внос, износ и прехвърляне на собственост върху културни ценности от 14 ноември 1970 г.

8. Конвенция за защита на световното културно и природно наследство, приета на 17-ата сесия на ЮНЕСКО на 16 ноември 1972 г.
9. Конвенция на УНИДРУА за откраднати или незаконно изнесени културни ценности (сключена в Рим на 24 юни 1995 г.)
10. Международна конвенция за опазване на нематериалното културно наследство (сключена в Париж на 17 октомври 2003 г.)
11. Конвенция за защита на световното културно и природно наследство (сключена в Париж на 16 ноември 1972 г.)
12. Пактът Рьорих, наричан още пакт на Знамето на Мира и Вашингтонски пакт, както и Договор за охрана на художествените и научни учреждения и исторически паметници, подписан на 15 април 1935 година във Вашингтон
13. Хагска (IV) конвенция относно законите и обичаите на сухоземната война от 1907 година
14. Втори протокол към Хагската конвенция от 1954 г. за защита на културните ценности в случай на въоръжен конфликт, 1999 г.
15. Договор „За защита на сгради и съоръжения, служещи за религиозни, образователни и благотворителни цели“ от 1935 г.
16. Споразумение за сътрудничество и взаимопомощ при задържане и връщане на културни ценности, незаконно внесени през държавните граници (Пловдив, 22 април 1986 г.).
17. Споразумение за сътрудничество между митническите служби при задържане и връщане на незаконно изнесени и внесени културни ценности (Москва, 15 април 1994 г.)

ANTI-TANK MISSILE COMPLEXES IN MODERN ARMED CONFLICTS

Veliko P. Petrov

Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, veliko_pp@abv.bg

***Abstract**: Today, anti-tank weapons allow small units to destroy heavily armored vehicles at considerable distances, which changes the tactics of conducting combat operations. Anti-tank complexes are a set of weapons, control systems and ammunition designed to defeat tanks, infantry fighting vehicles, armored personnel carriers and other armored targets. Today, anti-tank guided missiles remain the main precision-guided weapon at the tactical level, used against various armored targets, as well as lightly armored vehicles, vessels, aircraft, field fortifications, buildings and infantry - whether hidden or in the open. Thanks to cheap technology and huge surpluses from the Cold War, second-generation ATGMs are likely to remain in service and production in some countries, complementing more advanced ATGMs and barrage munitions. It is expected that these older systems will receive improvements in capabilities, which will allow them to operate with acceptable effectiveness at least until the mid-2030s of the 21st century.*

The ATGM arsenals of many countries will consist of a combination of simpler and cheaper ATGMs, barrage munitions, and advanced ATGMs with improved capabilities. While not ideal, this configuration offers several advantages. For example, second-generation ATGMs are more affordable and ready for mass production, while personnel, including reservists, can be trained to use them more easily. The latest generation ATGMs will continue to develop, although they will be produced and delivered in limited quantities. Perhaps the most significant factors contributing to this limitation are their complex designs, higher production costs, and longer production cycles.

While the technological advantages of newer generations of anti-tank missiles (ATGMs) are undeniable, they raise concerns from a military perspective. The increasing complexity of these systems, coupled with the often higher training requirements for calculations, risks turning a key tactical weapon – originally designed to be widespread, affordable and disposable – into an expensive, scarce and difficult-to-replenish asset, potentially difficult to use during a large-scale conflict.

Anti-tank guided missiles have revolutionized modern battlefield tactics, offering unparalleled precision and adaptability against armored threats. As technology advances, anti-tank missiles will play an increasingly important role in shaping the future of warfare. The continued evolution of ATGMs promises to redefine the balance of power on the battlefield, making them an indispensable asset in current and future conflicts.

***Keywords:** anti-tank weapons, anti-tank missile systems, anti-tank guided missiles*

ПРОТИВОТАНКОВИТЕ РАКЕТНИ КОМПЛЕКСИ В СЪВРЕМЕННИТЕ ВЪОРЪЖЕНИ КОНФЛИКТИ

Велико П. Петров

Съвременните въоръжени конфликти показват, че брониранатa техника продължава да бъде основен елемент на Сухопътните войски. Танковете осигуряват висока огнева мощ, защита и мобилност, но тяхната ефективност все

по-често се поставя под въпрос поради развитието на съвременните противотанкови комплекси. Днес противотанковите оръжия позволяват на малки подразделения да унищожават тежко бронирана техника на значителни разстояния, което променя тактиката на водене на бойните действия. Противотанковите комплекси представляват съвкупност от оръжия, системи за управление и боеприпаси, предназначени за поразяване на танкове, бойни машини на пехотата, бронетранспортьори и други бронирани цели. Тези комплекси са основни елементи от съвременната противотанкова отбрана и могат да бъдат преносими, монтирани на бойни машини или интегрирани в роботизирани системи.

До въвеждането на противотанковите управляеми ракети (ПТУР), противотанковите оръжейни системи разчитаха на стрелковите умения на оператора (мерача) и наличието на пряка видимост, което е рядка комбинация при активните бойни действия. ПТУР не само елиминират тези изисквания, но и разширяват обхвата на бой и позволяват непряк огън благодарение на бордовите си системи за задвижване и насочване. Тези характеристики позволяват на ракетата да извършва сложни маневри, като например удар отгоре надолу, избягване на препятствия или следване на „пияна“ траектория на полета, за да парира контрамерки с пряк удар. Те могат да носят по-тежки бойни глави и да нанасят много повече поражения на целта в сравнение с други оръжейни системи.

От въвеждането им през 50-те и 60-те години на миналия век, ПТУР са се развили от чисто противотанкови средства до универсални оръжия, способни да поразяват широк спектър от цели, включително бронирани бойни машини, нисколетящи самолети и укрепления. Днес ПТУР са на въоръжение в множество страни по света, като непрекъснато се разработват и произвеждат по-нови поколения от тези системи.

Важно е да се подчертае, че по-ранните очаквания, според които различни видове дронове ще заменят или ще поемат функциите на противотанкови ракети (ПТУР) на бойното поле, изглежда са били преувеличени. Опитът от продължаващите конфликти в Украйна и в Близкия изток показва, че тези видове оръжия успешно съществуват едновременно и се допълват взаимно, въпреки донякъде припокриващите се възможности.

Според пазарни анализи, очаква се световният пазар на преносими противотанкови оръжия да нарасне с 2,98% до 5% между 2025 и 2031 г. Анализът на IMARC Group определя най-ниската очаквана цифра, като прогнозира, че световният пазар на противотанкови ракети (ПТРК) може да достигне 4,3 милиарда щатски долара до 2033 г., със сложен годишен темп на растеж (CAGR) от 2,98% от 2025 до 2033 г. От своя страна, доклад на Research and Markets, публикуван през януари 2025 г., очаква пазарът на ПТРК да достигне 9,6 милиарда щатски долара до 2030 г., със CAGR от 5,0 % между 2023 и 2030 г .Други аналитични компании като цяло следват тези очаквания, прогнозирайки цифри за растеж между 3,35% (Market Research Future) и 4,1% (Coherent Market Insights).

Системите, които понастоящем са на въоръжение в различни страни по света, варират значително по възраст и поколение. Докато някои страни все още използват системи от първо поколение, като например 9М14 Малютка от

съветската епоха или нейните модернизирани производни, други вече са приели така наречените системи от пето поколение, като например Akeron MP на MBDA и Spike LR2 и Spike NLOS на Rafael. Гръбнакът на противотанковите ракетни оръжия в повечето страни обаче се състои от преносими и монтирани на превозни средства системи от второ и трето поколение.

Разликите между поколенията не винаги са категорични и имат голямо поле за дискусия. Възможностите могат да се различават значително между системите от едно и също поколение или между по-ранни и по-късни версии на ракети в рамките на едно и също семейство. Например, руската ПТУР „Корнет“ се счита от някои за система от трето поколение, въпреки че разполага с полуавтоматична система за насочване по линията на видимост (SACLOS), по-типична за ПТУР от второ поколение . От друга страна, ракетата 9M133M-2 на семейство „Корнет“ има обхват от 8 km и мощна тандемна бойна глава, способна да порази над 1300 mm еквивалент на валцувана хомогенна броня. В допълнение към това, пусковата станция е снабдена с термовизионен мерник за улесняване на насочването през нощта. Такива характеристики са по-често свързвани със системи от трето поколение.

Примери за системи от второ поколение включват: 9K115 «Метис», 9K111 «Фагот», 9K111-1 «Конкурс», семейство 9K133 «Корнет», семейство «Скиф» (Стугна-П), семейство BGM-71 TOW, семейство «Милан» и други. Въпреки че някои от тези системи са въведени през 70-те и 80-те години на миналия век, те остават в експлоатация и са непрекъснато модернизирани, за да се удължи експлоатационният им живот и да се подобрят бойните им възможности. Един от последните случаи на подобно подобрение е руската система 9K111-1M «Конкурс-М», която получи възможност за дистанционно управление, както съобщи концерн „Калашников“ на 27 декември 2024 г. Тази функция е предназначена да увеличи оцеляването както на системата, така и на нейния екипаж, а една система за дистанционно управление позволява на оператор на противотанков ракетен комплекс (ПТРК) дистанционно да управлява три пускови установки „Конкурс-М“ последователно през светлата част на денонощието.

Заслужава да се отбележи, че противотанковите ракети от второ поколение са въведени и масово произвеждани предимно по време на Студената война. Днес тези системи остават най-многобройните (с десетки хиляди в излишък) и са рентабилни за производство, като същевременно притежават достатъчна бойна ефективност.

За сравнение, ПТУР от трето поколение включват редица усъвършенствани възможности, които, от една страна, подобряват бойните им характеристики, но от друга, увеличават сложността, както и разходите за поддръжка и производство. Представители на това поколение включват системи като: FGM-148 Javelin, AT-1K Raybolt, Hongjian-12 (HJ-12) и други. Повечето системи със среден обсег от трето поколение са способни да атакуват цели в обхват от няколкостотин метра до над 5 km. Системите, класифицирани като трето поколение, обикновено влизат в експлоатация между 1990 и 2010 г. Те имат няколко общи характеристики, като например заключване преди изстрелване (LOBL), както и възможност за оператора

да избира между директни и повдигнати (атака отгоре) траектории. Тези ракети обикновено са оборудвани и с инфрачервена търсачка за насочване.

Режимът LOBL, наричан още „стреляй и забрави", е може би най-важното развитие, въведено в системите от трето поколение. В сравнение със системите с ръчно командване по линията на видимост (MCLOS) от първо поколение или SACLOS от второ поколение, където операторът трябва да държи мерника върху целта до удара, ПТУР с LOBL позволяват на екипажа бързо да променя позицията си след изстрелване, което увеличава оцеляването и тактическата гъвкавост на екипажите на ПТРК на бойното поле. Подобни нива на безопасност на екипажа от ответен огън обаче могат да бъдат постигнати и при системи от второ поколение, използващи дистанционно управляеми огневи постове SACLOS.

Последната отличителна черта на противотанковите ракети от трето поколение е способността за атака отгоре. Възникнала като решение за противодействие на напредъка в защитата на основните бойни танкове в края на 80-те и 90-те години на миналия век, тя се разпространи през десетилетията и се превърна в стандартен елемент в противотанковите ракети от трето поколение и по-новите им версии. Способността за атака отгоре позволява на ракетата да се насочи към по-слабата броня на покрива на силно бронирана цел, като например танк, като по този начин заобикаля по-голямата част от пасивната му защита.

Таблица 1.Ключови характеристики на избрани противотанкови ракети (ПТРК) от трето поколение

Система	**Страна на произход**	**Максимален обхват (км)**	**Възможност за атака отгоре**	**Режими на стрелба**
FGM-148 Javelin	САЩ	2.5 km (Базов CLU) 4 km (Лек CLU) 4.75 km (Монтиран на превозно средство)	Да	Режим LOBL или „стреляй и забрави"
Тип 01 LMAT	Япония	4 km	Да	Режим LOBL
AT-1K Рейболт	Южна Корея	2,5-3 km	Да	Режим LOBL
HJ-12 Hongjian-12	Китай	4 km (денем); 2 km (нощем)	Да	Режим LOBL

Важно е да се подчертае, че макар някои противотанкови ракети от трето поколение да са били използвани в бойни действия срещу бронирани машини, тези случаи обикновено са включвали технологично по-слаби противници в конфликти с ниска интензивност. Следователно, продължаващият руско-украински конфликт се превърна в първия въоръжен конфликт, в който противотанкови ракети от трето поколение (като FGM-148 Javelin) бяха разположени масово срещу равен противник. Въпреки че възможностите за атака отгоре и режим „стреляй и забрави" се считаха за важни, е трудно да се оцени цялостното им представяне

срещу руски бронирани машини, както и цялостното им въздействие върху войната.

Междувременно някои страни вече са разработили и внедрили противотанкови ракети (ПТУР) от четвърто и пето поколение – в зависимост от използваната класификация – като например Akeron MP на MBDA и Spike LR/LR2, Spike ER/ER2 и Spike NLOS системите на Rafael. Тези ПТУР започнаха да влизат в експлоатация след 2010 г. и обикновено разполагаха с по-усъвършенствани режими, като например възможност за заключване след изстрелване (LOAL), наричана още режим „стрелба и актуализиране". Режимът LOAL позволява на оператора да наблюдава бойното поле в реално време чрез IIR и/или дневната търсачка на снаряда и да актуализира параметрите на полета на целта или ракетата по време на полета, ако е необходимо. Този режим позволява провеждане на бойни действия извън линията на видимост (NLOS).

Илюстративен пример за такава система е OMTAS на турската компания Roketsan, която включва както LOBL, така и LOAL режими. Пусковата установка и ракетата OMTAS са свързани чрез радиочестотна връзка, което позволява на оператора да се насочва към целта, след като ракетата е в полет, както и да превключва целите по време на полет.

Забележително е, че някои класификации определят системите от четвърто поколение като подобни на тези от трето поколение, като основната разлика е връзката за данни между пусковата установка и оператора, позволяваща на оператора да променя параметрите на полета на ракетата, да превключва цели по време на полет или да прекрати мисията, ако е необходимо .

Най-модерните ПТУР до момента принадлежат към пето поколение. Тези системи се отличават със сложни възможности, като например управление от трети страни, което позволява тяхното използване в съвременна мрежово-центрична война. Те също така обикновено са много гъвкави, предлагайки многоплатформена интеграция и многоцелеви тандемни бойни глави с фрагментационни ръкави, способни да поразяват експлозивна реактивна броня (ERA) и броня над 1000 mm RHAe.

ПТУР от пето поколение обикновено се отличават с разширен набор от оперативни режими, включително режими LOBL, LOAL и огън по координати. Режимът „огън по координати" позволява стрелба по предварително определени координати в сценарии без видимост към целта (NLOS). Макар че последният режим не изисква операторът да проследява целта и подобрява оцеляването и маскирането, той е най-подходящ за стационарни цели. Някои системи, като Akeron MP и Spike NLOS на MBDA, позволяват обозначаване на целта от трети страни. Тази възможност означава, че данните за насочване могат да бъдат получени от пилотирани или безпилотни летателни апарати или наземни разузнавателни средства (ISR).

Според производителите, много системи от пето поколение са устойчиви на заглушаване, независимо дали използват оптични канали за данни, които нямат начин да бъдат заглушени, или криптирани радиочестотни (RF) канали за данни, които са доста трудни за заглушаване. Освен това, ПТУР от това поколение могат

да бъдат оборудвани със сложни търсачки, които имат както цветни телевизионни (TV), така и неохлаждани IIR канали, понякога заедно с други сензори.

Таблица 2. Ключови характеристики на избрани противотанкови ракети (ПТУР) от четвърто/пето поколение

Система	Страна на произход	Максимален обхват (км)	Възможност за атака отгоре	Режими на стрелба
FGM-148 Javelin	САЩ	2.5 km (Базов CLU) 4 km (Лек CLU) 4.75 km (Монтиран на превозно средство)	Да	Режим LOBL или „стреляй и забрави"
Тип 01 LMAT	Япония	4 km	Да	Режим LOBL
AT-1K Рейболт	Южна Корея	2,5-3 km	Да	Режим LOBL
HJ-12 Hongjian-12	Китай	4 km (денем); 2 km (нощем)	Да	Режим LOBL

Като знак за посоката, в която се движат нещата, най-новата версия на Spike NLOS на Rafael добави няколко допълнителни забележителни възможности. Първата е режим на залпов изстрел, при който до четири ракети могат да бъдат едновременно изстрелвани и управлявани, докато са във въздуха, от една пускова установка. Втората е възможност за предаване на насочване, при която контролът над ракета може да се прехвърли от една платформа на друга. Тактическата възможност, която това отваря, е оригиналната пускова платформа бързо да се премести или скрие след изстрел, докато втора платформа поема насочването, за да гарантира успешното попадение на целта. Трета възможност е качването на въздушни изображения на целта към пусковата платформа и след това съпоставянето на тези изображения с видеозаписа от самонасочващата система на ракетата. Това може да помогне на огневия екип бързо да разграничи и идентифицира правилната цел[38].

Могат да се идентифицират няколко тенденции в бъдещото развитие на ПТУР и те са:

Първа тенденция: ПТУР се насочват към по-голям обхват, не на последно място, за да запазят своята актуалност спрямо баражиращите боеприпаси. Докато по-голямата част от системите, които са в експлоатация в момента, имат максимален обхват до 5 km, изискванията за бъдещите системи сочат към увеличаване на дистанцията на отстояние.

Например, изискванията за тежката ракетна система за близък бой (CCMS-H), потенциален наследник на семейството BGM-71 TOW, включват максимален обхват от 4,5 km за пряко поразяване и обхват на съвместното поразяване, равен

[38] Spike NLOS – https://www.rafael.co.il/system/spike-nlos/

или по-голям от 8 km. Американската армия иска CCMS-H да запази много от предимствата на TOW, но да има способността да поразява най-модерните противникови танкове на разстояние до 10 000 m . Подобна тенденция може да се наблюдава в нарастващия брой системи за далечен бой Spike ER2 и Spike NLOS, закупени или поръчани по целия свят през последните години.

Както стана очевидно от конфликта в Украйна, системите – както преносими, така и монтирани на превозни средства – с максимален обхват от 4-5 km, действащи близо до противниковите линии, е вероятно да бъдат забелязани от един-единствен разузнавателен комплекс – като разузнавателни дронове – и да бъдат насочени към артилерия, баражиращи боеприпаси или други налични огневи средства много преди да са в позиция да се сблъскат с противника. Разстоянието до 5 km, комбинирано с режима „стреляй и забрави“, някога разбирано като достатъчна мярка за избягване на откриването на противников огън по тях, сега изглежда недостатъчно.

Втората тенденция се обуславя от последните развития в защитата на бронираните бойни машини (ББМ). В отговор на разпространението на противотанкови средства, включително усъвършенствани ракети и баражиращи боеприпаси, военните по целия свят ускориха темпото на внедряване на усъвършенствани защитни решения на бронираните машини. Следователно, способността за поразяване на бронирани машини, оборудвани с усъвършенствани многослойни защитни комплекси, вече става задължителна.

Трета тенденция е нарастващата гъвкавост на противотанковите ракети. Докато по време на Студената война този клас въоръжение се е разглеждал като основно оръжие за поразяване на противниковите бронирани машини, днес спектърът от бойни задачи, изпълнявани от ПТРК, е значително по-широк. Разнообразието от бойни сценарии и оперативни среди, в които се използват ПТРК, също се е увеличило.

Четвърта тенденция: има текущи разработки на възможности, които вероятно ще бъдат въведени в следващото поколение ПТУР или чрез подобрения на съществуващи системи. Например, MBDA представи Ground Warden AI на събитието Eurosatory 2024 - система, задвижвана от изкуствен интелект (ИИ), предназначена да подобри привличането на цели и процеса на вземане на решения за семейството оръжия Akeron MP . Други производители, включително Rafael Advanced Defense Systems, Lockheed Martin и други, също работят по разработването и внедряването на технологии за ИИ и машинно обучение в ракети, включително и ПТУР. Допълнителни подобрения на ПТУР могат да включват способност за роене, споделяне на данни между множество ракети в мрежа, нови задвижващи системи, автономно насочване и пренасочване, както и интеграция с пилотирани и безпилотни платформи.

Изводи:

1. Днес ПТУР остават основно прецизно насочвано оръжие на тактическо ниво, използвано срещу различни бронирани цели, както и лекобронирани машини, плавателни съдове, самолети, полеви укрепления, сгради и пехота – независимо

дали са укрити или на открито. Благодарение на евтините технологии и огромните излишъци от времето на Студената война, ПТУР от второ поколение вероятно ще останат в експлоатация и производство в някои страни, допълвайки по-усъвършенстваните ПТУР и баражиращи боеприпаси. Очаква се тези по-стари системи да получат подобрения във възможностите, което ще им позволи да работят с приемлива ефективност поне до средата на 30-те години на 21-ви век.

2. Арсеналите от ПТУР на много страни ще се състоят от комбинация от по-прости и по-евтини ПТУР, баражиращи боеприпаси и усъвършенствани ПТУР с подобрени възможности. Макар и да не е идеална, тази конфигурация предлага няколко предимства. Например, ПТУР от второ поколение са по-достъпни и готови за мащабно производство, докато разчетите, включително резервистите, може да бъдат обучени да ги използват по-лесно.

3. ПТУР от последно поколение ще продължат да се развиват, въпреки че ще се произвеждат и доставят в ограничени количества. Вероятно най-значимите фактори, допринасящи за това ограничение, са сложните им конструкции, по-високите производствени разходи и по-дългите производствени цикли.

4. Въпреки че технологичните предимства на по-новите поколения противотанкови ракети (ПТУР) са безспорни, те пораждат опасения от военна гледна точка. Нарастващата сложност на тези системи, съчетана с често по-високите изисквания за обучение на разчета, рискува да превърне едно основно тактическо оръжие – първоначално проектирано да бъде широко разпространено, достъпно и за еднократна употреба – в скъп, оскъден и труден за попълване актив, потенциално труден за използване по време на мащабен конфликт.

5. Противотанковите управляеми ракети революционизираха съвременните тактики на бойното поле, предлагайки несравнима прецизност и адаптивност срещу бронирани заплахи. С развитието на технологиите, противотанковите ракети ще играят все по-важна роля в оформянето на бъдещето на войната. Продължаващата еволюция на ПТРК обещава да предефинира баланса на силите на бойното поле, превръщайки ги в незаменим актив в съвременните и бъдещи конфликти.

Използвана литература:

1. Мороговский А. А., Применение противотанковых управляемых ракет в современном общевойсковом бою, https://libeldoc.bsuir.by/handle/123456789/63313
2. Alexey Tarasov, Modern ATGM capabilities, March 2025, https://euro-sd.com/2025/03/articles/42885/modern-atgm-capabilities/
3. Гиренко Александр Анатольевич,Современное состояние и возможные направления развития противотанковых ракетных комплексов сухопутных войск, https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-i-vozmozhnye-napravleniya-razvitiya-protivotankovyh-raketnyh-kompleksov-suhoputnyh-voysk?ysclid=mrm2enek3305945359
4. Marko Radovanović, Aleksandar Petrovski, Saša Smileski, Željko Jokić, Scientific Technical Review, 2023, Vol. 73, No.1(2023), Pages: 26-37,

Analysis Of The Development Of Five Generation Of Anti-Armor Missile Systems
5. I. Bozov, Remotely piloted aircraft systems (RPAS) in service to artillery formations, International Scientific Conference ―“Defense Technologies” DefTech 2022, стр.118-121, ISSN 2367-7902
6. И.Бозов, Оценка на разузнавателните възможности на безпилотни летателни апарати, International Scientific Conference ― “Defense Technologies” DefTech 2021, стр. 124-128, ISSN 2367-7902
7. Доклад на IMARC Group, https://www.imarcgroup.com/anti-tank-missile-system-market
8. Доклад за изследвания и пазари, https://www. Researchandmarkets .com/report/man-portable-anti-armor-weapons #tag-pos-2
9. Market Research Future, https://www.marketresearchfuture.com/reports/anti-tank-guided-missiles-market-40359
10. Съгласувани пазарни прозрения – https://www. Coherentmar ketinsights.com/industry-reports/manned-anti-tank-guided-missile-system-market?utm_source=chatgpt.com
11. Spike NLOS – https://www.rafael.co.il/system/spike-nlos/
12. Army Wants to Replace the Cold War-Era TOW Missile with a New Longer-Range Tank Killer, https://www.military.com/daily-news/2021/04/08/army-wants-replace-cold-war-era-tow-missile-new-longer-range-tank-killer.html
13. Ground Warden AI system, https://www.youtube.com/watch?v=9Zh-C-OyvgA

THE COMBAT EMPLOYMENT ON ANTI-TANK MISSILE COMPLEXES IN MODERN ARMED CONFLICTS

Veliko P. Petrov

Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, veliko_pp@abv.bg

***Abstract**: Modern armed conflicts are characterized by the widespread use of armored vehicles, which places an emphasis on effective countermeasures. Anti-tank guided missile systems (ATGMs) and anti-tank rocket launchers (RPGs) have become key tools for infantry in the fight against armored vehicles, significantly changing the balance of forces on the battlefield.*

The role of anti-tank units in defeating enemy armored vehicles has not decreased; targets are redistributed depending on the tactical and technical characteristics of anti-tank guns (ATGMs, SPGs). Barrel anti-tank artillery began to perform fire missions mainly from covered firing positions. The fight against enemy armored targets at the front end is almost entirely entrusted to the crews (crews) of ATGMs (portable ATGMs) and anti-tank rocket launchers (SPGs and RPGs).

Modern anti-tank guided missiles and associated systems (UAVs) have not rendered tanks useless, but they have dramatically increased the risks of their use, especially without adequate infantry cover, reconnaissance, and electronic warfare and active defense support. They have provided infantry and light units with a powerful means of deterring and destroying armored vehicles, capable of inflicting significant losses even on superior opponents and radically influencing combat tactics. The struggle between armor and the means to defeat it continues to be a dynamic arms and tactical race. In modern warfare, anti-tank guided missiles have emerged as an advanced technology that has redefined battlefield tactics and caused major changes in traditional strategies for the use of armored vehicles. With their precision, portability, and advanced targeting capabilities, ATGMs have become a key asset for militaries around the world, influencing the dynamics of armored warfare in modern combat. Anti-tank missiles are increasingly being paired with unmanned aerial vehicles (UAVs) for guidance, with the drones providing real-time reconnaissance and laser guidance, enabling combat beyond the line of sight.

Anti-tank missile systems have revolutionized modern battlefield tactics, offering unparalleled precision and adaptability against armored threats. As technology advances, ATGMs will play an increasingly important role in shaping the future of warfare.

***Keywords:** anti-tank weapons, anti-tank missile systems, anti-tank guided missiles*

БОЙНО ИЗПОЛЗВАНЕ НА ПРОТИВОТАНКОВИТЕ СРЕДСТВА В СЪВРЕМЕННИТЕ ОПЕРАЦИИ

Велико П. Петров

Съвременната военна операция е комплексна, многодомейнна (суша, въздух, море, космос, киберпространство) и синхронизирана кампания. Тя обединява военни, дипломатически, икономически и информационни ресурси за постигане на конкретни стратегически или тактически цели, основани на принципа на мрежово-центричната война и високоточни удари.

Операцията е основна форма за използване на въоръжените сили, представляваща отделно действие или съвкупност от съгласувани по цел, място и време действия, предназначени за постигане на желан ефект или крайно състояние. В най-общ смисъл всяко действие или съвкупност от действия може да бъде разглеждано като операция от гледна точка на използването на въоръжените сили. В една операция могат да бъдат включени по-малки (подчинени) операции, които допринасят за постигане целите на операцията[39].

Съвременните въоръжени конфликти се характеризират с широкото използване на бронирани машини, което поставя акцент върху ефективните мерки за противодействие. Противотанковите управляеми ракетни комплекси (ПТРК) и реактивните противотанкови гранатомети (РПГ) са се превърнали в ключови инструменти за пехотата в борбата с бронирани машини, променяйки значително баланса на силите на бойното поле.

Противотанковите средства са специализирани системи за борба с бронирани машини, включващи преносими ракетни комплекси, противотанкови оръдия, реактивните противотанкови гранатомети, мини и дронове. Те използват кумулативни заряди за пробиване на бронята и са основен елемент от съвременната отбрана.

Комплексът от дейности и мероприятия по борбата с танковете и другите бронирани средства се нарича противотанкова отбрана. За изпълнение на задачите на противотанковата отбрана се формират елементи от бойния ред, а те от специални подразделения, части и съединения наречени противотанкови.

Разглеждаме усъвършенстването на противотанковите огневи средства през последните 16 години по периоди, както следва:

В периода от 2010 г. до 2014 г. се наблюдава доминирането на остарелите противотанкови огневи системи и появата на нови заплахи. Основни противотанкови огневи системи през този период са:

1) Широко са използвани съветски системи от второ поколение (9К111 Фагот, 9К113 Конкурс) и техни копия, както и огромен брой РПГ-7 с различни модификации.

2) Западните армии и техните съюзници са въоръжени с ПТУР FGM-148 Javelin (САЩ) и Spike (Израел).

Тактики на използване в конфликти (Сирия, Ирак, Източна Украйна): Асиметрични конфликти: бойци от нередовни формирования (ИДИЛ, бунтовнически групировки) широко използваха РПГ-7, ПТРК „Фагот" и ПТРК „Конкурс" срещу правителствените сили, често устройвайки засади в градски райони или в пресечена местност. Ефективността срещу съвременни танкове (Т-72Б, Т-90) е ограничена поради динамична защита (ДЗ) и слабо обучените артилеристи.

[39] Доктрина на Въоръжените сили на Република България, Издание (Б), София 2025, Национална публикация на въоръжените сили на Република България НП – 01, МО, въведена със Заповед на министъра на отбраната № ОХ-1126/03.12.2025 г., стр. 33

Отбрана: Редовните армии (напр. украинските въоръжени сили в началото на конфликта в Донбас) използваха остарели противотанкови ракети (9К111 Фагот) предимно в отбрана, от предварително подготвени позиции. Недостатък беше уязвимостта на екипажа при продължително насочване по цел. В този период ограничено се използваха съвременни системи като Javelin и Spike, предимно от специални сили (напр. кюрдските сили „Пешмерга" срещу ИДИЛ). Техните ключови предимства като режимът „стреляй и забрави" и атаката отгоре бяха доказани, но не бяха широко използвани.

Изводи от този период: остарелите ПТРК и РПГ останаха основата на противотанкова отбрана на пехотата, но ефективността им срещу съвременни танкове с динамична защита беше недостатъчна. Съвременните противотанкови ракети се използваха пестеливо, но демонстрираха висок потенциал.

В периода от 2015 г. до 2019 г. се наблюдава масово постъпване на съвременни ПТРК и тактически иновации. Основни противотанкови огневи системи през този период са:

1) масирани доставки на ПТРК Javelin (Украйна), Spike (Саудитска Арабия, ОАЕ – конфликтът в Йемен) и NLAW (за Великобритания, а по-късно за Украйна).

2) появата и използването на по-модерни руски системи от трето поколение: 9К135 Корнет (разстояние до 10 km, тандемна бойна глава, лазерно-лъчево насочване) от нередовни сили (Сирия, Либия). Широко разпространено използване на РПГ-29 Vampire и РПГ-32 Hashim с тандемни бойни глави.

Тактики на използване: Активна отбрана и мобилни групи: преход от статична отбрана към създаване на мобилни противотанкови групи (3-5 души с ПТРК) на джипове или бронетранспортьори. Това позволява бърза смяна на позицията след стрелба, намалявайки уязвимостта от ответен огън (Сирия, Йемен). Използване на релефа и инфраструктурата: майсторско използване на градската застройка (мазета, горни етажи), гори и обратни склонове на хълмове за скрит подход, изстрелване на ракети и отстъпление. Това е особено характерно за украинските въоръжени сили в Донбас. Комбинирани атаки: комбинация от ПТУР или РПГ с минохвъргачен огън, импровизирани взривни устройства или групи за потискане на пехотното прикритие на танковете и отвличане на вниманието.

Борба с активната защита (АЗ): широко използване на тандемни бойни глави (ПТРК Корнет, РПГ-29, РПГ-32) за преодоляване на противодействие на динамичната защита. Тактика на двоен удар: първият изстрел с РПГ за задействане на динамичната защита, вторият с ПТУР за пробиване на отслабената броня.

Изводи от този период: масовото въвеждане на съвременни ПТРК (Javelin, Kornet) значително увеличи възможностите на пехотата. Тактиките станаха по-гъвкави и агресивни, базирани на мобилността и използване на местността. Тандемните бойни глави се превърнаха в стандарт за противодействие на динамичната защита.

В периода от 2020 г. до 2026 г. се наблюдава ерата на дроновете, активната отбрана и хиперзвуковите ракети.

Основни противотанкови огневи системи и технологии през този период са:

1) Интеграция с безпилотни летателни апарати (БЛА): БЛА се превръщат в неразделна част от противотанковия бой, от микро-БЛА за разузнаване на цели до атакуващи БЛА (като Switchblade 300/600 и Lancet-3), носещи кумулативна бойна глава и действащи като противотанкови ракети за еднократна употреба.

Развитие на активната защита на бронираните машини: широкото въвеждане на комплекси за активна защита от ново поколение (Arena-M, Afganit, Trophy, Iron Fist)[40], способни да прехващат не само РПГ, но и ПТУР. Това рязко намали ефективността на единичните изстрелвания на ПТРК от по-стар тип.

Нови противотанкови ракети (ПТУР): приемането и използването на най-новите системи: американската FGM-148 Javelin с модернизирана бойна глава, руската 9M133M Kornet-EM с увеличен обсег и термобарична бойна глава, и израелската SPIKE LR2. Появата на леки ПТРК за еднократна употреба (като NLAW, PzF 3-IT) с повишена ефективност срещу активна защита.

Миниатюризация и достъпност на дроновете: възходът на търговските FPV дронове, оборудвани с кумулативна бойна глава, които се превърнаха в масово произвеждано и евтино противотанково оръжие за нередовните сили (Украйна, Судан).

Тактики на използване (войната в Украйна): Мрежоцентричност: интегриране на ПТРК в единна система за разузнаване (БЛА, радари, пешеходни патрули) и управление на огъня чрез таблети/цифрови карти[41]. Позволява бързо насочване на ПТУР към открити цели. Огневи чували и окопна война: организиране на сложни системи от засади с кръстосан огън от ПТРК от различен тип (далекобойни Корнети + близкобойни Джавелини и NLAW + FPV дронове), прикрити от минохвъргачки и картечници. Целта е да се гарантира унищожаването на танкове с първото попадение, на които са пробили активната им защита.

Приоритет на тилови проекции и слабите места: екипажите целенасочено се стремят да поразят танка в задната част, отстрани или покрива на купола/моторното отделение, където бронята е по-слаба и активната им защита е по-малко ефективна. FPV дроновете атакуват предимно в горната полусфера.

Противодействие на активната защита: използват се няколко подхода: масиран залп (няколко ПТУР/РПГ/дрона едновременно); атака от изключително близко разстояние (преди да се задейства активната защита); използване на ПТУР с пикираща траектория отгоре (Джавелин); използване на FPV дронове, атакуващи от неочаквани посоки[42].

Изводи от този период: противотанковата борба се е превърнала във високотехнологично мрежово-центрично противоборство. Безпилотните летателни апарати се превърнаха в ключов елемент. Ефективността на единична противотанкова ракета срещу танк със съвременна активна защита рязко намаля, което изисква комбинирано използване на различни оръжия (ПТУР, РПГ, дронове,

[40] Center for Strategic & International Studies (CSIS): Active Protection Sys- tems (2023), https://www.csis.org/.

[41] Royal United Services Institute (RUSI): Drone War in Ukraine (2023), https://rusi.org/.

[42] Oryxspioenkop: Overcoming APS in Ukraine (2023), https://www.oryxspioenkop.com/

артилерия) и сложни тактики. Миниатюрните дронове за атака се превърнаха в ново, широко разпространено и страховито противотанково оръжие.

Еволюцията на противотанковите средства в съвременните конфликти демонстрира постоянна технологично и тактическо противоборство на „меч и щит". От остарели системи и прости тактики на засада (2010-2014 г.), конфликтите преминаха към ерата на масово използване на високоточни ПТУР от трето поколение и тандемни бойни глави, гъвкави мобилни групи и сложни тактики за маскировка и атака (2015-2019 г.). Настоящият етап (2020-2026 г.) се характеризира с интегрирането на противотанкови ракети (ПТУР) в мрежата за разузнаване и управление, доминирането на БЛА като разузнавателни и ударни средства, широкото въвеждане на ефективна активна защита на танковете и разработването на ответни действия за развитие на тактиката за тяхното преодоляване (масирани залпове, дронове с FPV, атаки отгоре и от близки разстояния)[43].

Въпреки развитието на технологиите, ключовите фактори за успех остават:

- ✓ обучението и подготовката на екипажа: способността за бързо откриване на цел, избор на позиция, точно изстрелване и незабавна промяна на позицията; ефективно разузнаване: откриване на цели, преди да достигнат линията на атака (БЛА, наземни постове);
- ✓ комбинирано използване: синергия на ПТУР, РПГ, щурмови дронове, минохвъргачки, артилерия и пехота;
- ✓ елементът на изненадата: щателна маскировка и изборът на време и направление на атака.

Въз основа на резултатите от анализа на поуките от воденето на артилерийски бойни действия е установено, че характеристиките на използването в съвременните условия на въоръжена борба са:

- ✓ увеличаване на разстоянията между огневи позиции за изпълнение на задачите от средствата за огнева поддръжка;
- ✓ прилагане на принципа на „маньовър - огневи налет - маньовър" при използване от две до пет огневи позиции;
- ✓ използване на високоточни боеприпаси, за изпълнение на задачите с 1- 2 оръдия или огневи взвод.

Използването на ДУЛС със способности за оптично, инфрачервено, радио и радиотехническо разузнаване позволи да се провежда непрекъснато и денонощно наблюдение на противника в тактическата дълбочина и да се предават разузнавателни данни на тактическия оперативен център в реално време. Основните методи за въздушно разузнаване от БЛС при обслужване стрелбата на артилерийския огън са полет по зададен маршрут, търсене на цел в зададена зона и облитане на няколко района – за доразузнаване на разкрити обекти. Максимизирането на ефективността на бойните действия на артилерията е постигнато, чрез интегрирането на радиолокационни, звукови и въздушни средства за разузнаване, както и прилагането на принципа „разузнаване-удар".

[43] Defense Express: FPV Drones in Ukraine (2024), https://en.defence-ua.com/

Сега артилерията е възприела съвременни алгоритми, при които данните за целите се изпращат директно от таблетите на операторите на безпилотни летателни апарати до таблетите на артилерийските разчети (екипажи), където те незабавно се одобряват от командирите, ако е необходимо, и често, без никакви допълнителни управленски стъпки, стрелбата се извършва в реално време по идентифицирани цели, в рамките на десетки секунди след тяхното откриване. Това взаимодействие е особено ефективно, когато артилерийски батареи, взводове и дори оръдия са причислени към батальони, щурмови групи и отряди.

Анализът на използването на противотанкова артилерия по време на войната на Русия и Украйна изисква корекции в тактиката на използване на противотанковите артилерийски подразделения, методите и принципите на обучение и подготовка на оръдейните разчети (екипажи). На базата на анализ на наличната информация са необходими промени в тактиката на използване на противотанкова артилерия в следното:

1) Разчетите на противотанковите артилерийски оръдия (ПТРК, СПГ) изпълняват задачи самостоятелно, и по-рядко в рамките на взвода. Преди това, използването на противотанковите артилерийски подразделения в танкоопасни направления се използваха повзводно или побатарейно, на стика между зоните за отговорност на съседни подразделения и др., с интервали между оръдията (бойните машини) от 150-200 метра. Поради активното разузнаване, провеждано с помощта на различни видове безпилотни летателни апарати, откриването на съсредоточаване на противотанкови артилерийски оръдия (бойни машини) е неприемливо.

2) Разчетите на противотанковите артилерийски оръдия не се разполагат на минимално разстояние от линията за съприкосновение с противника (предния край на отбраната), а изпълняват огневи задачи предимно чрез стрелба от закрита огнева позиция. Огневите позиции на цевната противотанкова артилерия се разполагат на разстояние 4-6 km от линията за съприкосновение. Задачите за унищожаване брониранитe цели на противника с право мерене се възлагат на ПТРК, които се разполагат в укрития на разстояние 4-5 km от линията на съприкосновение и заемат огневи позиции за изпълнение на огневи задачи по надеждно разузнати цели.

3) Смяна на огневата позиция, ако е възможно, след изпълнение на всяка огнева задача, или разчетът внимателно извършва маскировка и инженерно оборудване на огневите позиции, предотвратявайки откриването ѝ от безпилотни летателни апарати. Маскировката след изпълнение на огнева задача трябва да отнема не-повече от 15 минути (времето, необходимо за организиране на търсене на огнева позиция с помощта на безпилотен летателен апарат и подготовка на данни за контрабатареен огън от противниковата артилерия).

4) Оръдейният разчет (екипажа на бойната машина на ПТРК) може постоянно да пребивава и живее в оборудвани укрития (блиндажи, бункери и др.) на разстояние 150-300 m от маскираните оръдия (бойни машини) до получаване на огневата задача. Това минимизира вероятността от откриване от противникови

разузнавателни средства по време на маршове, развръщане и заемане на огневи позиции.

5) Оръдейният разчет (екипажа на ПТРК) е обучен и подготвен за самостоятелна дейност в продължение на 2-3 месеца в подготвен и оборудван блиндаж. Разчетът трябва да притежава умения за скрита работа през този период. При получаване на огнева задача, разчетът за кратко време се придвижва към оръдието (бойната машина), изпълнява огневата задача, маскира оръдието и бързо и скрито се връща в укритието си.

6) Противотанковата артилерия се разполага в укрития и щателно се маскира. Използват се окопи с различни конструкции в зависимост от условията на местността, на разстояние 3-5 km от предния край (линията за бойно съприкосновение). Извежда се на предварително подготвени огневи позиции само след получаване на потвърдена информация за характера на целта, нейното местоположение и координати. Решаващата роля в маскировката на оръдието (ПТРК) играе способността на командира на оръдието (ПТРК) да използва най-ефективно условията на околната среда; укритието не трябва да се откроява от околния фон при оглед на местността, включително от минимални височини при провеждане на разузнаване с помощта на безпилотни летателни апарати.

7) Придвижването на оръдия (бойни машини) към нови огневи позиции се извършва пооръдейно (самостоятелно), а не като част от взвода в колона, през нощта (в условия на ограничена видимост), по възможност под прикритието на средства за радиоелектронна борба.

8) Времето, прекарано на огнева позиция, не трябва да надвишава 15 минути (при изпълнение на огневи задачи със смяна на огневи позиции), като огънят се открива само след гарантирано разкриване на целта[44].

9) Тактиката на използване на скитащи огневи средства (танкове, оръдия, минохвъргачки и ПТУР) е получила широко разпространение. Скитащите огневи средства се използват за подвеждане на противника относно истинското местоположение на огневите средства и броя на бронираните машини. Придвижвайки се скрито по определен маршрут и сменяйки огневи позиции, разчетът (екипажът) на скитащото огнево средство изпълнява огневи задачи самостоятелно или в отговор на команди (сигнали).

10) На подстъпите към опорните пунктове и районите за съсредоточаване се оборудват минно-взривни заграждения. Местността по възможните пътища за излизане на атакуващите (щурмови) подразделения и пътищата за влизане на подкрепленията, ако е възможно, се пристрелват предварително от различни артилерийски подразделения, като се вземат предвид техните тактическо-технически възможности.

11) Огневите позиции по време на бой в град обикновено се избират на места, където при извикване могат да бъдат незабавно заети за поразяване на

[44] Капустин, П. И. Артиллерийская разведка. Дивизион, батарея, взвод, отделение : учеб. / П. И. Капустин, В. В. Рябоконь, В. Г. Ильев ; под общ. ред. П. И. Капустина. – Минск : ВА РБ, 2019.– 310 с.

противникови бронирани машини и веднага след изпълнение на огневата задача да се преместят на нова огнева позиция или в укритие. При избора на огнева позиция е важно да се обмислят маршрутите и пътищата на движение, като се картографират предварително с помощта на карти на градовете.

Изводи:

1. Ролята на противотанковите подразделения в поразяването на бронираните машини на противника не е намаляла; целите се преразпределят в зависимост от тактическо-техническите характеристики на противотанковите оръдия (ПТРК, РПГ). Цевната противотанкова артилерия започна да изпълнява огневи задачи предимно от закрити огневи позиции. Борбата с противниковите бронирани цели на предният край е почти изцяло поверена на разчетите (екипажите) на ПТРК (носими ПТРК) и реактивните противотанкови гранатохвъргачки (СПГ и РПГ).

2. Съвременните ПТРК и свързаните с тях системи (БЛА) не са направили танковете безполезни, но драстично са увеличили рисковете от използването им, особено без адекватно прикритие на пехотата, разузнаване и поддръжка за радиоелектронна борба и активна защита. Те са предоставили на пехотата и леките подразделения мощно средство за възпиране и унищожаване на бронирани машини, способно да нанесе значителни загуби дори на превъзхождащи противници и радикално да повлияе на бойната тактика. Борбата между бронята и средствата за нейното побеждаване продължава да бъде динамична надпревара във въоръжаването и тактиката.

3. В съвременната война, противотанковите управляеми ракети се очертаха като напреднала технология, които предефинираха тактиките на бойното поле и предизвиквайки големи изменения в традиционните стратегии за използването на бронираните машини. Със своята прецизност, преносимост и усъвършенствани възможности за насочване, ПТУР се превърнаха в ключов актив за военните по целия свят, влияейки върху динамиката на войната с бронираните средства в съвременния бой. Противотанковите ракети все по-често се свързват с безпилотни летателни апарати (БЛА) за насочване, където дроновете осигуряват разузнаване в реално време и лазерно насочване, което позволява водене на бойни действия отвъд линията на видимост.

4. Противотанковите ракетни комплекси революционизираха съвременните тактики на бойното поле, предлагайки несравнима прецизност и адаптивност срещу бронирани заплахи. С развитието на технологиите, ПТРК ще играят все по-важна роля в оформянето на бъдещето на войната.

Използвана литература:

1. Волчкевич, А. Ю. Противотанковые комплексы в вооруженных конфликтах современности, Минск: БНТУ, 2026. – С. 14-18, https://rep .bntu.by/handle/data/167510
2. Доктрина на Въоръжените сили на Република България, Издание (Б), София 2025, Национална публикация на въоръжените сили на Република

България НП – 01, МО, въведена със Заповед на министъра на отбраната № ОХ-1126/03.12.2025 г.
3. Center for Strategic & International Studies (CSIS): Active Protection Systems (2023), https://www.csis.org/.
4. Royal United Services Institute (RUSI): Drone War in Ukraine (2023), https://rusi.org/.
5. Oryxspioenkop: Overcoming APS in Ukraine (2023), https://www.oryxspioenkop.com/
6. Defense Express: FPV Drones in Ukraine (2024), https://en.defence-ua.com/
7. I. Bozov, I. Katsev, Assessment of unmanned aerial vehicles' reconnaissance effectiveness when used by artillery reconnaissance formations, International Scientific Conference ― “Defense Technologies” DefTech 2021, стр. 109-115, ISSN 2367-7902
8. И. Бозов, Анализ на техническите възможности на противотанкови ракетни системи FGM-148 JAVELIN И 9M133 KORNET, International Scientific Conference “Defense Technologies” DefTech 2025, стр. 584-590, ISSN 2815-4282
9. И. Бозов, Ред за изпълнение на задачи от безпилотни летателни системи в интерес на артилерията, International Scientific Conference “Defense Technologies” DefTech 2024, стр. 167-172, ISSN 2367-7902
10. Капустин, П. И. Артиллерийская разведка. Дивизион, батарея, взвод, отделение : учеб. / П. И. Капустин, В. В. Рябоконь, В. Г. Ильев ; под общ. ред. П. И. Капустина. – Минск : ВА РБ, 2019.– 310 с.
11. Война по-украински: артиллерийские дуэли решают все, Zvezda.ru 2024, https://zvezdaweekly.ru.
12. Рог В. Н., Ракетные войска и артиллерия в военных конфликтах XXI века, https://rep.bntu.by/bitstream/handle/data/144249/86-91.pdf?sequence =1&isAllowed =y&ysclid=mronxw1eut428010496

THE NORTHERN SEA ROAD – WHAT IS IT IMPORTANT FOR? A BRIEF ANATOMY OF THE ARCTIC BRIDGEPORT.

Stoyan G. Stoychev

Professor in National and International Security Department in Information Sciences Faculty at University for Library Studies and Information Technologies, Sofia, Bulgaria
E-mail: s.stoychev@unibit.bg; sstoychev_ss@abv.bg

Abstract: *Some of the aspects concerning the situation of Greenland, the appetites for its control by a country that is stepping down from the throne of a world hegemon, and the aspects related to one of the new geostrategic and geoeconomic routes – the Northern Sea Route (NSR) – are examined. In an attempt to present the essence and importance of the Arctic bridgehead, a brief retrospective is given of both the environmental, economic and energy factors in it – especially along the NSR corridors. Some actions by the US, which are related and aimed at gaining control of the entry points of this route through large-scale invasions, are also examined, but some of the possible revisions of these invasions are also presented. In the final part, a brief look is taken at the developing multipolar world and a brief overview of the various interests and influences in it.*

Keywords: *Greenland, Northern Sea Route, US Corps of Engineers, Arctic bridgehead, northern flank of defense.*

СЕВЕРНИЯТ МОРСКИ ПЪТ – С КАКВО Е ВАЖЕН ТОЙ? КРАТКА АНАТОМИЯ НА АРКТИЧЕСКИЯ ПЛАЦДАРМ.

Стоян Г. Стойчев

Професор в катедра „Национална и международна сигурност, факултет „Информационни науки", Университет по библиотекознание и информационни технологии (УниБИТ), София, България,
E-mail: s.stoychev@unibit.bg; sstoychev_ss@abv.bg

Резюме: *Разгледани са някои от апектите, касаещи положението на Гренландия, апетитите за нейното овладяване от на една страна, отстъпваща от трона на световен хегемон, аспектите, свързани и с едно от новите геостратегически, геоикономически трасета – Северният морски път (СМП). В опит да се представи същността и значението на Арктическия плацдарм, в кратка ретроспекция са разгледани както веонните, така и икономическите, и енергийните фактори в него – най-вече по коридорите на СМП. Разгледани са и едни действия от страна на САЩ, които са свързани и са насочени към овладяването на контрола на входните точки на този път, чрез мащабни инфестиции, но са представени и част от възможните ревизии на тези инфестиции. Във финалнта част се прави един кратък поглед към развиващият се многополюсен свят и бегла част от различните интереси и влияния в него.*

Ключови думи: *Гренландия, Северен морски път, Инженерен корпус на САЩ, Арктически плацдарм, сеневрен фланг на отбрана.*

Въведение

В продължение на едни мисли, изследвания и позиции на автора на доклада, които той представи в една предишна своя публикация под името/заглавието „Гренландия, Давос, Светът – кратка ретроспекция“ – намираща се под печат за едно от изданията на УниБИТ, ситуациите около Гренландия и Северният морски път търпят своето развитие и сега, в съвсем скоро до написването на този доклад време. И с тази публикация авторът ще представи една част от това развитие на ситуации, които са и важни, и значими както за Европа, така и за Света и световните сили в него, които се заявяват като такива на настоящия етап.

Методология

При изготвянето на своя доклад авторът е използвал системният подход, като най-подходящ за изследване на взаимосвързани и сродни дейности. Реализирането на доклада е постигнато и с използването на методите на литературния обзор, на изследванията и сравненията, на системния анализ, на теоретичните изследвания.

Резултати

В търсене на отговора на въпросът, поставен в заглавието на доклада – с какво е важен Северният морски път (СМП) изследванията ни водят към следното:

В оформилата се в последните няколко години съвременна стратегическа конкуренция в Света, Гренландия и СМП са едни от ключови елементи от новата арктическа геополитика, свързани както с с контрола на стратегическите транспортни коридори от една страна, така и с топенето на ледената покривка, което от своя страна дава нови възможности, нови перспективи както в чисто икономически план, така и във военен от и за използването на това геополитическо трасе – СМП, а това пък определя не на последно място и глобалното съперничество между САЩ, Русия и Китай. Гренландия, която е разположена до важния Гренландско-исландско-британски рубеж, но и проток (Greenland–Iceland–United Kingdom - GIUK gap), който от своя страна служи за охрана и достъп от Северния ледовит към Атлантическия океан. И в тази връзка, дори и в разрез със съюзнически действия, планове и позиции, президентът на САЩ заяви съвсем открито желанието си Гренландия да бъде предадена на страната му. По този начин островът, описван от много специалисти като Леден къс земя с площ над 2,16 млн. кв. км, се превърна не само в една от горещите точки на планетата, той се превърна и в точка на притовопоставяне между съюзниците от НАТО – в лицето на САЩ от една страна и на страните-членки на Алианса от другата страна на Атлантика, най-вече страните от ЕС. Както посочихме, островът със своята близост до GIUK gap, дава възможност и за наблюдение, но и за евентуален контрол върху движението на кораби, идващи от арктическите маршрути, което от своя страна кара държавите от Пакта да засилват присъствието си в региона, а и дори да искат да притежават този остров (САЩ).

От друга страна трябва да се каже недвусмислено, че наблюдението и евентуалният контрол върху движението на корабите (каквито и да са те, на когото и да са също), идващи от арктическите маршрути не разкрива напълно военното

измерение на СМП. Отдавна не е тайна, че в съвременни условия, с напредъка на технологиите, със способностите, които притежават хиперзвуковите ракетни комплекси, територията на Арктика, възприемана в редица случаи и като северната арктическа шапка на Земята, със Северния полюс, разделяла от векове Русия и Америка, вече е в много голяма степен пречка, а не защита или трудна за преодоляване зона - защита за страните от Севеврноатлантическият пакт, в това число и за САЩ. Според думите и на президента Тръмп, но и според редица военни стратези, не само руснаците (и техните въоръжени сили), но и китайците (не само с техните въоръжени сили) са завладяли вече Арктика и не само това, ами са и обкръжили отвсякъде и самата Гренландия. И подразбриайки се от всичко това, се ползват от привилегиите да използват и редкоземните метали (РЗМ) , и минералите, и положението което имат, че и през овладяната Гренландия да печелят в съвременната стратегическа конкуренция – конкуренция, която на основата на енергийните ресурси, на достъпа до тях и ползването им, печели надпреварата в създаването и в поддържането на една от важните, определящите технологии на съвременния свят – изкуствения интелект (ИИ). Или енергийните ресурси, разбирай горива, осигуряват повече енергия, а в основата на създаването, обучаването и използването на изкуственият интелект стои именно енергията. Разбира се, тук, отваряйки дума за енергията и нейното осигуряване, не само за или от ИИ, трябва да кажем, че и атомната енергия или енергията добивана от атомните електроцентрали също дава своя дан в тази надпревара, в тази световна конкуренция – но тя няма да бъде предмет на изследване в настоящия доклад.

Връщайки се в чисто военното отношение и измерението, значението на СМП към него, освен като предимства и печалби в конкуренцията за САЩ и президента Тръмп е ясно, че освен реалната заплаха за бърз достъп през Арктика до територията на САЩ на руските, че и китайските ракетни хиперзвукови комплекси, невъзможността за контрол на СМП, тоест, ако не се установи такъв от страна на САЩ - ще бъде и реално препятствие за достъпа на въоръжените сили на САЩ, както в Европа, така и в азиатския Индо-Тихоокеански регион.

Но определено, това не е единствената причина, заради която САЩ изразиха своите апетити към притежаването му открито и дори безпардонно.

Северният морски път е и най-краткият път между Азия и Европа, минавайки край брековете на Русия, той (СМП) съкращава с до 50% разстоянието между Европа и Азия спрямо южния маршрут през Суецкия канал. От своя страна не само намаляващите дебели ледове в Арктика, а и наблюдаваното в последните години топене на същите, улесняват корабоплаването и разкриват достъп до нови залежи от суровини и минерали в самия Гренландски регион. Тоест, Гренландия има в своето „портфолио" и множество икономически и транспортни фактори, които отново допринасят за нездравословните (за страните членки на НАТО – от една страна САЩ и от друга, страните членки и на ЕС) отношения между кълнящите се в целостта и здравината на НАТО негови членки.

Както посочихме, не само чисто плавателните и/или търговските перпективи на СМП стоят в основата на това желание, а и чисто икономическите фактори дори излизат на преден план, на предна позиция. Това допринася за тази яростна

стратегическа конкуренция, в която всеки имащ се за голям играч на световната сцена търси възможности както за достъп и влияние до и над него, така и за възможността да влияние върху неговото ползване и от своя страна - да участва в „делата в Арктика". И тук като един незаобиколим икономически фактор се появява познатия ни енергиен фактор. Фактор, който вече прави не само желание на световните „играчи" да са там, но фактор, който се очертва като основа на „битката за Арктика" – като фундаментална причина да се обособи и да се включат световните сили/"играчи" в този горещ (чисто стратегически и геополитически) Арктически плацдарм.

Какво стои в основата на този икономически и енергиен фактор, който става основа за развитието на Арктическият плацдарм в съвременните условия? С какво точно там се появяви този интерес, за който са готови да водят битка световните сили? Ами, смело можем да посочим, че в тази основа стоят резултатите от някои геоложки изследвания, според които там, в Арктика, има неразработени находища от над 1,67 трилиона куб. метра природен газ, от над 90 милиарда барела петрол, от РЗМ и минерали на стойност от над един трилион долара. В добавка могат да се добавят и едни от още по-новите геоложки проучвания около хребета Гакел, и решението на ООН, което потвърждава, че включените в заявката на Русия (Руската Федерация) 1,2 милиона кв. километра шелф са част от Федерацията в геоложки план. А това от своя страна увеличава потенциалните руски запаси от въглеводороди с 5 милиарда тона, които милиарди съвсем разбираемо се превръщат в различни видове горива. А горивата, както посочихме и по-горе са енергия.

И ако все пак с Гренландия всичко ще завърши по един доста мирен начин (според автора на доклада) – САЩ ще получат всичко, което желаят и без да използват сила, или като прогноза: „въпросът Гренландия" между САЩ от една страна и Дания, плюс останалите страни членки на НАТО, които са членки и на ЕС, от друга страна, ще приключи с разширяване на настоящото споразумение за присъствието на американски военни сили (например, безсрочен наем на няколко десетки хиляди квадратни километра, ако не и стотици хиляди, за военни бази и необходима им инфраструктура), плюс допълнителни споразумения за проучване и добив на редкоземни метали (РЗМ) и минерали, Но както посочихме малко по-горе, освен всичките тези „придобивки", знаем, че там не става въпрос или не стои въпросът само за военните бази, за РЗМ и минералите, които могат да бъдат добивани и ползвани след това от САЩ - там стои и другият важен въпрос или важна придобивка – достъпа и възможността да се ползва – военно, икономически и да се влияе на използването на Северния морски път (СМП) – транспортно, геоложко, енергийно, геополитическо и стратегическо.

Но да използване същата алегория, както в по-ранния доклад за Гренландия, Давос и Светът - къде в крайна сметка е „ключът от бараката", наречена в нашия случай СМП?

Ако Гренландия, като част от GIUK gap, е крайната, западната врата, реално изходът на СМП към Европа и към Северният Атлантик (не следва да се изключват нито САЩ, както видяхме, нито Канада, която пък е част от United

Kingdom - UK), то другата, източната врата или входът към тази толкова важна зона, оформяща този съвременен Арктически плацдрам, се намира между Азия и Северна Америка - залива Провидение, в югоизточната част на полуостров Чукотка, в самото Чукотско море, в близост до Беринговият проток . И именно, не само чрез контролът на едната точка иили над част от територия, в близост до официално приетата крайна точка на СМП, каквато се явява Гренландия със своето географско положение, а и контролът над другата точка – в случая, входната точка на СМП от изток, САЩ се опитват да решат ребусът наречен в нашия случай „ключът от бараката“ на СМП. И реално, именно двете точки на началото и на краят на СМП, оформят генерално т.нар. Арктически плацдарм, в който плацдарм свветовните сили се опитват да спечелят и да задържат определено стратегическо предимство над конкурентите си, над обявените и за заплаха, и за предизвикателство противостоящи (по отношение на интереси, влияние, хегемония) страни.

Тук идва резонно въпросът: Всъщност, как контролът над Гренландия може да допринесе за контролът над СМП? И ако казусът, възникнал между съюзните САЩ и Дания, плюс останалите европейски страни членки на Пакта, свързан или отнесен към „право за ползване“ на острова, вече е решен, то остава въпросът, всъщност остава нерешен въпросът за ползването на СМП от страна на САЩ. Защо? Ами, защото в крайна сметка договор, в каквато и да е форма, за ползването на част от територията на Гренландия, на добив и ползване на РЗМ и минерали в недрата й, не е признаване на тази територия (която ще бъде отдадена на САЩ) като изконна, а и законна американска земя. А от там и правото на регулации над или при ползване на СМП няма да бъде притежание и на САЩ.

Тогава какво? Тогава, освен опитите, придобивайки правото да ползват определена територия от Гренландия (за военни бази, за инфраструктура, свързана с тях, за развитие на проекти за добив и ползване на РЗМ и минерали), да могат да влияят и да контролират по някакъв начин както плаването на корабите по СМП, така и на чисто икономическите, а от там и на чисто енергийните проекти, придобивки и възможности в Арктическият плацдарм от западна посока или от западната страна на този плацдарм, САЩ обръщат поглед към тези възможности (за контрол, влияние, развитие на способности) и от източна страна, от входната точка към плацдарма от Изток: от Азия и Северна Америка. Защото не само на САЩ и на тяхната държавна администрация е ясно, че влиянието и контролът над една зона, над един горещ плацдарм, какъвто се е оформил на настоящия етап от развитието на световната стратегическа конкуренция СМП, само и единствено от едната му страна или само и единствено над една определена, малка част от него не е никаква гаранция за успех – не е никаква гаранция, че с това влияние и с този частичен контрол, ще могат не само да поддържат своето световно господство като хегемнон, но и да не изостават в тази световна конкуренция. Която конкуренция, както видяхме не е само за транспортът през СМП, не е само и за добива и ползването на РЗМ и минерали, не е само за икономическите ползи, а и за основна част от тях – енергийните ползи, осигуряването на енергийни ресурси и на енергията добивана от тях, а на тази основа е конкуренция най-вече за

възможността за развитие, обучение и ползване на една от най-върховите съвременни технологии, имаща всички фактори и предпоставки да бъде разглеждана и като голяма, стратегически важна и определяща инфраструктура - Изкуственият интелект.

Така, в светлината на възможностите за влияние и контрол над СМП (по възможност не само едностранно – не само от западна страна на тази маршрут) и над икономическите и енергийните ползи от това, в светлината на отстояване на позиция в свевтовната стратегическа конкуренция също, идва официалното известие на Инженерния корпус на Армията на САЩ относно Съвместната база Елмендорф-Ричардсън (Joint Base Elmendorf–Richardson - JBER) в Анкъридж. Известие, в което се посочва, че Инженерният корпус на армията на САЩ задейства проект за 7 милиарда долара, наречен „Рекапитализация на Файтъртаун" в базата Елмендорф-Ричардсън (JBER) в Аляска.

Надявам се, след всичко споделено до тук в доклада, на всеки четящ го сега е ясно, че това не е просто рутинна административна стъпка! Става дума за едно мащабно, едно голямо и на качествено ново ниво преформатиране на северния фланг на американската отбрана, чрез финансова инжекция, оценявана, както беше посочено на около 7 милиарда долара. В проектът за Рекапитализация първо е направен обстоен анализ и от него се извежда важният извод, че съществуващата летищна инфраструктура в югоизточна Аляска вече не съответства на оперативните планове на Пентагона, което налага изграждането на изцяло нов сектор, придобил кодовото наименование „Рекапитализация на Файтъртаун" (Fightertown Recapitalization - FTR) или „Боен град". И ако на пръв поглед, изхождайки от името на проекта, той да изглежда основно като логистично разширение, изхождайки от неговата същност, от мястото на което е обявено изпълнението на този проект, вторият поглед, погледът на реалността ни показва, че това е опит за създаване, за развитие, за подобрение на качесвено нови нови на способностите, които тази „географска точка" – базата Елмендорф-Ричардсън, следва да придобие и чрез тях да бъде в състояние и самата база, и САЩ като цяло, да контролират прехода между Пасифика и бързо освобождаващият се от лед Северен ледовит океан, по чиято територия се оформя и този Арктически плацдрам, с основа СМП - с неговите арктически коридори.

В програмата на проекта FTR е включено както изграждането на нови писти, специализирани хангари, ремонтни работилници, заводи за производство на боеприпаси и рафинерии за авиационно гориво, така и изграждането, и обновяването на съществуващите симулационни центрове, щабни помещения и сгради, а също и жилищни комплекси за допълнителен персонал. Официалните източници посочват, че строителството ще бъде синхронизирано с доставките на нови авиационни платформи. Тук обаче възниква първият сериозен въпрос: Защо САЩ решават да концентрират толкова критична маса от ресурси в една-единствена база, която се намира в обсега на руските брегови и стратегически ракетни комплекси? Да, с подобрените си способности, които следва да се придобият от JBER, основната идея на този проект е насочена към поодбряване, ако не и тотално контролиране на възможността за използване на СМП от към

Тихият океан, но според някои експерти и анализатори от специализираното издание The War Zone, JBER неизбежно се превръща в приоритетна цел още в началните часове на евентуален мащабен конфликт. Това обяснява защо в плановете за изпълнение на проекта „внезапно се появяват“ изисквания за тежко фортифицирани хангари и подземни системи за съхранение, способни да издържат на ракетен обстрел.

По-нататък, изследването, направено в доклада ни разкрива, че един от най-интересните детайли, които изтичат покрай техническите спецификации на проекта, е потенциалното разполагане на перспективния изтребител от шесто поколение, условно наричан F-47 . Както се изказа за него президентът Тръмп: In terms of all of the attributes of a fighter jet, there’s never been anything even close to it, from speed to maneuverability, to what it can have, to payload, тоест, По отношение на всички качества на изтребител, никога не е имало нищо дори близко до него, от скорост до маневреност, до това, което може да има, до полезен товар. Неговият първи полет (на изтербителя F-47) се очаква около 2028 година в рамките на програмата Next Generation Air Dominance (NGAD). Има индикации, че параметрите на „Бойния град“ се проектират именно с оглед на тежките изисквания за поддръжка, радиопоглъщащо покритие и цифрова интеграция, нужни за този тип платформи. Това изглежда логично, но има един проблем – съдбата на самата програма за шесто поколение в момента е финансово несигурна и Пентагонът неколкократно ревизира разходите. За всички експерти, не само в Пентагона става все по-ясно с всеки изминал ден, че в опит да задържат своята световна доминация (не само въздушна такава) и своя хегемонизъм над по-голямата част от света (в защита на своите национални интереси) на САЩ се налага да заделят все повече и повече средства за странични, непредвидени и не включени предварително в планираните разходи средства – най-вече парични. Дори и предизборната кампания на Тръмп, с основния й слоган тогава Make Amerika Great Again (MAGA) – Да направим Америка велика отново, превърнал се след това в политическо движение, с всички негови поддръжници, не е в състояние да осигури всички необходими парични средства за това разкъсване между запазване и поддържане на световната доминация на САЩ и за свеого рода завръщане (макар и в определена степен) към Доктрината Монро – за налагане и провеждане на определена изолационистка политика от страна на Щатите.

И ако в момента JBER осигурява логистиката на 11-та въздушна армия и 3-то изтребително крило, които оперират с F-22 Raptor, използват също и самолети за далечно радиолокационно откриване и управление E-3 Sentry, както и транспортни самолети C-17 Globemaster III, то както видяхме самият проект, обявен от Инженерният корпус на Армията на САЩ следва да надгради може да се каже епохално – до качествено нови ниво на бойните способности на Бойният град, на самите САЩ в този толкова важен и чувствителен за тях регион – регион, който може напълно реално да се приеме като входът от изток, от Азия към СМП. А кой е основният „играч“, които заявява все по-открито, не само с декларации или на книга, своите амбиции за световна доминация, която да постигне по един мирен начин, включително и чрез широко изъпозване на коридорите на СМП – разбира

се с помощта на Русия – големият противостоящ, голямото предизвикателсвто – Китайската Народна Република, Китай. А като включим и Руската Федерация, с нейният арктически флот, с нейните амбиции, които нарастват и се развиват не само по СМП, то предизвикателствата и противостоянете на тези световни сили от страна на САщ става все по-остро, все по-чувствително, все по-налещашо и нетърпящо отлагане – защото, които изостане и с крачка, той губи позиции в съвременната стратегическа конкуренция.

Картината на това надграждане на JBER с проекта FTR включва също така и базирано във базата 176-то крило на Националната гвардия на Аляска, а също така и развърнатият там през 2023 година Отряд 1 от 55-та Оперативна група/оперативно крило, подчинена на базата Офът в Небраска (Offutt Air Force Base) , като с този отряд разполагащ и използващ едни от стратегическите самолети за радиотехническо разузнаване RC-135V/W Rivet Joint, базата надгарди със способности и за радиотехническо разузнаване (РТР) и радиоелектронна борба (РЕБ), често наричана и радиолелектронна война (РЕВ). Тази модификация на Boeing (RC-135V/W), чиито корени датират от епохата на Студената война, се използва в района за прехващане на руски и китайски комуникации (основните предизвикателства и противостоящи страни), картографиране на радари за ПВО и проследяване на телеметрия при ракетни изпитания. Разполагането им в Анкъридж драстично съкращава времето за полет до Беринговия проток и Охотско море. Според редижа, запознати с техните способности, а и не само с техните, експерти търсенето на разузнавателни данни в широкият регион на Североизточна Азия е нараснало критично, а Аляска служи като най-удобния трамплин за шпионаж срещу затворените руски военни зони в Камчатка и Приморието. Но за следващото поколение бойна платформа F-47 ще трябва и в тази посока да се търси определено надграждане, което за момента не е ясно в каква посока или в какви домейни, освен въздушният ще бъдат те. Могат да се направят предположения от автора, че тези, нови, надградени способности, следва да включват и способности за използване комбинирано, съвместно на платформи и системи както в кибердомейна, така също и в домейнът космос, а предвид разположението на JBER също така и в домейна море/вода.

Изследването ни, макар и в този лимитиран формат, ще бъде много непълно, ако в него нве представим малко и от другата, обратната страна на монетата, наречена Световна доминация и Стратегическа конкуренция. Какво има предвид автора в случая – най-малкото това, че зад тези по-скоро тактическите аргументи (към настоящият момент) на ВВС на САЩ, за които се търси с проекта FTR да нарастнат до оперативно-стратегически аргументи и способности, прозира една по своята същност – геостратегическа и геоикономическа нервност. Кои са основните причини за тази нервност, кое я инициира и дава поле за проявленията й? Отговорът е почти ясен, за стигналите до тази част на доклада, но все пак – пълнотата (по-добрата) на изследването ни изсиква да я представи и авторът. И представянето в случая стартира с Руската Федерация, с Русия, с Москва и нейните амбиции, подкрепени с редица дейности и десйвтия по ускореното развитие на използването на Северния морски път (СМП). Русия разглежда СМП като основна

алтернатива на Суецкия канал, инвестирайки не само в ледоразбивачен флот и брегова отбрана, но също така и в проучвания на шелфът и морското дъно, в нейните прилежащи територии и икономическата й зона в Северния ледовит океан, в изграждане на плаващи АЕЦ, в платформи, базирани на използването на ИИ и други високи технологии. За Русия, съгласно нейното законодателство, а и съгласно международните спогодби, съществуващи към момента, това е вътрешна транспортна артерия, защитена от международни санкции. За Вашингтон и САЩ обаче, установяването на руски контрол над този маршрут означава загуба на стратегически лостове в Арктика. И както беше посочено по-горе, с модернизацията на JBER, с нарастването на нейните способности една от важните цели на проекта FTR несъмнено е осигуряването на възможност за бързо прехвърляне на ударни сили от Армията на САЩ, способни да блокират източния вход на СМП в района на Чукотка, на Беринговия проток, на Аляска като цяло.

На следващо място тази нервност от страна на САЩ се корени в действията и на Китай, който от своя страна също се обяви за „близка до Арктика държава" и активно развива концепцията за „Полярен копринен път". Пекин финансира съвместни енергийни проекти с Русия в Ямал и изпраща свои научноизследователски кораби, които, според доклади на Пентагона, извършват хидрографско разузнаване на морското дъно за нуждите на китайския подводен флот. И виждайки от своя страна Китай като основен противник, като основно предизвикателство за САЩ за съхраняване и поддържане на тяхното световно господство по море, за тяхната геостратегическа и геоикономическа доминация, Щатите правят опит, чрез създаването на „Бойния град" в Аляска един вид да изградят севрният зъб на клещите, на северният затвор на тези клещи, които пък САЩ изграждат на юг чрез съюзите AUKUS и QUAD – и по този начин да сложат прът в амбициите на Поднебесната Империя за Полярният път на коприната, а и за тяхното световно надигане или по-точно Продължаването с усилени темпове на ТОВА НАДИГАНЕ.

Заключение

JBER в Анкъридж отдавна служи като административен център за мащабните въздушни маневри Red Flag-Alaska и Northern Edge. Те се провеждат в рамките на Обединения тихоокеански полигон в Аляска (JPARC) – огромно въздушно и сухоземно пространство, което позволява симулиране на сложни действия по радиотехническо разузнаване, по радиоелектронна война и масирани въздушни боеве. По оценка на различни военни експерти и анализатори, значението на JPARC ще нараства, тъй като Пентагонът изпитва остър недостиг на полигони в континенталната част на САЩ, където могат да се тестват системи с голям обсег без риск от компрометиране на честотите. А както посочихме, значението на базата ще нараства и по отношение на способностите и преминаването на следващо, ново поколение платформи – както във въздуха, така и в другите домейни.

Но дори и след всичко това, трябва да кажем, че версия за абсолютно американско доминиране (NGAD) обаче изглежда стабилна разглеждайки само проекта FTR, един вид – изглежда стабилна само на книга, по т.нар. проектна

документация. Числата, с тяхното финансово най-вече измерение и географските реалности в тази част на света показват една друга , малко по-различна картина. Близостта на Аляска до Руската федерация превръща региона в предна позиция, която в случай на реален конфликт между най-мощните ядрени сили, на която позиция реално няма да има време за развръщане на каквито и да са големи или мащабни сили. Съвременните руски хиперзвукови комплекси „Кинжал" и „Циркон", както и стратегическите крилати ракети Х-101, изстрелвани от ракетоносците Ту-95МС, някъде над вътрешността на Сибир, могат да достигнат съоръженията в Анкъридж за броени минути. В този смисъл милиардите, инвестирани в „Рекапитализация на Файтъртаун" (FTR), могат да се окажат вложени в статична мишена, чието унищожение е технически предрешено. Концентрацията на авиация, боеприпаси и гориво на едно място опровергава в голяма степен дори концепцията на самите САЩ за „гъвкаво бойно използване" (Agile Combat Employment), която изисква дисперсия (разсредоточаване в различните домейни), а не струпване.

Но с представените данни за проекта FTR, с предприемане на толкова мащабни стъпки и за текуща модернизация, и за надграждане на JBER с всички посочени нови способности в близкото бъдеще показва, че САЩ не са съгласни, не се отказват от монопола си над морските трасета, на морските пътища в световен, глобален план. Реалностите в съвременния, развиващ се и изграждащ се пред очите ни многополюсен свят показват, че тази доминация, че този монопол вече не е като на световен хегемон, а той изтънява силно и е подложен на редица „ревизии" от останалите световни сили на международната арена – които не принадлежат към т.нар. Западен свят. Или САЩ, всъщност отказват да приемат загубата на монопола си над глобалните морски пътища, в случая и над СМП. Но следва да видим, да ни покаже времето напред дали опитът да се застрашат едновременно източните граници на Русия и северните логистични маршрути на Китай, с изискванията за тези действия на едни огромни по мащаби ресурси - ресурси, които надхвърлят в пъти капацитета на седеммилиардния проект в Елмендорф-Ричардсън (проектът JBER) няма да доведе до щракването на Капана на Тукидид за САЩ, вместо да успеят да щракнат самите те клещите около амбициите на Китай, а и около тези на Русия, свързани или отнесени с коридорите на СМП, а и не само с тях?

Литература

1. Стойчев, С., 2023. Операции в множество домейни/Multi-domain operations – MDO. София: издателство Дио-Мира, ISBN 978-619-7696-14-1.
2. Йорданова, С., 2023. Еволюция на съвременните конфликти: Анализ на „новите" войни и техните и техните динамики, монография. София: академично издателство „За буквите – О писменехь", ISBN 978-619-185-637-4.
3. Симеонов, Т., 2014. Правна уредба на мениджмънта на сигурността и отбраната. София: ВА „Г. С. Раковски", ISBN: 978-954-9348-82-8.

4. Гренландия на арктическия кръстопът, 2026. [viewed 21 July 2026]. Available from: https://armymedia.bg/2026/01/24/%D0%B3%D1%80%D0%B5%D0%BD%D0%BB%D0%B0%D0%BD%D0%B4%D0%B8%D1%8F-%D0%BD%D0%B0-%D0%B0%D1%80%D0%BA%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D1%8F-%D0%BA%D1%80%D1%8A%D1%81%D1%82%D0%BE%D0%BF%D1%8A%D1%82/.
5. The GIUK Gap's strategic significance, 2019. [viewed 21 July 2026]. Available from: https://www.iiss.org/publications/strategic-comments/2019/the-giuk-gaps-strategic-significance/.
6. Air Force's Fightertown Alaska Plan Takes Shape, 2026. [viewed 22 July 2026]. Available from: https://www.twz.com/air/air-forces-fightertown-alaska-plan-takes-shape.
7. Plans For New Hardened Aircraft Shelters Notably Absent From New USAF Base Modernization Strategy, 2024. [viewed 21 July 2026]. Available from: https://www.twz.com/air/plans-for-new-hardened-aircraft-shelters-notably-absent-from-new-usaf-base-modernization-strategy.
8. F-47 program producing test aircraft, on schedule for 2028 flight, 2026. [viewed 21 July 2026]. Available from: https://www.defensenews.com/industry/techwatch/2026/07/30/f-47-program-producing-test-aircraft-on-schedule-for-2028-flight/.

MAPPING THE EVOLVING ADVERSARY - A LONGITUDINAL ANALYSIS OF ADVANCED PERSISTENT THREAT TACTICS AND DEFENSIVE CO-EVOLUTION

Marius Iulian Mihailescu[1], Stefania Loredana Nita[2], Laurentiu Bogdan Asalomia[4], Valentina Marascu[1,3]

[1]Faculty of Engineering and Computer Science, Spiru Haret University, Bucharest, Romania, m.mihailescu.mi@spiruharet.ro
[2]Faculty of Information Systems and Cyber Security, Military Technical Academy "Ferdinand I", Bucharest, Romania, stefania.nita@mta.ro
[3]National Institute for Laser, Plasma and Radiation Physics Magurele, Romania; Faculty of Mathematics and Computer Science, Bucharest University, Bucharest, Romania, v.marascu.mi@spiruharet.ro
[4]Northern Marine Management Limited, Glasgow, Scotland, United Kingdom; e-mail: asalomiabogdan@yahoo.com

***Abstract**: This paper addresses that limitation through a longitudinal analysis of TTP evolution across multiple APT groups over the past decade, mapped against the MITRE ATT&CK framework. Tracking a single actor, Russia's APT29, from the 2017 NotPetya-era emphasis on destructive malware through the 2020 SolarWinds supply-chain compromise to the 2023–2024 shift toward cloud-identity attacks documented in joint government advisories, alongside comparative cases including the 2023 Volt Typhoon living-off-the-land campaign against U.S. critical infrastructure and the 2023 cascading supply-chain compromise of 3CX, the paper's contributions are threefold: (1) a comparative timeline documenting the shift from malware-centric intrusions toward living-off-the-land techniques, software supply-chain compromise, and cloud-native attack paths; (2) a co-evolutionary model correlating specific defensive advances — EDR adoption, behavioral analytics, zero-trust architectures — with corresponding adversary adaptations, revealing recurring displacement patterns rather than outright tactic abandonment; and (3) a set of forward-looking indicators, derived from this historical pattern analysis, meant to help defenders anticipate likely next-generation evasion strategies rather than respond reactively to already-observed techniques. The work supports threat intelligence teams and detection engineers in shifting from reactive, signature-based defense toward anticipatory, pattern-informed security architecture.*

***Keywords**: advanced persistent threats, MITRE ATT&CK, living-off-the-land, threat intelligence, cloud security, attacker-defender co-evolution*

Introduction

Advanced Persistent Threat (APT) groups are not one-time intrusions but standing capabilities: the same state-linked units reappear across a decade of campaigns, adapting their tools each time a defensive measure closes off a previously reliable avenue. Treating any single campaign in isolation, the dominant unit of analysis in most incident reporting, captures a snapshot of tradecraft at one moment but says little about where that tradecraft came from or where it is likely to go next.

This longitudinal pattern is underused. Much of the technical literature on APT tradecraft is organized by campaign or by actor at a single point in time, cataloguing the

tactics, techniques, and procedures (TTPs) a group used in a specific intrusion without systematically tracking how those TTPs changed across the group's own history or in response to specific defensive developments. The result is a body of knowledge that is excellent at describing what has already been observed and comparatively weak at anticipating what a given actor is likely to do once its current techniques stop working, leaving detection engineering in a largely reactive posture: new signatures and detections follow disclosure of a technique rather than anticipating its likely successor.

This paper aims to fill an unaddressed research gap in the field of cybersecurity. Specifically, it conducts a full-lifecycle long-term tracking and analysis of the evolution of TTPs of multiple APT groups—professional groups that lurk long-term to launch cyberattacks—over the past decade, by benchmarking against the industry-standard MITRE ATT&CK framework.

Instead of limiting its analysis to a general overview of all groups, the paper selects a typical case for in-depth research: the Russian group APT29. It fully tracks and records three distinct attack campaigns launched by this group over an eight-year period, then cross-compares the trajectory of APT29’s tactic changes with that of other state-backed threat actors.

This paper has three core contributions. First, it compiles a timeline that enables horizontal comparison, clearly documenting the entire transformation of attack trends: in the early days, attackers relied primarily on self-developed malware to initiate intrusions, but later gradually shifted to three new types of attack vectors, namely Living-off-the-land techniques, software supply chain intrusions, and native attack paths specifically designed for cloud environments. Second, it proposes a co-evolution model that maps the specific technical upgrades of defenders to the corresponding adjustments made by attackers. This model demonstrates that improvements in defensive capabilities only force attackers to switch to other techniques of the same category, and never lead them to abandon their original attack objectives. Third, it summarizes a set of predictive indicators, all extracted from the patterns of offensive and defensive evolution sorted out earlier, that help defenders anticipate the next generation of defense-evasion strategies that attackers may adopt, rather than being forced into a reactive, hasty response only after these new strategies appear in actual attacks.

Section 1 first sorts out the core principles of the MITRE ATT&CK framework, as well as all existing previously published research related to APT attack tactics and the co-evolution of offensive and defensive parties. Section 2 proposes a long-term analysis framework that divides the entire development process of TTPs into four stages. This framework is not proposed out of thin air; it is finally developed by using a purpose-built "retention score" indicator to map each of the four stages to the core tactic categories of MITRE ATT&CK. Section 3 puts this analysis framework into practice, using it to conduct a comparative case study covering five attack campaigns. Section 4 compiles the predictive indicators specifically designed for proactive defense. Section 5 discusses the limitations of the analysis framework itself, and the final conclusion section summarizes all the core contributions of this paper once again.

1 Background and Related Work

1.1 The MITRE ATT&CK Framework as a Common Reference

To compare all attack tactics used by attackers time and again over an extended period, there must first be a set of unified terminologies that are universally recognized and not arbitrarily altered. Otherwise, it is impossible to clarify what changes have occurred in these attack methods, let alone record the evolutionary trajectory of these behaviors. The de facto general standard currently used in this field is the MITRE ATT&CK framework. This framework was initially an internal tool for the R&D team, and it was officially released to the public only in May 2015. At its initial launch, it categorized 96 specific techniques under 9 tactics. It is a purposefully organized, continuously updated classification system for attacker behaviors, whose classification is centered on two completely distinct dimensions.

The first dimension is tactics, which in simple terms refers to the core goal an attacker aims to achieve through a certain action. For example, maintaining a long-term presence on a target system (persistence), or moving from a compromised device to other devices on the same network (lateral movement), both fall under the scope of tactics.

The other dimension is techniques, which refers to the specific practical methods attackers use to achieve that goal (Strom et al., 2018). Not only is the content contained within the framework valuable, but the step-by-step expansion process of the framework itself can also provide critical supporting information for the core argument this paper intends to put forward. Enterprise ATT&CK, which is purpose-built for enterprise scenarios, only covered the Windows system when it was first launched. In 2017, it expanded its scope to add support for Mac and Linux systems; in 2019, it added a matrix specifically for cloud scenarios; and in 2020, it released a matrix adapted for Industrial Control Systems.

Attackers had long begun to shift their focus to cloud environments and systems other than Windows, and the timing of the framework's addition of these corresponding contents was only slightly later than the emergence of this trend, which this paper also accurately records. Throughout this article, ATT&CK is only used as a set of general descriptive vocabulary, and no causal-related claims will be derived from it. The framework itself is only responsible for recording the observed, actual behaviors carried out by attackers, and never explains the motivations behind these behaviors. The co-evolution explanation that will be proposed in Section 2 of this paper, however, fills in the interpretive content that this framework has deliberately omitted from its inception.

1.2 Documented Evolution: From Destructive Malware to Living-off-the-Land

The most well-documented case of iteration in cyberattack techniques is that advanced persistent threat attacks, which originally relied primarily on custom malware, are abandoning these old methods, and a growing number of attackers are shifting to the "live off the land" technique.

The so-called advanced persistent threat refers to a type of professional cyberattack activity that is specifically planned, able to lurk in target systems for a long time, and continuously steal data or cause damage. In the past, most such attacks required the development of exclusive malware to complete intrusion operations. Today's "live off the

land" approach is different: it does not require attackers to write custom malware, and instead completes all intrusion operations using only management tools that come with the operating system itself—namely PowerShell, WMI, and otherwise legitimate remote access tools. These tools are normally used by computer administrators for daily system maintenance; when attackers misuse them to carry out malicious acts, the resulting malicious traffic can blend into ordinary system management traffic, making it indistinguishable to outside observers, and thus extremely difficult to detect traces of the attack.

The most typical and representative recent user of this technique is the hacking group Volt Typhoon; original source materials link this group to China. The United States and multiple international agencies released a joint advisory in May 2023 that specifically documented the group's activities: it relies heavily on "live off the land" techniques, maintains an extremely low operational profile over the long term, and quietly sustains access to critical infrastructure across multiple sectors in the United States, including communications, energy, transportation, and water services. By February 2024, these relevant agencies released a follow-up advisory confirming that the scope of the attack was even broader than what was documented in the 2023 advisory. The earliest source for these records is Cybersecurity and Infrastructure Security Agency, National Security Agency, & Federal Bureau of Investigation, 2023.

The appeal of this approach is direct: detection tools built to flag known-malicious binaries have comparatively little to alert on when the tools in use are the same ones system administrators use every day, which is precisely why living-off-the-land activity recurs across otherwise unrelated actors rather than remaining a single group's signature.

1.3 Attacker-Defender Co-Evolution as an Analytic Frame

Security research has long used an arms-race framing to describe the relationship between attackers and defenders, but applying that framing systematically to APT tradecraft, rather than invoking it as a metaphor, requires connecting specific defensive advances to specific adversary responses rather than describing both sides' evolution in parallel. Zero trust architecture, formalized by the U.S. National Institute of Standards and Technology as a shift from perimeter-based defense to continuous, resource-level verification (Rose, Borchert, Mitchell, & Connelly, 2020), is a useful test case: it directly targets the assumption — that a credential or network position, once obtained, grants durable trust — that living-off-the-land and identity-based techniques depend on. Whether the resulting adversary adaptation is a genuinely new technique or a displacement of an existing objective onto a new technique is the question the framework in Section 2 is built to answer, and the case analysis in Section 3 to test.

2 A Longitudinal Framework for TTP Evolution

2.1 Four Eras of APT Tradecraft

The cases reviewed in Section 1 suggest a rough periodization, not because any actor cleanly exits one era before entering the next, but because each era is organized around a dominant technique for achieving the same underlying objectives — initial access, persistence, and command and control — that becomes dominant once the previous era's

technique is reliably detected. The malware-centric era relies on custom or repurposed malicious code delivered via phishing or exploited vulnerabilities, exemplified by the 2017 NotPetya attack's destructive payload (U.S. Department of Justice, 2020). The living-off-the-land era relies on native administrative tools rather than custom code, exemplified by Volt Typhoon. The supply-chain era compromises a trusted third party to reach many victims through one intrusion, exemplified by the 2020 SolarWinds compromise (Cybersecurity and Infrastructure Security Agency, 2021) and, in an escalated form, the 2023 3CX compromise, in which an initial supply-chain compromise of a trading-software vendor was itself used to stage a second supply-chain compromise of 3CX's own build environment. The cloud-native era targets identity and cloud infrastructure directly — tokens, OAuth grants, cloud API permissions — rather than the network perimeter, exemplified by the cloud-focused tactics that international agencies documented in Russian SVR activity in 2024 (Cybersecurity and Infrastructure Security Agency, National Cyber Security Centre, et al., 2024).

2.2 Mapping a Single Actor's Trajectory

Figure 1 places a single actor's campaigns against this periodization: APT29, tracked under different public names across its campaigns (Cozy Bear, Nobelium, Midnight Blizzard), appears in the supply-chain era through SolarWinds in 2020 and again in the cloud-native era through the Microsoft corporate-email intrusion first detected in January 2024 (Microsoft Threat Intelligence, 2024), giving a single-actor trajectory across two eras within four years. The other cases plotted — NotPetya, Volt Typhoon, and 3CX — corroborate that the eras are not strictly sequential across the field as a whole: different actors occupy different eras at the same calendar time, consistent with the framework's claim that era transitions are driven by which defenses a given target has adopted rather than by calendar time alone.

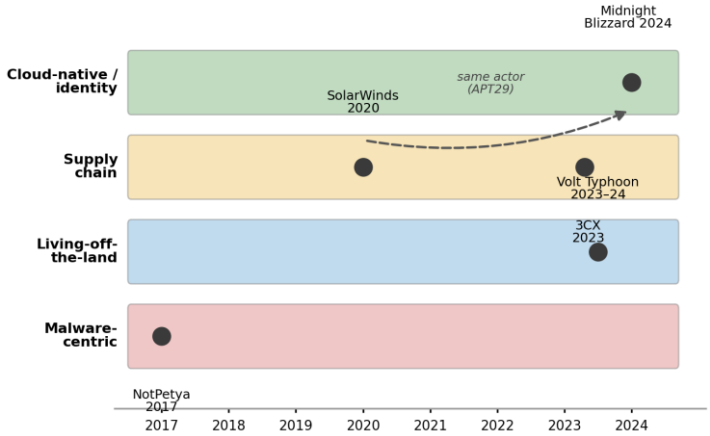


Figure 1: Four eras of APT tradecraft, 2017–2024, with APT29's cross-era trajectory

2.3 Formalizing Displacement versus Abandonment

The periodization in Section 2.1 can be formalized as a persistence score P, tracking how much of a technique's underlying objective survives a given defensive advance rather than being abandoned outright. For a defensive advance with detection coverage C of a specific technique, normalized to [0,1], and an adversary's demonstrated adaptation rate R toward an adjacent technique serving the same objective, also normalized to [0,1]:

$$P = 1 - C(1 - R) \quad (1)$$

P approaches 1 when an adversary fully displaces a newly detected technique onto an adjacent one (R near 1), meaning the underlying objective persists despite the defensive advance, and approaches 1−C when no adjacent technique is available (R near 0), meaning the objective is genuinely disrupted. Every case examined in Section 3 scores closer to the first outcome than the second, which is the empirical basis for this paper's central claim that improving defenses displace APT tradecraft rather than eliminate it.

3 Comparative Case Analysis

To test whether this analytical framework can be adapted to real-world practical scenarios, this section applies it to actual cases, and a total of five initiatives are selected to apply this framework. The time span of these initiatives ranges from 2017 to 2024, and they belong to four distinct country-affiliated actors. The selection of these five cases is not arbitrary, and there are two clear selection criteria. The first criterion is that all four development stages proposed in Section 2.1 must be covered, with none omitted. The second criterion is that, whenever conditions permit, it is preferable to be able to track the development trajectory of the same actor across more than one stage from these cases.

Table 1 collates the core details of each case, and the subsequent discussion will unpack the information transfer patterns that gradually emerge after comparing these cases side by side.

Table 1: Five APT campaigns, 2017–2024, mapped onto era, defensive trigger, and adaptation

Campaign (year)	**Actor**	**Era**	**Defensive trigger**	**Adversary adaptation**
NotPetya (2017)	Sandworm (Russia GRU)	Malware-centric	N/A (destructive wiper)	M.E.Doc update-channel trojan
SolarWinds (2020)	APT29 (Russia SVR)	Supply chain	Endpoint/perimeter detection maturing	Trusted vendor update (Sunburst)
3CX (2023)	Lazarus (North Korea)	Supply chain (cascading)	Single-vendor supply-chain vetting improving	Chained 2nd-vendor compromise
Volt Typhoon (2023–24)	PRC state-sponsored	Living-off-the-land	EDR / malware detection maturing	Native OS tools, no custom malware
Midnight Blizzard (2024)	APT29 (Russia SVR)	Cloud-native / identity	Network perimeter defenses maturing	OAuth / cloud-identity token abuse

The clearest illustration of displacement rather than abandonment is APT29's own trajectory. The group's SolarWinds campaign, disclosed in December 2020, compromised a trusted software vendor's build process to reach roughly 100 companies and nine federal agencies through a routine update channel (Cybersecurity and Infrastructure Security Agency, 2021). As detection of anomalous software supply-chain activity matured over the following three years, the same group — publicly tracked by Microsoft as Midnight Blizzard — shifted its initial-access approach entirely: the intrusion into Microsoft's own corporate environment, detected in January 2024, began with a password-spray attack against a forgotten test account and proceeded through abuse of an over-privileged legacy OAuth application, with no custom malware and no software supply chain involved at any stage (Microsoft Threat Intelligence, 2024). A joint advisory issued the following month confirmed this was not an isolated tactic but a broader pattern in the group's cloud-targeting activity (Cybersecurity and Infrastructure Security Agency, National Cyber Security Centre, et al., 2024). The underlying objective across both campaigns — durable, high-value access to a target's internal systems — did not change; the technique used to obtain it changed completely.

A second, complementary pattern appears in the supply-chain and living-off-the-land eras: displacement operates not only across an actor's own campaigns but within a single technique category, as adversaries push further into the category once its most basic form is defended against. The 2023 compromise of 3CX illustrates this within the supply-chain era: Mandiant's investigation found that the attackers, attributed to North Korea's Lazarus group, had reached 3CX not through a single compromised vendor but through a chain of two — first compromising a trading-software vendor, then using that access to compromise a 3CX employee and, from there, 3CX's own build environment — the first documented instance of a supply-chain compromise used to stage a second one (Mandiant, 2023). Volt Typhoon illustrates the same pattern within living-off-the-land activity: rather than a single intrusion, U.S. and international agencies documented sustained, multi-year prepositioning across critical infrastructure sectors using native administrative tools, resilient enough that the actor rebuilt its access after an initial disruption of its infrastructure in 2024.

Among the five cases we studied, the situations that arose were completely identical—not a single case deviated from this unified pattern. None of the defensive measures we examined one by one were able to completely eliminate the adversary’s original core objectives. These defenses did not actually stop the adversary from achieving their goals; they only forced the adversary to adopt a new set of action methods, and this new set of methods happened to fall into an entirely new category that the existing defense system had not yet covered. This pattern of the adversary always being able to bypass defenses, switch methods, and sustain their objectives is exactly the core content that the "persistence score" in Subsection 2.3 is specifically designed to record, and it is also the core foundation for the forward-looking judgment proposed in Section 4. Extrapolating from this unified pattern makes it very clear: if in all previous cases, it has consistently been that "the adversary only switched methods and never abandoned their original goals", rather than that "the defenses truly eliminated the adversary’s core objectives", then the domain where the adversary is most likely to

launch new actions next is precisely those categories that current defenses have not yet covered.

4 Forward-Looking Indicators for Anticipatory Defense

4.1 Recurring Displacement Patterns as Predictive Signal

If the persistence score in Section 2.3 is consistently high across historical cases, the practical implication for threat intelligence is to treat a currently effective defense not as a closed problem but as a predictor of where an actor's next adaptation is likely to appear. Concretely, this means tracking which ATT&CK tactic categories a given defensive investment covers well, and treating the adjacent, less-covered categories serving the same adversary objective as the higher-priority area for anticipatory detection engineering, rather than waiting for the first confirmed incident in that category before building detections for it. EDR adoption's own history illustrates the point: as endpoint detection matured against custom malware, adversaries increasingly targeted EDR agents directly, including through vulnerable-driver abuse to disable detection outright rather than evade it — a displacement onto the defensive tool itself rather than around it, which the framework in Section 2 would flag as a predictable next step once EDR coverage of conventional malware became reliable.

4.2 Candidate Next-Generation Evasion Vectors

Applying the same displacement logic forward, three categories currently less covered than their adjacent, well-defended alternatives stand out as plausible next-generation vectors. First, further identity- and cloud-permission abuse beyond the OAuth and token techniques already documented, particularly against the newer generation of cloud-native applications and service-to-service authentication that zero trust architectures are still in the process of covering. Second, continued and more automated living-off-the-land activity, since the fundamental asymmetry it exploits — that defenders cannot simply blacklist an operating system's own administrative tools — has no obvious technical fix. Third, AI-assisted tooling for reconnaissance and lure generation, which does not introduce a new tactic category in ATT&CK terms but plausibly increases the rate at which existing categories such as initial access and defense evasion are refined, compressing the time between a defensive advance and the adversary's displaced response. None of these projections is a prediction of a specific future incident; they are, consistent with the framework's purpose, statements about which categories warrant anticipatory detection investment now rather than after the fact.

5 Discussion and Limitations

The framework proposed here has real limits. The persistence score in Section 2.3 formalizes a pattern that this paper assesses qualitatively rather than through a validated quantitative scoring exercise; a fuller test would require coding a much larger sample of campaigns against consistent criteria for defensive coverage and adversary adaptation, which was beyond the scope of the five-case comparison here. The case selection is also skewed toward campaigns with public, high-confidence attribution and extensive government or vendor reporting, which favors a small number of well-resourced state

actors, particularly Russian and North Korean groups, over the larger population of less-documented intrusions; whether the same displacement pattern holds for actors that receive less sustained public scrutiny is accordingly untested here. Finally, the forward-looking indicators in Section 4 are extrapolations from a consistent historical pattern rather than certainties, and should be read as a prioritization tool for anticipatory detection engineering rather than as a forecast of specific incidents.

Conclusion

This paper set out to address a gap in how APT tradecraft is typically studied: treated campaign by campaign, existing research documents what adversaries have done well but says comparatively little about where a given actor's tradecraft is headed next. It developed a four-era longitudinal framework — malware-centric, living-off-the-land, supply-chain, and cloud-native — formalized through a persistence score, and mapped against the MITRE ATT&CK framework. Applied to five campaigns spanning 2017 to 2024, including a single actor's own trajectory from the SolarWinds supply-chain compromise to cloud-identity attacks on Microsoft's corporate environment, the analysis found a consistent pattern: defensive advances displaced adversary technique onto a less-covered adjacent category far more often than they eliminated the underlying objective. Building on this pattern, the paper proposed forward-looking indicators intended to help threat intelligence teams and detection engineers anticipate the next displacement before it is first observed in an incident, shifting practice from reactive, signature-based defense toward anticipatory, pattern-informed security architecture.

References

1. Cybersecurity and Infrastructure Security Agency. (2021, April 15). Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations (Alert AA20-352A). Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a
2. Cybersecurity and Infrastructure Security Agency, National Security Agency, & Federal Bureau of Investigation. (2023, May 24). People's Republic of China state-sponsored cyber actor living off the land to evade detection (Advisory AA23-144A). Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
3. Cybersecurity and Infrastructure Security Agency, National Cyber Security Centre, et al. (2024, February 26). SVR cyber actors adapt tactics for initial cloud access (Advisory AA24-057A). Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a
4. Mandiant. (2023, April 20). 3CX software supply chain compromise initiated by a prior software supply chain compromise; suspected North Korean actor responsible. Google Cloud Blog. Retrieved from https://cloud.google.com/blog/topics/threat-intelligence/3cx-software-supply-chain-compromise
5. Microsoft Threat Intelligence. (2024, January 25). Midnight Blizzard: Guidance for responders on nation-state attack. Microsoft Security Blog.

Retrieved from https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/

6. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology.
7. Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). MITRE ATT&CK: Design and philosophy. The MITRE Corporation.
8. U.S. Department of Justice, Office of Public Affairs. (2020, October 19). Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in cyberspace [Press release]. Retrieved from https://www.justice.gov/archives/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

CRISIS MANAGEMENT AS A GUARANTEE OF NATIONAL SECURITY

Kaloyan A. Iliev, Ivan K. Vladov

Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, k.a.iliev@abv.bg , ivankvladov@abv.bg

***Abstract**: The dynamic and unpredictable nature of the contemporary security environment has significantly increased the importance of crisis management as an integral component of national security. Globalization, technological advancement, climate change, hybrid threats, cyberattacks, pandemics, and geopolitical instability have expanded the spectrum of risks affecting the security and resilience of modern states.*

The effective crisis management is not merely a mechanism for mitigating the consequences of emergencies but a strategic instrument for safeguarding national interests, protecting critical infrastructure, ensuring societal continuity, and strengthening national resilience. The improving crisis management capabilities through modernization, digital transformation, international cooperation, and continuous institutional development significantly contributes to enhancing national security in an increasingly complex and uncertain global environment.

Consequently, crisis management has evolved from a reactive emergency response mechanism into a comprehensive strategic process encompassing prevention, preparedness, response, recovery, and adaptation.

***Keywords:** Crisis management, national security, resilience, risk management, emergency management, hybrid threats, critical infrastructure.*

Introduction

The international security environment in the 21st century is characterized by complexity, uncertainty, and multidimensional risks. Traditional military challenges are increasingly combined with natural disasters, industrial accidents, pandemics, cyberattacks, climate risks, disinformation, and hybrid operations. These risks can interact with each other and cause cascading consequences in the political, economic, social, technological, and environmental spheres.

Modern crises show that adverse events rarely remain within the responsibility of a single institution. A cyber incident can disrupt the functioning of energy, transport or healthcare; a natural disaster can disrupt communications and supply chains; a geopolitical conflict can cause humanitarian, economic and informational consequences far beyond the immediate area of confrontation. National security therefore depends not only on military capabilities, but also on the ability of institutions and society to anticipate, prevent, manage and overcome crises.

The aim of the study is to systematize the relationship between crisis management and national security and to identify the core capabilities required for effective crisis management. The analysis focuses on four interrelated areas: the crisis management cycle, institutional and inter-institutional coordination, the resilience and protection of critical infrastructure, and the role of technology. Special attention is paid to the Bulgarian context and the implications for national security.

Theoretical Aspects of Crisis Management

- **Concept and development**

A crisis can be defined as an emergency situation characterized by uncertainty, urgency, and high risk that threatens fundamental values, public safety, critical infrastructure, economic stability, or the normal functioning of institutions and requires decision-making with incomplete information and limited time.

Modern crises are characterized by their systemic nature. Their consequences can transcend organizational, sectoral, and national boundaries.

Crisis management is gradually evolving from a predominantly reactive model of civil protection and emergency response to a comprehensive management process. Its goal is no longer just to limit damage after a crisis, but to reduce vulnerabilities before it occurs, maintain essential functions during the crisis, and improve institutional effectiveness after it ends.

The crisis management cycle includes five interrelated phases: **prevention, preparedness, response, recovery and lessons learned (figure 1).**

Figure 1. The Crisis Management Cycle



Prevention involves identifying hazards and reducing vulnerabilities through risk assessment, planning and protective measures. Preparation involves developing plans, training personnel, conducting exercises, and providing resources and communication systems. Response focuses on saving lives, protecting property, maintaining essential services, and limiting the spread of the crisis. Recovery aims to rebuild affected communities, infrastructure, institutions, and economic activity. The final phase involves analyzing the actions taken, learning lessons, and implementing organizational improvements.

These phases should not be seen as isolated stages. Lessons learned from response and recovery should inform prevention and preparedness, and changes in the risk environment require continuous adaptation of plans and capabilities.

- **Sustainability and principles**

National resilience represents the strategic ability of the state and society to anticipate, tolerate, absorb, adapt and recover from disruptive events, while preserving the essential functions of government and society.

From a national security perspective, resilience reduces the opportunities for exploiting societal and institutional weaknesses through cyberattacks, disinformation, economic pressure, and hybrid operations. Therefore, investments in preparedness, system redundancy, public awareness, interagency collaboration, and critical infrastructure protection have both crisis and strategic effects.

Effective crisis management is based on several basic principles. Preparation creates the foundation through planning, training, exercises and resourcing. Prevention and risk mitigation reduce the potential consequences. A clear allocation of responsibilities and coordination are particularly important in crises requiring simultaneous action by multiple institutions. Flexibility allows for adaptation of actions as the situation changes. Timely information management and strategic communication reduce uncertainty and maintain public trust.

Crisis Management within the National Security System

- **Institutional architecture and inter-institutional coordination**

National security now goes beyond the traditional military dimension and includes political, economic, social, environmental, technological and information aspects. In this expanded context, crisis management represents a key national security capability, as it protects national interests, supports the continuity of state governance, reduces vulnerabilities and maintains public trust.

An effective institutional architecture operates at strategic, operational and tactical levels. Strategic authorities set policies, legal frameworks, priorities and resources. Ministries and specialized structures translate these decisions into sectoral plans and operational procedures. Regional and local authorities implement protective measures and provide initial response in affected areas.

The effectiveness of the system depends on interoperable communications, common procedures, regular exercises and clearly defined responsibilities.

Modern crises require both a Whole -of- Government and a Whole -of- Society approach . Government institutions, the military, police, intelligence agencies, emergency medical services, local authorities, and critical infrastructure operators must be able to share information and coordinate their decisions.

At the same time, the private sector, scientific organizations, non-governmental organizations, volunteer groups, media, and citizens have made significant contributions to preparedness, response, and recovery.

- **Armed Forces, Civil Protection and Critical Infrastructure**

In democratic societies, civilian authorities bear the primary responsibility for crisis management, while the armed forces can provide specialized capabilities in crises beyond the capabilities of civilian structures.

Military organizations have capabilities for strategic mobility, engineering support, logistics, communications, medical support, intelligence, and specialized personnel. Their support may include evacuation, disaster relief, transportation infrastructure restoration, temporary facility construction, medical assistance, logistical support, and protection of critical infrastructure.

Civil-military interaction must be based on clearly defined legal responsibilities, interoperable procedures and civilian control. Regular joint exercises are particularly important, through which weaknesses in communications, logistics, decision-making and resource allocation can be identified.

Critical infrastructure is a central element of national security. Energy, transportation, telecommunications, the financial sector, healthcare, water supply, and digital systems ensure the functioning of the state and the economy.

Protecting them requires risk assessment, system redundancy, physical security, cybersecurity, sustainable supply chains, and effective public-private collaboration.

- **NATO and European Union Perspectives**

NATO and the European Union increasingly view resilience and crisis preparedness as integral elements of security.

NATO places emphasis on civil preparedness, as collective defense depends on resilient civil infrastructure, secure transportation, reliable energy supplies, communications, and continuity of government.

The European Union is developing integrated mechanisms for civil protection, coordinated disaster response, cybersecurity and cross-border assistance. Both approaches confirm the understanding that modern crises cannot be managed solely through military instruments.

Crisis Management in the Republic of Bulgaria

The international resilience framework is of particular importance for Bulgaria. The country has built an institutional and regulatory framework for crisis management that combines national legislation, strategic planning and inter-institutional coordination with commitments within NATO and the European Union.

The National Security Strategy considers crisis management and resilience as important elements of national security, while **the National Defense Strategy of the Republic of Bulgaria for the period 2025–2035** emphasizes the deterioration of the regional security environment, hybrid threats, cyber risks, civil preparedness, civil-military interaction, and the protection of critical infrastructure.

The crisis management architecture in Bulgaria includes national and local authorities, ministries responsible for defense, interior, health, transport, environment, energy and digital governance, as well as regional and municipal structures.

The Directorate General for Fire Safety and Civil Protection plays a key role in prevention, warning, rescue activities and crisis response. The Bulgarian Armed Forces can assist civil authorities through engineering, transport, logistics, medical, communication and other capabilities.

The security environment in the Black Sea region further increases the importance of preparing for hybrid threats, cyber incidents, disinformation, supply chain disruptions, natural disasters, and other cascading risks.

Critical energy, transportation, communication, health, water and digital systems must be protected from both physical and cyber threats.

Further development of the Bulgarian system should be aimed at increasing interoperability, digital transformation, cybersecurity, resilience of critical infrastructure, strategic communication, professional training and conducting regular inter-institutional exercises.

Contemporary challenges and directions for development

- **Hybrid threats, information warfare and cybersecurity**

Hybrid threats combine military and non-military tools, including cyberattacks, disinformation, sabotage, economic pressure, and influence operations.

Their ambiguity makes it difficult to identify the perpetrator and make decisions. Information manipulation can increase panic, public polarization, and distrust during crises. Therefore, strategic communication and media literacy must be integrated into crisis preparedness and response.

Digital transformation creates significant opportunities, but also new vulnerabilities. Critical services increasingly depend on interconnected information systems, cloud technologies, industrial control systems and digital communications. Cybersecurity must be integrated into every phase of the crisis management cycle through vulnerability assessments, audits, response planning, training and secure information exchange.

- **Climate risks and disaster preparedness**

Climate risks are one of the long-term drivers of crises. Floods, wildfires, droughts and extreme weather events can affect infrastructure, food and water resources, public health and economic activity.

Therefore, disaster risk reduction must include sustainable infrastructure, environmental monitoring, early warning systems, sustainable spatial planning and population preparation.

- **Artificial Intelligence and Emerging Technologies**

Artificial intelligence, machine learning, satellite surveillance, unmanned systems, robotics, geographic information systems, and big data analysis can significantly improve situational awareness and decision support.

Artificial intelligence systems can process large volumes of information, identify patterns, aid in forecasting, and facilitate decision-making. Remote sensing and unmanned systems can speed up damage assessment, search and rescue, infrastructure inspection, and monitoring of hazardous areas.

However, these capabilities require cybersecurity, regulatory compliance, ethical oversight, and skilled personnel. AI systems can create risks related to transparency, accountability, algorithmic bias, and malicious influence.

Therefore, the human factor must remain at the forefront of strategic decisions, especially when the consequences concern human life or fundamental rights. The appropriate model is human-centric decision-making , in which technology supports, but does not replace, professional judgment and democratic accountability.

- **Strategic priorities**

Future developments must combine strategic forecasting and integrated risk assessment with interoperable digital systems, secure communications and decision support systems based on artificial intelligence.

Inter-institutional interaction should be strengthened through common operating procedures, joint exercises and integrated command and control mechanisms.

International cooperation within NATO and the European Union must remain a priority, as many of today's crises transcend national borders.

Professional education and continuous training are also key. Future crisis management professionals must combine leadership and management skills with competencies in risk analysis, cybersecurity, digital technologies, strategic communications, and international security.

At the societal level, ongoing public awareness and preparedness programs should increase preparedness and confidence. These measures create an adaptive system capable of learning from crises and continuously improving its capabilities.

Conclusion

Crisis management has become a strategic component of national security, not a function limited solely to emergency response. The complexity and interconnectedness of modern risks require states to integrate prevention, preparedness, response, recovery, and institutional learning into a single framework geared towards resilience.

The analysis shows that effective crisis management strengthens national security by reducing vulnerabilities, improving inter-institutional coordination, protecting critical infrastructure, and ensuring the continuity of essential state functions.

Resilience should be understood as the ability of a state and society to anticipate, tolerate, adapt and recover from disruptive events, while maintaining their vital functions.

The Bulgarian context confirms the need to align national capabilities with NATO and European Union resilience policies. Interoperability between institutions, civil-military cooperation, protection of critical infrastructure, cybersecurity, strategic communication, professional training and the responsible use of emerging technologies are particularly important.

Artificial intelligence and digital technologies offer significant opportunities for faster analysis, improved situational awareness and more efficient resource allocation, but they should support, not replace, professional judgment and democratic accountability.

Ultimately, prevention and preparation are more sustainable than relying solely on response. Therefore, crisis management should be seen as **a long-term investment in**

national resilience, national security, and the ability of the state and society to function effectively in the face of uncertainty.

References

1. Alexander, D. (2015). Disaster and emergency planning for preparedness, response, and recovery. Oxford University Press.
2. Aven, T. (2021). Risk, surprises and black swans. Routledge.
3. Bozov I., Petrov V., Elements of the planning process for nato crisis, disaster and emergency response exercises, International Scientific Conference ― Defense Technologies DefTech 2020, Faculty of Artillery, AD and CIS, 2020, Shumen, pp. 81-87, ISSN 2367-7902.
4. Boin, A., Hart, P., Stern, E., & Sundelius, B. (2021). The politics of crisis management: Public leadership under pressure (2nd ed.). Cambridge University Press.
5. Comfort, L. K. (2019). The dynamics of risk: Changing technologies and collective action in seismic events. Princeton University Press.
6. European Commission. (2024). Niinistö report: Safer together – Strengthening Europe's civilian and military preparedness and readiness.
7. European Union Agency for Cybersecurity (ENISA). (2024). ENISA threat landscape 2024.
8. International Organization for Standardization. (2019). ISO 22301:2019 security and resilience – Business continuity management systems – Requirements.
9. International Organization for Standardization. (2021). ISO 22361:2022 security and resilience – Crisis management – Guidelines.
10. Kapucu, N., & Ustun, Y. (2018). Collaborative crisis management and leadership in public administration. International Journal of Public Administration, 41(7), 548–561.
11. National Institute of Standards and Technology. (2024). NIST Cybersecurity Framework (CSF 2.0).
12. NATO. (2022). NATO 2022 Strategic Concept. Brussels, Belgium.
13. NATO. (2025). Crisis management.
14. OECD. (2024). Framework on management of emerging critical risks. OECD Publishing.
15. United Nations Office for Disaster Risk Reduction. (2015). Sendai framework for disaster risk reduction 2015–2030.
16. World Economic Forum. (2025). Global risks report 2025.
17. World Health Organization. (2023). Health emergency and disaster risk management framework.
18. Council of Ministers of the Republic of Bulgaria. (2018). National strategy for disaster risk reduction 2018–2030. Sofia, Bulgaria.
19. Council of Ministers of the Republic of Bulgaria. (2024). National security strategy of the Republic of Bulgaria. Sofia, Bulgaria.
20. Council of Ministers of the Republic of Bulgaria. (2025). National defence strategy of the Republic of Bulgaria (2025–2035). Sofia, Bulgaria.

21. Ministry of Defence of the Republic of Bulgaria. (2025). White paper on defence and the armed forces of the Republic of Bulgaria. Sofia, Bulgaria.
22. Ministry of Interior of the Republic of Bulgaria. (2024). National plan for disaster protection. Sofia, Bulgaria.
23. National Assembly of the Republic of Bulgaria. (2006). Disaster Protection Act. State Gazette, No. 102/2006 (as amended).
24. National Assembly of the Republic of Bulgaria. (2009). Defence and Armed Forces of the Republic of Bulgaria Act. State Gazette, No. 35/2009 (as amended).
25. National Assembly of the Republic of Bulgaria. (2019). Cybersecurity Act. State Gazette, No. 94/2018 (as amended).
26. State Agency for National Security. (2024). Annual report on the activities of the State Agency for National Security. Sofia, Bulgaria.

COMMAND AND CONTROL IN THE AGE OF ARTIFICIAL INTELLIGENCE

Kaloyan A. Iliev, Alexandra K. Vladova

Faculty of Artillery, Air Defense and Communication and Information Systems, National Military University, Shumen, Bulgaria, k.a.iliev@abv.bg , atanasova_aleksandra@abv.bg

***Abstract**: Artificial intelligence (AI) is becoming one of the factors that are changing the nature of modern military capabilities and the way in which command and control are implemented. The development of digital technologies, unmanned systems, sensors, communication networks and means for processing large data sets creates opportunities for significantly accelerating the information and analytical process. At the same time, the complexity of the operational environment is increasing and the need for timely decision-making in the face of incomplete, contradictory and rapidly changing information is increasing.*

Keywords: *Artificial intelligence, new challenges, military leader, technological transformations, make decisions, military education, ctrategic mhinking, practical advice.*

Introduction

NATO identifies artificial intelligence as an important technology for maintaining the Alliance's technological advantage, while setting requirements for legitimacy, accountability, explainability, reliability, manageability and limiting algorithmic bias (NATO, 2021, 2024). Therefore, the implementation of AI in the military sphere should be considered not only as a technological issue, but also as an organizational, personnel and leadership issue.

In this environment, Command and Control (C2) is becoming increasingly important. The effectiveness of a commander depends not only on the availability of forces and means, but also on the ability to receive timely reliable information, assess the situation, develop options for action and control the implementation of decisions. AI can support each of these stages through automated information processing, pattern detection, predictive analysis and presentation of results in a format suitable for command.

The purpose of this report is to analyze AI as a tool of military leadership with a leading emphasis on command and control in the Armed Forces of the Republic of Bulgaria. It examines the practical applications of AI, its impact on military decision-making, human-machine interaction, opportunities for the development of national capabilities, and the requirements for the future military leader.

Military Leadership and Command and Control in the Age of AI

Military leadership is traditionally based on the commander's ability to understand the situation, formulate a goal, organize the actions of subordinates and be responsible for the decisions made. Digitalization does not change this basic function, but it changes the information environment in which it is implemented. The commander increasingly has to work with large volumes of data, automated systems and various sources of information.

In this context, AI should be seen as a means of enhancing the information and analytical capabilities of the command. Its role is to shorten the time between receiving data and its transformation into useful information for the decision. This is especially important in situations where the time factor has a direct impact on the success of the operation.

The relationship can be represented as a sequence: information → analysis → situational awareness → assessment → decision → action → control. AI can support all stages, but should not be accepted as an autonomous carrier of command responsibility. It is this distinction that is fundamental for military leadership in the context of digitalization.

Practical applications of AI in command and control

- **Information collection and integration**

One of the most practical applications of AI is the automated integration and pre-processing of information from multiple sources. At the command post, data can come from intelligence assets, drones, radars, communications systems, reports from units, and other sensors. AI can help filter out duplicate or irrelevant information and highlight data that is potentially important for the current decision.

- **Analysis of the operational situation**

Once the data is integrated, AI can help analyze the operational environment. Algorithms for detecting changes, classifying objects, and identifying recurring patterns are particularly useful. This allows the headquarters to focus human analytical resources on the issues of highest importance.

- **Support for staff work**

AI can automate some of the routine activities in headquarters – structuring reports, extracting key information, comparing data, tracking tasks and preparing reference materials. The freed up time can be directed to more complex functions such as assessment, planning, coordination and control.

- **Forecasting analysis and evaluation of options**

Given sufficient reliable data, AI can assist in predictive analysis and comparison of action options. It is important to view the result as an analytical recommendation, not an automatic decision. The commander and staff must assess the assumptions, limitations, and risk associated with each option.

- **Control and feedback**

AI can help track the implementation of decisions by comparing planned and actual indicators. In case of deviations, the system can signal the command authority and help update the operational picture. This forms a continuous cycle between decision, implementation and feedback.

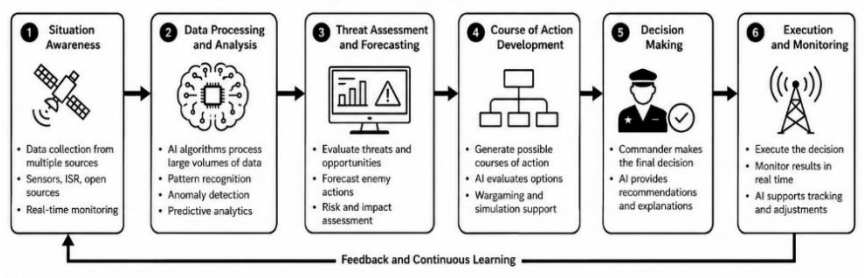


Figure 1. AI-Supported Military Decision-Making Proces

The figure shows that AI accelerates the information-analytical part of the process, while the final professional judgment and command decision remain a human function.

AI and the military decision-making process

Military decision-making is a central function of command. Traditionally, it involves assessing the situation, determining possible courses of action, assessing risk, making choices, and following up. The implementation of AI can reduce the time to complete information-analytical tasks without changing the principle of command responsibility.

The practical value of AI lies in its ability to assist the commander in dealing with information that exceeds the volume and speed of human processing. The system can suggest relationships between events, detect trends, and indicate areas that require additional attention.

The quality of the input data remains a critical factor. Inaccurate, incomplete, or manipulated data can lead to incorrect algorithmic results. Therefore, the commander should view AI as an assistive tool that requires professional verification and critical evaluation.

Human-machine interaction in the command and control system

Effective use of AI requires a clear division of functions between humans, headquarters, and the technological system. AI is particularly well-suited for rapid data processing and pattern recognition, while humans have the ability to make contextual judgments, lead, moral judgment, and take responsibility.

This model should not be understood as a confrontation between man and machine. On the contrary, the goal is to create a complementary interaction, in which AI increases the analytical capacity of the command, and the commander uses the results to form a reasoned decision.

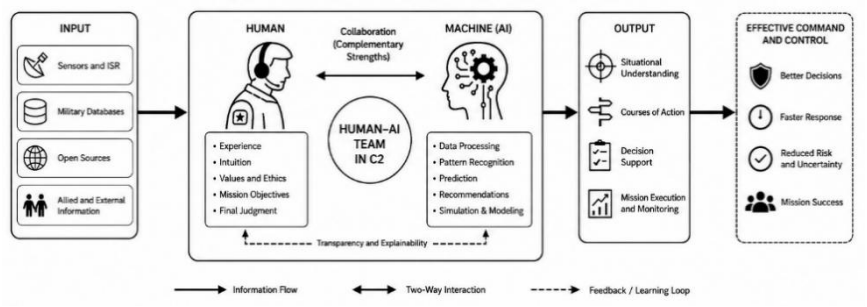


Figure 2. Human-Machine Interaction in Command and Control

Opportunities for the application of AI in the Armed Forces of the Republic of Bulgaria

For the Armed Forces of the Republic of Bulgaria, the implementation of AI should be considered as part of the digital transformation and the development of modern command and control capabilities. The national defense policy must combine technological solutions, personnel training, protected infrastructure, quality data and compatibility with allied systems.

- **Strategic level**

At the strategic level, AI can help analyze information from a wide range of sources, assess trends, and prepare options for developing defense capabilities. The main benefit is to improve the information base for strategic planning.

- **Operational level**

At the operational level, the prospects are related to building a common operational picture, integrating information from different types of armed forces, and supporting operational planning. AI can assist headquarters in processing large volumes of information and in tracking the dynamics of the operation.

- **Tactical level**

At the tactical level, AI can assist commanders through faster processing of information from the immediate environment, automated analysis of data from UAVs and other sensors, assistance with situational awareness, and management of available resources.

- **Joint Command and Control**

Of particular importance is the ability to connect the Army, Air Force, and Navy through a common information environment. From a military leadership perspective, this allows the commander to obtain a more comprehensive picture and assess the mutual influence of the actions of the various components.

- **Logistics, cyber defense and military education**

In logistics, AI can support forecasting needs and technical support. In cyber defense, it can support anomaly detection and early warning. In military education, AI can be integrated into command and staff training and simulations, allowing for more dynamic training of command staff.

It is important to distinguish between existing publicly confirmed capabilities and opportunities for future development. The implementation of AI should be phased and based on testing, evaluation, verification and validation of systems.

New requirements for the military leader

The development of AI is changing not so much the nature of military leadership as the tools with which it is implemented. A military leader must possess sufficient technological literacy to understand the capabilities and limitations of the systems used.

Particularly important are the ability to critically evaluate algorithmic results, understanding the risk of automation bias, the ability to work with an information-rich operational picture, and the ability to make decisions in the event of failure or limited availability of digital systems.

Thus, a need is being formed for a new type of digital military leadership, in which the commander does not become a programming specialist, but a competent user and critical evaluator of technological capabilities.

Ethical, legal and organizational aspects

Military applications of AI place high demands on human control and command responsibility. NATO has set out principles for the responsible use of AI, including legality, responsibility and accountability, explainability and traceability, reliability, manageability and limiting unwanted deviations (NATO, 2021, 2024).

In a command and control system, this means that the commander must be able to understand the role of AI in preparing a given recommendation, assess its reliability, and reject it when professional judgment or the operational situation dictates.

Organizationally, it is necessary to establish procedures for testing, evaluation and control, rules for working with data and mechanisms for action in the event of a technical failure. Technological dependence should not lead to a loss of command ability in a degraded information environment.

Prospects for the development of AI as a tool of command and control

The development of AI in the Armed Forces should be gradual and oriented towards specific command needs. Priority should be given to systems that provide a measurable effect on situational awareness, speed of information processing, and the quality of military decisions.

The practical model can be developed in five stages: first – building quality data, digital infrastructure and trained personnel; second – using AI for information support; third – integrating predictive analytics into C2; fourth – joint use of AI by different types of armed forces; and fifth – deepening alliance interoperability.

This approach is consistent with the emphasis of NATO's revised 2024 strategy on an AI-ready workforce, quality data, interoperability, and Testing, Evaluation, Verification and Validation capabilities (NATO, 2024).

Conclusion

Artificial intelligence is a significant tool for the development of military leadership and especially for the improvement of command and control. Its main value is not limited to the automation of individual activities, but lies in the ability to shorten the time between receiving information, its analysis and making a military decision.

Practical applications of AI in C2 include integration of information sources, analysis of the operational situation, support for staff work, forecasting, evaluation of options, resource management and performance control. For the Armed Forces of the Republic of Bulgaria, compatibility between the types of armed forces, the protected information environment and compliance with NATO standards and capabilities are of particular importance.

At the same time, the implementation of AI should not lead to a weakening of human control. The commander remains the bearer of professional judgment, makes the decision and bears responsibility for it. AI provides speed, analytical capabilities and warnings, but cannot replace human leadership, value judgment and responsibility.

Therefore, the main thesis of the report can be formulated as follows: the effective integration of artificial intelligence into the command and control system can increase the speed, quality and validity of military decisions, provided that human control and command responsibility remain paramount.

The future military leader will have to combine military-professional competence, leadership qualities, technological literacy, analytical thinking and ethical responsibility. It is the ability to combine human intelligence and artificial intelligence that will be one of the key factors for the effectiveness of command and control in the Armed Forces.

References

1. Antonov S., Bozov I., Artificial intelligence in automated design and engineering systems (CAD CAM CAE systems), International Scientific Conference ― Defense Technologies DefTech 2023, Faculty of Artillery, AD and CIS, 2023, Shumen, pp. 270-279, ISSN 2367-7902.
2. Baboş, A. (2021). Artificial Intelligence as a Decision Making Tool for Military Leaders. Land Forces Academy Review, 26(4), 269–273.
3. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L, 2024/1689.
4. Execrank.com. (2018). Artificial Intelligence (AI) - Challenges and Opportunities. [online] Available at: https://www.execrank.com/board-of-directors-articles/artificial-intelligence-ai-challenges-and-opportunities [Accessed 10 Jul. 2018].

5. Horowitz, M. (2018). Artificial Intelligence, International Competition, and the Balance of Power.
6. Mircheska, S. (2025). The Future of Military Leadership: How Artificial Intelligence Is Changing Military Conflict. Security and Defense, (1), 104–113.
7. Ministry of Defense of the Republic of Bulgaria. (2021). Program for the Development of the Defense Capabilities of the Armed Forces of the Republic of Bulgaria 2032. Ministry of Defense.
8. Ministry of Defense of the Republic of Bulgaria. (2025). National Defense Strategy. Ministry of Defense.
9. Menihardt, C.-F. (2025). Artificial Intelligence and Its Impact on Leaders and Leadership. Annals Academy of Romanian Scientists Series on Military Sciences, 17(1), 131.
10. NATO. (2021). Summary of the NATO artificial intelligence strategy. North Atlantic Treaty Organization.
11. NATO. (2024). Summary of NATO's revised artificial intelligence (AI) strategy. North Atlantic Treaty Organization.
12. US Department of Defense. (2023). Data, analytics, and artificial intelligence adoption strategy. US Department of Defense.
13. https://digital-strategy.ec.europa.eu/bg/policies/artificial-intelligence

Proceedings of International Scientific Conference "Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

RESILIENT NAVIGATION AND CONTROL OF STRIKE UAVS IN GNSS-DENIED AND ELECTROMAGNETICALLY CONTESTED ENVIRONMENTS

Jordan Alexiev

Faculty of Aviation, Georgi Benkovski Bulgarian Air Force Academy, Dolna Mitropolia, Bulgaria, alex.et@abv.bg

Abstract: *The paper examines navigation and flight-control resilience of strike unmanned aerial vehicles operating under GNSS degradation, denial, jamming and spoofing. A system-functional model is proposed in which navigation resilience is achieved by integrity monitoring, multisensor state estimation and controlled reconfiguration of the navigation and guidance functions. Four operating states are distinguished: nominal, degraded GNSS, GNSS-denied and recovery. The approach separates the availability of a sensor from confidence in its data and links navigation integrity to the admissible mode of trajectory control. The model provides a basis for deriving architecture and algorithm requirements without relying on a single navigation source.*

Keywords: *strike UAV, resilient navigation, GNSS-denied, electronic warfare, sensor fusion, integrity monitoring, reconfiguration*

УСТОЙЧИВА НАВИГАЦИЯ И УПРАВЛЕНИЕ НА УДАРНИ БЛА В GNSS-DENIED И РАДИОЕЛЕКТРОННО ОСПОРВАНА СРЕДА

Йордан Алексиев

Факултет „Авиационен", Висше военновъздушно училище „Георги Бенковски", гр. Долна Митрополия, България, alex.et@abv.bg

Резюме: *Разглежда се устойчивостта на навигацията и управлението на ударни безпилотни летателни апарати при деградация, недостъпност, заглушаване и подвеждане на GNSS. Предложен е системно-функционален модел, основан на контрол на достоверността, многосензорно оценяване на състоянието и управляема реконфигурация. Разграничени са четири режима: нормален, деградиран GNSS, GNSS-denied и възстановяване. Подходът свързва достоверността на навигационното решение с допустимия режим на траекторно управление и създава основа за извеждане на архитектурни и алгоритмични изисквания.*

Ключови думи: *ударен БЛА, устойчива навигация, GNSS-denied, радиоелектронно противодействие, сензорно обединяване, достоверност, реконфигурация*

1. Въведение

Нарастващата зависимост на безпилотните летателни апарати от спътниковата навигация превръща устойчивостта на позиционирането, навигацията и времето (PNT) в системен проблем, а не само в характеристика на GNSS приемника. Съвременните оценки на авиационната и отбранителната среда показват увеличаване на случаите на заглушаване и подвеждане на GNSS и поставят акцент

върху необходимостта от многоизточникови и системно устойчиви решения [1–3]. За ударния БЛА последствията са особено съществени, защото грешката в собственото местоположение се пренася към траекторното управление, географското привързване на сензорната информация и изпълнението на мисионния план.

GNSS-denied средата не трябва да се разбира единствено като пълно отсъствие на спътников сигнал. Практическият проблем обхваща спектър от състояния: намалена точност, загуба на сигнали от част от видимите спътници, ниска достоверност, временна недостъпност, широколентово заглушаване и приемане на правдоподобни, но неверни навигационни данни. Jamming и spoofing имат различна физическа природа, но и при двата случая критичният системен въпрос е дали бордовата система може своевременно да установи, че навигационният източник вече не трябва да се използва с предишната тежест [2,4].

Научният проблем е определянето на принципи за запазване на навигационната достоверност и управляемостта на ударния БЛА при променяща се наличност и качество на навигационната информация. Целта на изследването е да се предложи системно-функционален модел за устойчива навигация и управление, който свързва откриването на деградация, оценката на достоверността, многосензорното обединяване и реконфигурацията на управляващия контур. Акцентът не е върху конкретен тип платформа или конкретен навигационен алгоритъм, а върху архитектурната логика, която позволява автономно преминаване между нормален и деградирани режими.

2. GNSS/EW деградация и въздействие върху управлението

Класическият навигационен контур използва GNSS за ограничаване на натрупващата се грешка на инерциалната навигационна система. При краткотрайна загуба на спътникови измервания INS осигурява непрекъснатост, но грешките в положението и скоростта нарастват с времето. Визуалната одометрия, визуално-инерциалната навигация, LiDAR, теренното и образното съпоставяне, барометричните и радиовисотомерните измервания, както и сигнали от независими източници могат да ограничават дрейфа, но всяко средство има собствени зависимости от средата и ресурса [5–8]. Поради това съвременните обзори стигат до общ извод: няма единичен сензор, който да осигурява необходимата устойчивост във всички GNSS-denied условия; необходимо е обединяване на взаимно допълващи се източници [5,6].

При радиоелектронно противодействие трябва да се разграничат поне три вида деградация. Първият е загуба на наличност, при която GNSS решението изчезва или качеството му рязко пада. Вторият е деградация на точността, когато решение продължава да се формира, но с нарастваща грешка. Третият и най-опасен е загубата на достоверност, при която системата получава правдоподобна, но несъответстваща на реалното движение информация. Именно третият случай налага независима проверка на навигационните данни чрез динамични, сензорни и пространствени ограничения [2,4,9].

За ударния БЛА навигационната грешка влияе върху няколко функционални вериги едновременно: стабилизация и полет по траектория; оценка на оставащия ресурс и време; географско привързване на наблюденията; изпълнение на пространствени ограничения; синхронизация с други системи. Следователно устойчивостта трябва да се разглежда като свойство на цялата верига „сензор – оценка – навигационно решение – насочване – управление“, а не като локална функция на приемника.

В табл. 1 са обобщени основните форми на деградация и функционалните реакции, които следва да осигури автономната система.

Таблица 1: Основни форми на деградация и необходима функционална реакция

Източник / състояние	**Проява**	**Системен риск**	**Необходима реакция**
GNSS заглушаване	Ниско C/N_0, загуба на измервания	Загуба на абсолютна корекция	Изолиране на GNSS; преминаване към независими източници
GNSS spoofing	Правдоподобно, но несъгласувано решение	Скрито отклонение на траекторията	Проверка на достоверност; кръстосана валидация; отхвърляне
INS дрейф	Нарастваща грешка с времето	Постепенна загуба на позиционна точност	Корекция чрез външни/сценови измервания
Визуална деградация	Нисък контраст, дим, облачност, еднообразен терен	Ненадеждна визуална одометрия	Намаляване на тежестта; друг сензорен канал
Отказ/ресурсно ограничение	Липса на сензор или изчислителна функция	Непълен навигационен набор	Реконфигурация и ограничен режим на управление

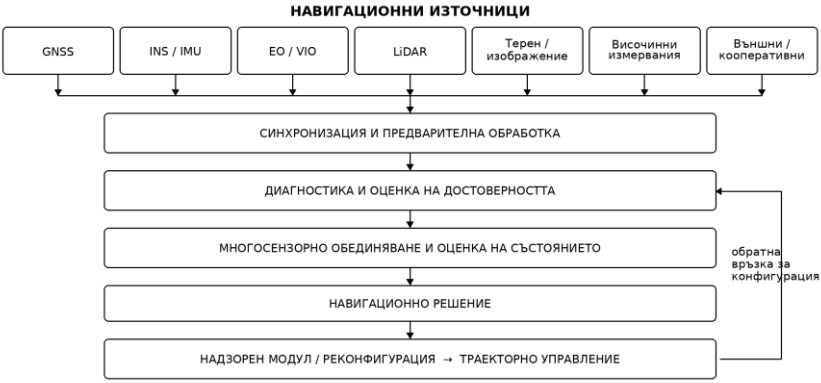
3. Системно-функционален модел за устойчива навигация

Като входни източници моделът може да използва GNSS, INS/IMU, визуални и визуално-инерциални средства, LiDAR, теренно и образно съпоставяне, височинни измервания и външни или кооперативни навигационни данни. Конкретният набор не е фиксиран; устойчивостта се определя от способността на архитектурата да оценява достоверността на източниците, да ги обединява и да се реконфигурира при деградация.

Предложеният модел се основава на три принципа. Първо, наличността на измерване не е равнозначна на неговата достоверност. Второ, навигационното решение трябва да бъде резултат от контролирано обединяване на източници с различна и променяща се надеждност. Трето, режимът на управление трябва да бъде съобразен с текущата достоверност на оценката за състоянието. Така устойчивостта се реализира не чрез опит за запазване на всяка функция на всяка

цена, а чрез поддържане на минимално необходимото информационно качество за безопасно и мисионно допустимо управление.

Архитектурно моделът последователно свързва предварителната обработка, диагностиката и оценката на достоверността, многосензорното обединяване, формирането на навигационно решение и надзорната реконфигурация с траекторното управление. Фиг. 1 представя тази логика заедно с основните групи навигационни източници. Надзорният модул не замества алгоритъма за оценка на състоянието, а управлява конфигурацията на източниците и допустимото използване на полученото навигационно решение.



Фигура 1: Функционална архитектура на устойчива навигация и управление

Тази структура разделя два въпроса, които често се смесват. Първият е „каква е най-добрата оценка на положението в момента“, а вторият – „достатъчно надеждна ли е тази оценка за конкретното управляващо действие“. Именно вторият въпрос е критичен при оспорвана електромагнитна среда. Ако системата не може да различи висока точност от висока достоверност, тя може да продължи да управлява по формално „валидно“, но подвеждащо решение.

4. Многосензорна интеграция и оценка на достоверността

Многосензорната интеграция при GNSS-denied навигация обикновено комбинира високочестотната непрекъснатост на инерциалните измервания с периодични корекции от независими източници. Визуално-инерциалните и LiDAR-визуално-инерциалните архитектури са сред активно изследваните решения, тъй като използват геометрията на средата за ограничаване на инерциалния дрейф [6,7]. За малки БЛА обаче тяхното приложение се ограничава от маса, енергия, изчислителен ресурс, динамиката на платформата и качеството на сцената. Поради това при ударен БЛА по-важен е принципът на взаимното допълване на сензорите, отколкото фиксираният набор от сензори.

Оценката на достоверността трябва да предшества или да съпътства обединяването. Практически тя може да използва няколко групи признаци: качество на самото измерване; съгласуваност с прогнозата на движението; съгласуваност между независими сензори; времева устойчивост; физическа правдоподобност и геометрични ограничения. Приемането или отхвърлянето на GNSS само по флаг „има/няма решение“ е недостатъчно при spoofing, защото подвеждащото решение може да изглежда непрекъснато и статистически гладко [4,9].

Следователно във всеки момент системата следва да поддържа не само оценка на състоянието, но и оценка на качеството на тази оценка. Тази метаинформация може да се разглежда като навигационна увереност, формирана от наличността, достоверността и степента на взаимна съгласуваност. Тук не се предлага универсален числов праг: конкретните прагове са зависими от платформата, мисията, сензорния набор и допустимата грешка. Предлага се принципът, че преминаването към по-ограничен режим се задейства от загуба на достоверност, а не едва след пълна загуба на навигационно решение.

5. Реконфигурация на навигацията и управляващия контур

Реконфигурацията представлява целенасочена промяна на използваните източници, алгоритми и ограничения върху управлението при установена деградация. За системния анализ са достатъчни четири режима. В нормален режим GNSS участва като един от основните източници за абсолютна корекция и всички планирани функции са достъпни. В режим „деградиран GNSS“ измерванията продължават да се приемат, но тежестта им се намалява и се засилва независимата проверка. В GNSS-denied режим спътниковите измервания се изолират и решението се поддържа чрез INS и достъпните независими източници. Режимът на възстановяване се въвежда, за да се избегне незабавното повторно доверяване на GNSS след кратко появяване на сигнал.

Тези режими са представени в табл. 2. Те не са „нива на автономност“, а състояния на навигационната архитектура, които могат да се реализират с различна алгоритмична сложност.

Таблица 2: Режими за реконфигурация на навигацията и управлението

Режим	**Условие**	**Навигационна конфигурация**	**Управляващо следствие**
S0 Нормален	GNSS и другите източници са съгласувани	GNSS/INS + налични допълващи измервания	Номинално траекторно управление
S1 Деградиран	Съмнение или частична деградация на GNSS	Намалена тежест на GNSS; засилена проверка	Запазване на мисията с повишен контрол
S2 GNSS-denied	GNSS е недостъпен или недостоверен	INS + независими сценови/други измервания	Ограничения според натрупаната неопределеност

Режим	**Условие**	**Навигационна конфигурация**	**Управляващо следствие**
S3 Възстановяване	GNSS отново е наличен	Постепенна повторна валидация и включване	Връщане към номинален режим след потвърждение

Съществена особеност е връзката между навигационната неопределеност и допустимото траекторно поведение. При нарастваща неопределеност системата не трябва автоматично да запазва всички мисионни режими. Може да се наложи ограничаване на маневреността, преминаване към предварително проверена геометрия на маршрута, използване на по-консервативни пространствени ограничения или прекратяване на конкретен етап. Тази логика превръща навигационната устойчивост в част от управлението на мисията, без да смесва навигационния контур с решенията на по-високо мисионно ниво.

От архитектурна гледна точка реконфигурацията следва да бъде двустранна. Отдолу нагоре диагностиката и оценката на достоверността информират надзорния модул за реалното качество на навигационната информация. Отгоре надолу текущият режим и ограниченията на мисията определят какво качество на навигационното решение е минимално допустимо. Това позволява една и съща платформа да използва различни комбинации от сензори и ограничения в различни фази, без да се приема, че „GNSS-denied“ е един постоянен и еднозначен режим.

6. Особености при ударни БЛА

При ударните БЛА устойчивостта на навигацията трябва да се оценява не само по средната позиционна грешка, а по способността да се запази контролируемо и предвидимо поведение при частична загуба на информация. Особено значение имат три свойства. Първото е автономното разпознаване на деградацията, тъй като комуникационният канал към оператор може също да бъде ограничен. Второто е ограничаването на разпространението на грешка от навигационния към мисионния контур. Третото е способността за безопасно преминаване към ограничен, но безопасен набор от функции, когато пълното изпълнение вече не е подкрепено от наличната информация.

Този подход е съвместим с по-широкото разбиране за функционална автономност: отделните функции на системата могат да запазват различна степен на самостоятелност при деградация. Например управлението на полета може да остане напълно автономно, докато географското привързване на външни обекти временно има по-ниска достоверност. Така се избягва бинарното описание „автономен/неавтономен“ и се получава реалистичен модел на остатъчните способности.

От гледна точка на авиационното въоръжение съществено е разграничаването между устойчивост на собствената навигация и достоверност на данните, използвани от средствата за насочване. Двете са свързани, но не са идентични. Грешка в положението на носителя може да повлияе на геопривързани функции, но определени бордови сензорни режими могат да поддържат относително наблюдение независимо от абсолютното GNSS решение. Следователно

архитектурата трябва да пази произхода, качеството и референтната система на информацията, вместо всички данни да се третират като еднакво достоверни.

7. Дискусия

Предложеният модел има три основни предимства. Първо, премества фокуса от „заместване на GNSS“ към управление на достоверността на навигационната информация. Второ, свързва многосензорното обединяване с реконфигурацията на управляващия контур, така че деградацията да води до определено системно поведение. Трето, позволява архитектурните изисквания да се извеждат независимо от конкретен набор сензори: необходимите функции са диагностика, независима проверка, обединяване, оценка на неопределеността и контролирано превключване на режими.

Ограничението на настоящото изследване е концептуалният характер на модела. Не се определят универсални числови прагове за навигационна достоверност, допустим дрейф или време за работа без абсолютна корекция, защото тези параметри зависят от платформата, динамиката, мисията и сензорната конфигурация. Следващо равнище на изследване е формализиране на показателите за навигационна достоверност и експериментално сравнение на различни конфигурации при сценарии на последователна деградация.

Заключение

Устойчивата навигация на ударен БЛА в GNSS-denied и радиоелектронно оспорвана среда не се свежда до използване на резервен навигационен източник. Необходима е системна архитектура, която разпознава деградацията, оценява достоверността на разнородните измервания, формира многосензорно навигационно решение и реконфигурира режима на управление според реалното качество на информацията.

Предложен е системно-функционален модел с четири режима – нормален, деградиран GNSS, GNSS-denied и възстановяване. Основният извод е, че устойчивостта се определя от способността да се запази достатъчно достоверно навигационно решение и съответстващ му режим на управление, а не непременно от непрекъсната наличност на GNSS. Подходът създава основа за последващо извеждане на конкретни архитектурни, сензорни и алгоритмични изисквания към автономни ударни БЛА.

Литература

1. NATO. “NATO addresses electromagnetic interference threats to civil aviation safety.” NATO News, 8 May 2025.
2. NATO Communications and Information Agency. “NCIA and NSPA join forces to test new sensor to counter GNSS signal threats and improve NATO’s situational awareness.” 24 Apr. 2025.
3. European Space Agency. “No signal left behind: new ways to detect jamming and spoofing.” 25 Aug. 2026.

4. European Union Agency for the Space Programme. “Galileo Open Service Navigation Message Authentication (OSNMA).” 2026.
5. Jarraya, I., et al. “GNSS-denied unmanned aerial vehicle navigation: analyzing computational complexity, sensor fusion, and localization methodologies.” Satellite Navigation, vol. 6, 2025, art. 9. https://doi.org/10.1186/s43020-025-00162-z.
6. Alqudsi, Y., Alameri, A., Abdallah, A. M., and Ahmed, G. “State-of-the-art and future directions in autonomous navigation for UAVs in GNSS-denied environments: A comprehensive review of techniques, architectures, and applications.” Information Fusion, 2026, 104714. https://doi.org/10.1016/j.inffus.2026.104714.
7. “LiDAR-Visual-Inertial Fusion Architectures for GNSS-Resilient Aerial Navigation: Performance Assessment.” IEEE/AIAA Digital Avionics Systems Conference, 2025. https://doi.org/10.1109/DASC66011.2025.11257343.
8. Rozhak, Y. R., and Havano, B. I. “Research of Existing Sensor Data Fusion Methods for Autonomous Navigation of Unmanned Aerial Vehicles (UAVS).” Computer Systems and Networks, vol. 8, no. 1, 2026, pp. 219–228. https://doi.org/10.23939/csn2026.01.219.
9. Jiang, C., Zhou, X., Chen, H., and Liu, T. “UAV Positioning Using GNSS: A Review of the Current Status.” Drones, vol. 10, no. 2, 2026, 91. https://doi.org/10.3390/drones10020091.
10. European Space Agency. “ESA teams up with Leonardo against satnav jamming.” 16 June 2025.

CLASSIFICATION OF AUTONOMOUS FUNCTIONS IN STRIKE UAVS

Jordan Alexiev

Faculty of "Aviation", "Georgi Benkovski" Bulgarian Air Force Academy, DolnaMitropolia, Bulgaria,alex.et@abv.bg

Abstract: *Strike unmanned aerial vehicles increasingly operate under navigation, communication, sensing and mission uncertainties that limit conventional remote and pre-programmed control. The paper identifies the main vulnerabilities of control and guidance systems and proposes a system-functional classification of autonomous functions into eight interconnected classes. The classification separates function from level of autonomy and provides a basis for mission-dependent autonomy profiles, architecture design and algorithm selection.*

Keywords: *strike UAV, autonomy, autonomous functions, navigation, mission management, resilient autonomy, cooperative autonomy*

КЛАСИФИКАЦИЯ НА АВТОНОМНИТЕ ФУНКЦИИ ПРИ УДАРНИ БЛА

Йордан Алексиев

Факултет „Авиационен" ,Висше военновъздушно училище „ГеоргиБенковски", гр. Долна Митрополия, Република България, alex.et@abv.bg

Резюме: *Ударните безпилотни летателни апарати все по-често действат при навигационна, комуникационна, сензорна и мисионна неопределеност, които ограничават дистанционното и предварително програмното управление. В статията са систематизирани основните уязвимости на системите за управление и насочване и е предложена системно-функционална класификация в осем взаимосвързани класа. Разграничават се автономна функция и степен на автономност, като се създава основа за мисионно-зависими профили, архитектура и алгоритми.*

Ключови думи: *ударен БЛА, автономност, автономни функции, навигация, управление на мисията, устойчива автономност, кооперативна автономност*

Въведение

Развитието на ударните безпилотни летателни апарати (БЛА) се характеризира с прехвърляне на все повече функции от оператора и наземната станция към бордовите изчислителни средства. Причината е не само технологичното развитие, а и нарастващата уязвимост на традиционното управление: деградация на навигационната поддръжка, прекъсване на командно-информационния обмен, ограничена достоверност на сензорните данни, противодействие по маршрута, откази на бордови подсистеми и динамично изменение на бойната обстановка. При тези условия способността за самостоятелно възприемане, оценяване, планиране и адаптиране се превръща в условие за запазване на изпълнимостта на мисията.

Съществуващите подходи описват автономността чрез нива, степен на човешко участие или функционални способности. Рамката ALFUS я свързва със сложността на мисията, средата и човешкото взаимодействие [5], а НАСА предлага функционално разлагане на автономните системи, включващо възприемане, оценяване на състоянието, планиране, изпълнение и диагностика [4]. Европейската агенция по отбрана развива подхода „автономност като функция“, според който различните функции на една система могат да имат различна степен на автономност [2,3]. Във военен контекст допълнително значение имат човешкият контрол, надеждността и ограниченията на автономното поведение [1,8].

Научният проблем е системното разграничаване и групиране на автономните способности на ударния БЛА и свързването им с мисионните изисквания, архитектурата и алгоритмите. Целта на изследването е да се предложи системно-функционална класификация на автономните функции при ударни БЛА. За постигането ѝ се анализират принципите за управление и основните уязвимости на системата за управление и насочване, формулират се критерии за класифициране и се определят основни класове според функционалния резултат на съответните автономни способности.

1. Развитие на принципите за управление

За целите на изследването системите за управление могат условно да се подредят според нарастващата самостоятелност на бордовата система: дистанционно, програмно, функционално автономно, мисионно автономно и кооперативно/разпределено управление. Това подреждане не представлява универсална скала на автономност, а показва преместването на част от функциите за възприемане, оценяване, планиране и действие от оператора към БЛА.

При дистанционното управление качеството на командно-информационния канал е критично. Програмното управление намалява тази зависимост, но следва предварително зададена логика. Функционалната автономност прехвърля към борда отделни функции - навигация, възприемане, проследяване, планиране или диагностика. Мисионната автономност разширява самостоятелността до планиране и адаптиране на изпълнението в рамките на зададени цели и ограничения. При групови системи възникват и функции за обмен на информация, координация и разпределение на задачи [7,8].

2. Основни уязвимости на системата за управление и насочване

Необходимостта от автономни функции се проявява най-ясно чрез основните уязвимости на системата за управление и насочване на ударния БЛА. Първата група обхваща определянето на собственото местоположение и положението на целта. Сигналите на глобалните навигационни спътникови системи (ГНСС) могат да бъдат заглушавани или подвеждани, инерциалната навигационна система натрупва грешка, а визуалното и теренното съпоставяне зависят от качеството на наблюдаваната сцена, метеорологичните условия и наличната картографска информация [6,10].

Втората група обхваща комуникациите и командно-информационния обмен - прекъсване, заглушаване, ограничена пропускателна способност и закъснения. Третата е свързана със средствата за възприемане и разпознаване на обстановката, при които непълни или противоречиви сензорни данни, сложен фон, динамични обекти и примамки могат да доведат до неправилна оценка [9]. Четвъртата група е противодействието по маршрута - зони за откриване, радиоелектронно противодействие и противовъздушна отбрана, които изменят риска и могат да направят предварително зададения маршрут или план неадекватен.

Петата група включва откази и деградация на сензори, навигационни, комуникационни и изчислителни модули, както и ограничения на енергията и други ресурси. Шестата е уязвимостта на предварително зададената логика на мисията: при промяна на цел, маршрут, ограничения или състав на групата предварително програмираното поведение може да стане недостатъчно. Така основните източници на потребност от автономност могат да се обобщят като: навигация и насочване към целта; комуникации; възприемане на средата; противодействие; откази и ресурсни ограничения; динамика на мисията. Връзката между тези уязвимости и необходимите автономни функции е обобщена в табл. 1.

Таблица 1. Основни уязвимости и потребности от автономни функции

Област	**Типичен проблем**	**Необходима автономна функция**
Местоположение и насочване към целта	Деградация на ГНСС; натрупване на грешка в ИНС	Автономно определяне на положението; многосензорна навигация
Комуникации	Прекъснат или ограничен командно-информационен обмен	Управление на връзката; автономно продължаване в зададени граници
Възприемане на средата	Непълни, шумни или противоречиви сензорни данни	Откриване и проследяване; обединяване на данни; оценка на достоверност
Противодействие	Промяна на зони за откриване, РЕБ и ПВО	Ситуационна оценка; оценка на риска; адаптация и препланиране
Бордови системи	Откази, деградация и ресурсни ограничения	Самодиагностика; преконфигуриране; управление на ресурсите
Динамика на мисията	Промяна на задача, цел, ограничения или състав	Мисионно препланиране; преразпределение на задачи

3. Принципи за класифициране на автономните функции

В настоящото изследване автономна функция се определя като функционално обособена способност на БЛА да възприема и обработва информация, да оценява собственото състояние и средата, да формира или избира допустимо действие и/или да го изпълнява в зададени граници без непосредствено управление от оператор. Автономната функция отговаря на въпроса „какво може системата да извършва самостоятелно“, а степента на автономност - „до каква степен го

извършва без човешка намеса“. Следователно функцията и степента на автономност са различни характеристики.

Класифицирането се основава на четири принципа: (1) основен функционален резултат; (2) място във функционалния цикъл „възприемане - оценка - планиране - действие“; (3) обект на управление - собствено състояние, среда, мисия, комуникации, група или взаимодействие с човека; (4) минимизиране на припокриването между класовете. Водещ е първият принцип: една функция се отнася към класа, чийто основен резултат тя формира. По този начин припокриващите се функции се отнасят към класа, определен от техния основен функционален резултат.

4. Класификация на автономните функции при ударни БЛА

На тази основа се предлага класификация в осем взаимосвързани функционални класа. Те не представляват последователни нива на автономност: конкретен БЛА може да притежава висока самостоятелност в една функция и ограничена в друга. Класификацията определя основните функционални области на автономността, за всяка от които може да се задава различна степен на автономност в зависимост от мисията и средата.

4.1. Автономни функции за полет и навигация

Обхващат стабилизацията и управлението на полета, определянето на положение и ориентация, изпълнението на зададена траектория, локалното избягване на препятствия и поддържането на навигационно решение при деградация на външни източници. Основният резултат е надеждно пространствено движение на БЛА. Планирането и препланирането на мисията не се включват в този клас, освен когато се отнасят до локално безопасно движение.

4.2. Автономни функции за сензорно възприемане

Включват управление на бордовите сензори, предварителна обработка, откриване, локализиране, класификация, идентификация и проследяване на обекти. Основният резултат са структурирани наблюдения за обекти и техните характеристики, които служат като вход към последващата ситуационна оценка.

4.3. Автономни функции за информационно обединяване и ситуационна оценка

Преобразуват наблюденията, външните данни и оценките за собственото състояние в текущ модел на обстановката. Включват съпоставяне и обединяване на информация, оценка на достоверността и неопределеността, разпознаване на събития и оценка на риск. Основният резултат е интерпретирана ситуационна картина, а не отделно сензорно наблюдение.

4.4. Автономни функции за планиране и управление на мисията

Обхващат структуриране на задачата, определяне на последователност от действия, планиране и препланиране на мисионно ниво, избор между допустими варианти и управление на ресурсите. Основният резултат е мисионно решение и план за действие, формирани в рамките на зададените от оператора цели и ограничения.

4.5. Автономни функции за устойчивост, самодиагностика и преконфигуриране

Включват откриване на аномалии и откази, диагностика, оценяване на техническата деградация, преминаване към резервни или ограничени режими и преконфигуриране на достъпните средства. Основният резултат е запазване на остатъчната способност на системата и възможност за безопасно продължаване, изменение или прекратяване на мисията.

4.6. Автономни комуникационни и мрежови функции

Включват управление на комуникационните връзки и информационния обмен, приоритизиране на данните и адаптиране към променящо се качество или прекъсване на свързаността. Основният резултат е поддържане на необходимата информационна свързаност; решенията за разпределение на задачи между няколко БЛА принадлежат към кооперативните функции.

4.7. Автономни кооперативни и колективни функции

Обхващат споделяне и съгласуване на ситуационна информация, съвместно възприемане, разпределение и преразпределение на задачи, координация и разпределено планиране. Основният резултат е съгласувано групово поведение, което не може да бъде сведено до автономността на отделния БЛА.

4.8. Функции за взаимодействие човек - автономна система

Обхващат задаване на цели и ограничения, представяне на състоянието, увереността и риска, надзор, разрешаване на критични действия, намеса и поемане или предаване на управление. Основният резултат е ясно разпределение на правомощията и информационното взаимодействие между оператора и автономната система. Обобщената системно-функционална класификация е представена в табл. 2.

Таблица 2. Системно-функционална класификация на автономните функции

Код	**Клас**	**Основни функции**	**Функционален резултат**
АФ-1	Полет и навигация	Управление на полета; положение; траектория; локално избягване	Пространствено движение
АФ-2	Сензорно възприемане	Сензори; откриване; класификация; идентификация; проследяване	Структурирани наблюдения
АФ-3	Информационно обединяване и ситуационна оценка	Обединяване; достоверност; неопределеност; събития; риск	Ситуационна картина
АФ-4	Планиране и управление на мисията	Задачи; план; препланиране; избор; ресурси	Мисионно решение и план
АФ-5	Устойчивост, самодиагностика и преконфигуриране	Аномалии; откази; диагностика; деградация; резервни режими	Остатъчна способност

АФ-6	Комуникационни и мрежови	Връзки; обмен; приоритет; адаптация към свързаността	Информационна свързаност
АФ-7	Кооперативни и колективни	Споделяне; задачи; координация; разпределено планиране	Съгласувано групово поведение
АФ-8	Човек - автономна система	Цели; ограничения; надзор; разрешаване; намеса	Разпределение на правомощията

5. Взаимодействие между автономните функции

Класовете не действат изолирано. Сензорното възприемане (АФ-2) формира наблюдения, които чрез информационно обединяване и ситуационна оценка (АФ-3) се превръщат в модел на обстановката. Планирането и управлението на мисията (АФ-4) използват този модел за избор и актуализиране на действията, а функциите за полет и навигация (АФ-1) реализират пространственото изпълнение. Взаимодействието между основните функционални класове е представено на фиг. 1, като устойчивостта (АФ-5), комуникационните и мрежовите функции (АФ-6), кооперативните функции (АФ-7) и взаимодействието човек - автономна система (АФ-8) имат напречен характер и влияят върху целия функционален цикъл.



Фигура 1: Взаимодействие между основните класове автономни функции

От тази структура следва, че автономността е многомерна характеристика. Автоматичното управление на полета не означава мисионна автономност, както и автономното откриване на обект не означава самостоятелно планиране на мисията. Поради това ударният БЛА е по-коректно да се описва чрез набор от автономни функции и степента на автономност на всяка от тях, а не чрез единно ниво за цялата система.

6. Дискусия

Предложената класификация създава причинно-следствена връзка между уязвимостите на системата и функционалните средства за тяхното компенсиране. Навигационната деградация изисква автономни функции за определяне на положение и поддържане на движение; ограничената свързаност - комуникационна адаптация и мисионна самостоятелност; непълната сензорна информация - възприемане, обединяване и оценка на достоверността; динамичната среда - ситуационна оценка и препланиране; отказите - самодиагностика и преконфигуриране; груповото действие - кооперативни функции. Това показва, че необходимият набор от функции се определя от конкретните уязвимости, мисията и средата.

Класификацията е концептуална и не задава количествени степени на автономност. Тя съзнателно не развива подробно типовете мисии, конкретните архитектури и алгоритми. Следващото равнище на изследване е формиране на мисионно-зависим функционален профил, при който за всеки клас се определя необходимата степен на автономност и ролята на оператора.

Заключение

Систематизирани са основните уязвимости на системите за управление и насочване на ударни БЛА и е показана причинно-следствената връзка между тях и необходимостта от автономни функции. Предложена е системно-функционална класификация в осем класа, разграничени според основния функционален резултат: полет и навигация; сензорно възприемане; информационно обединяване и ситуационна оценка; планиране и управление на мисията; устойчивост, самодиагностика и преконфигуриране; комуникационни и мрежови функции; кооперативни и колективни функции; взаимодействие човек - автономна система.

Основният извод е, че функционалният обхват и степента на автономност са две различни характеристики на ударния БЛА. Предложеният подход позволява системата да се описва чрез функционален профил и създава основа за последващо определяне на необходимата степен на автономност за конкретни мисии, както и за извеждане на архитектурни и алгоритмични изисквания.

Използвана литература

1. Department of Defense. (2023). DoD Directive 3000.09: Autonomy in Weapon Systems.
2. European Defence Agency. (2024). EDA Action Plan on Autonomous Systems (APAS).
3. European Defence Agency. (2026). Autonomous Systems Taxonomy: Autonomy as a Function. https://eda.europa.eu/what-we-do/eu-policies/autonomous-systems/taxonomy
4. Fong, T. W., Frank, J. D., Badger, J. M., Nesnas, I. A., & Feary, M. S. (2018). Autonomous Systems Taxonomy. NASA Technical Report 20180003082.
5. Huang, H.-M., Messina, E., & Albus, J. (2007). Autonomy Levels for Unmanned Systems (ALFUS) Framework, Volume II: Framework Models

Version 1.0. NIST Special Publication 1011-II-1.0. https://doi.org/10.6028/NIST.SP.1011-II-1.0

6. Jiang, C., Zhou, X., Chen, H., & Liu, T. (2026). UAV Positioning Using GNSS: A Review of the Current Status. Drones, 10(2), 91. https://doi.org/10.3390/drones10020091
7. Michailidis, E. T., & Karanasiou, I. S. (2026). A Review of AI-Enabled UAV-Based Systems for Defense Applications. Drones, 10(8), 602. https://doi.org/10.3390/drones10080602
8. NATO. (2022). Summary of NATO's Autonomy Implementation Plan.
9. Tang, G., Ni, J., Zhao, Y., Gu, Y., & Cao, W. (2024). A Survey of Object Detection for UAVs Based on Deep Learning. Remote Sensing, 16(1), 149. https://doi.org/10.3390/rs16010149
10. Zhuang, L., Zhong, X., Xu, L., Tian, C., & Yu, W. (2024). Visual SLAM for Unmanned Aerial Vehicles: Localization and Perception. Sensors, 24(10), 2980. https://doi.org/10.3390/s24102980

AUTONOMOUS EXECUTION OF STRIKE UAV MISSIONS: FUNCTIONAL AUTONOMY PROFILES

Jordan Alexiev

Faculty of "Aviation", "Georgi Benkovski" Bulgarian Air Force Academy,
DolnaMitropolia, Bulgaria,alex.et@abv.bg

Abstract: *The paper proposes a mission-dependent method for defining autonomy requirements of strike UAVs. Mission type, operational environment, threats and platform constraints are translated into function-specific degrees of required autonomy. A functional autonomy profile is introduced as a vector description instead of a single overall autonomy level. The method distinguishes the required mission profile from the autonomy capability profile implemented by a particular UAV, enabling direct comparison between mission requirements and system capabilities.*

Keywords*: strike UAV, mission autonomy, autonomy profile, contested environment, deep strike, cooperative mission*

АВТОНОМНО ИЗПЪЛНЕНИЕ НА МИСИИ ОТ УДАРНИ БЛА: ФУНКЦИОНАЛНИ ПРОФИЛИ НА АВТОНОМНОСТ

Йордан Алексиев

Факултет „Авиационен" ,Висше военновъздушно училище „ГеоргиБенковски",
гр. Долна Митрополия, Република България, alex.et@abv.bg

Резюме: *Предложен е метод, зависим от характера на мисията за определяне на изискванията към автономността на ударните БЛА. Типът мисия, средата, заплахите и ограниченията на платформата се преобразуват в степени на необходима автономност за всеки функционален клас. Въвежда се функционален профил на автономност като векторно описание вместо единно ниво на автономност. Разграничават се профилът, изискван от мисията, и профилът на автономните способности на конкретния БЛА, което позволява непосредственото им съпоставяне.*

Ключови думи: *ударен БЛА, мисионна автономност, функционален профил, оспорвана среда, далекобойна мисия, кооперативна мисия*

Въведение

Автономността на безпилотните летателни апарати не е единна характеристика на системата. Един БЛА може да изпълнява самостоятелно навигационни задачи, но да остава зависим от външно целеуказване; друг може да притежава развито сензорно възприемане, но ограничени способности за мисионно препланиране. Европейската агенция по отбрана изрично развива подхода „автономност като функция", като свързва необходимата автономност с конкретните функции, типа мисия и условията на средата [1, 2]. Рамката ALFUS също разглежда

автономността чрез взаимодействието между сложност на мисията, сложност на средата и човешко участие [3].

За ударните БЛА този проблем се изостря от комуникационно и навигационно противодействие, динамично изменение на заплахите, ограничен ресурс и необходимост от действие на различна оперативна дълбочина. Програмата CODE на DARPA показва практическия смисъл на този преход: при ограничена комуникация и недостъпна GPS навигация безпилотни системи запазват мисионното намерение, споделят информация и адаптират действията си с ограничено външно управление [4, 5]. Следователно използването на едно общо „ниво на автономност“ е недостатъчно за описание на реалните изисквания към системата.

Научният проблем е определянето на необходимата автономност не като единна скаларна величина, а като съвкупност от функционални изисквания, зависещи от мисията и условията на нейното изпълнение. Целта на статията е да се предложи метод за формиране на функционален профил на необходимата автономност на ударен БЛА и за съпоставянето му с реално притежаваните автономни способности на системата. За постигането ѝ се класифицират основните мисии, систематизират се факторите на средата, въвежда се степен на необходима функционална автономност и се формират сравнителни профили за характерни мисии.

1. Основни класове мисии на ударните бла

За целите на функционалния анализ е по-полезно мисията да се класифицира според характера на задачата и условията на изпълнение, а не само според конструктивния тип на БЛА. Един и същ клас платформа може да изпълнява ударна, разузнавателно-осигуряваща, примамваща или комуникационна роля, като необходимият профил на автономност се изменя съществено. Основните класове мисии и техният функционален акцент са обобщени в табл. 1.

Таблица 1. Основни класове мисии и характерни изисквания

Клас мисия	Характеристика	Функционален акцент
Тактическа ударна	Предварително определена цел; относително кратък мисионен цикъл	Полет, навигация, насочване, базово управление на мисията
Търсене и въздействие	Целта не е точно локализирана; необходимо е откриване и проследяване	Сензорно възприемане, ситуационна оценка, мисионно планиране
Далекобойна ударна	Голяма далечина и продължителност; преминаване през различни зони на противодействие	Навигация, устойчивост, мисионно управление, ресурсна адаптация
Осигуряваща / примамваща	Подпомага общата ударна операция без задължително собствено поразяване	Навигация, мрежово взаимодействие, координация, зададена роля
Групова / кооперативна	Множество БЛА с разпределени или специализирани роли	Комуникация, кооперация, разпределяне на задачи, обща ситуационна картина

Далекобойните ударни мисии (deep strike) са показателни, защото съчетават голяма продължителност, изменение на комуникационната и навигационната среда и преминаване през различни зони на риск. Към 2026 г. украинската официална терминология използва Deep Strike за далекобойни безпилотни способности с обсег над 2000 km [6]. Наблюденията от войната в Украйна показват и използване на смесени ударни вълни с БЛА-примамки за натоварване и разкриване на системите за противовъздушна отбрана [7, 8]. Това показва, че приносът на отделния БЛА към мисията не се определя единствено от собствената му ударна функция.

2. Фактори, определящи необходимата автономност

Необходимата автономност се определя от съчетанието между характеристиките на мисията, средата и ограниченията на системата. За обобщено описание може да се използва зависимостта

$$A_{\text{необх}} = f(M, E, P, R)$$

където M характеризира мисията; E - средата на изпълнение; P - ограниченията на платформата и полезния товар; R - рисковете и ограниченията за изпълнение. Средата включва достъпността и достоверността на навигационните източници, качеството на комуникацията, радиоелектронното противодействие, зоните за откриване и противовъздушна отбрана, терена, метеорологичните условия и динамиката на обстановката.

Съществено е, че тези фактори могат да се изменят в рамките на една мисия. При далекобойна задача маршрутът може условно да се представи като последователност от зони Z1, Z2, …, Zn с различни характеристики. Следователно необходимата автономност е функция не само на мисията, но и на текущото състояние на средата: Анеобх = f[M, Z(t)]. Така функционалният профил може да се изменя по фази: например по-висока автономност на навигацията и устойчивостта при деградирана комуникация и по-висока сензорна автономност във фаза на търсене.

3. Функционален профил на необходимата автономност

За формиране на профила автономните способности на ударния БЛА се структурират в осем функционални класа: АФ-1 - полет и навигация; АФ-2 - сензорно възприемане; АФ-3 - информационно обединяване и ситуационна оценка; АФ-4 - планиране и управление на мисията; АФ-5 - устойчивост, самодиагностика и преконфигуриране; АФ-6 - комуникационни и мрежови функции; АФ-7 - кооперативни и колективни функции; АФ-8 - взаимодействие човек - автономна система. В настоящата статия тези класове се използват като координатни оси на мисионния профил.

За мисия Mj функционалният профил на автономност (ФПА) се определя като вектор

$$PA(Mj) = [L1j, L2j, L3j, L4j, L5j, L6j, L7j, L8j]$$

където Lij е необходимата степен на автономност на i-тия функционален клас при мисия j. Така вместо твърдението „БЛА е на ниво 4 автономност“ се получава многомерно описание, което показва за кои функции автономността е критична и за кои може да остане ограничена. При изменение на средата профилът може да бъде динамичен и да се изменя по отделните етапи на мисията. Логиката за формиране на профила е представена на фиг. 1.



Фигура 1: Логика за формиране на функционален профил на автономност

4. Степен на необходима функционална автономност

За сравняване на профилите е необходима компактна скала, която не представлява универсално „ниво на автономност“ на целия БЛА. Предлага се петстепенна оценка от 0 до 4, приложима поотделно към всеки функционален клас и показваща каква степен на самостоятелност изисква конкретната мисия. Предложената скала е представена в табл. 2.

Таблица 2. Степен на автономност на отделна функция

Степен	Характеристика
0	Автономно изпълнение не се изисква. Функцията може да се изпълнява чрез външно управление или да не е необходима за конкретната мисия.
1	Предварително зададено автоматизирано изпълнение. Функцията се изпълнява по зададени правила, параметри или последователности без самостоятелна адаптация.
2	Ограничена функционална автономност. Системата избира между предварително определени допустими действия в зададен диапазон от условия.
3	Адаптивна функционална автономност. Системата оценява собственото състояние и средата и адаптира изпълнението към очаквани изменения в зададени граници.
4	Висока функционална автономност в динамична среда. Системата оценява измененията, избира допустимо поведение и преконфигурира изпълнението при частична неопределеност в зададените ограничения.

Скалата описва необходимата самостоятелност на функцията, а не правомощието за конкретно критично действие. Последното е отделен аспект на взаимодействието човек - автономна система и може да бъде ограничено независимо от високата автономност на навигацията, възприемането или мисионното управление.

5. Илюстративни функционални профили

За демонстриране на подхода в табл. 3 са представени илюстративни профили за пет характерни мисии. Стойностите служат за сравнителен анализ и не представляват нормативни стойности или резултат от изпитване на конкретна система. При практическо приложение те трябва да се определят от конкретния сценарий, платформата, средата, ограниченията и критериите за приемлив риск.

Таблица 3а. Илюстративни профили - функционални класове АФ-1 - АФ-4

Мисия	**АФ-1**	**АФ-2**	**АФ-3**	**АФ-4**
Тактически удар	3	2	2	2
Търсене и въздействие	3	4	4	4
Далекобойна ударна	4	2	4	4
Осигуряваща / примамваща	3	1	2	3
Групова / кооперативна	3	3	4	4

Таблица 3б. Илюстративни профили - функционални класове АФ-5 - АФ-8

Мисия	**АФ-5**	**АФ-6**	**АФ-7**	**АФ-8**
Тактически удар	2	2	0	2
Търсене и въздействие	3	2	1	2
Далекобойна ударна	4	3	1	2
Осигуряваща / примамваща	3	2	3	1
Групова / кооперативна	4	4	4	2

Сравнението показва, че усложняването на мисията не води до равномерно нарастване на всички компоненти на профила. При търсене и въздействие доминират сензорното възприемане, ситуационната оценка и мисионното управление. При далекобойната мисия нарастват изискванията към навигацията, ситуационната оценка, устойчивостта и автономното управление на мисията, тъй като условията могат да се изменят по маршрута. При примамващата роля не е необходима висока автономност на разпознаването, но се увеличава значението на координацията в общата операция. При груповите мисии комуникационните и кооперативните функции стават равностойни на индивидуалните мисионни функции.

Този резултат подкрепя тезата, че една и съща базова платформа може да има различен функционален профил при различни роли. Обратно, една мисия може да бъде изпълнявана от хетерогенна група, в която отделните БЛА имат специализирани профили - ударен, разузнавателен, примамващ, комуникационен или кооперативен възел.

6. Формиране, актуализиране и съпоставяне на профилите

За практическо използване на функционалния профил се предлага последователност от пет стъпки. Първо, мисията се разлага на основни етапи или състояния. Второ, за всеки етап се определят характеристиките на средата и ограниченията - навигационни, комуникационни, сензорни, ресурсни и свързани със заплахите. Трето, за всеки от осемте функционални класа се оценява необходимостта от самостоятелно изпълнение. Четвърто, по скалата 0-4 се определя необходимата степен за всяка функция. Пето, полученият изискван профил се съпоставя с профила на автономните способности на конкретния БЛА.

Предлагат се два взаимно свързани профила. Изискваният профил P_req описва автономността, необходима за изпълнение на мисията в зададените условия, а профилът на способностите P_cap описва степента на автономност, която конкретната система реално може да осигури. За всеки критичен функционален клас условието за функционална пригодност е реализираната способност да не е по-ниска от изискваната. При многоетапна мисия изискваният профил може да се определя за всеки етап, а проектният профил на системата - по максималната необходима стойност на всеки компонент.

Разграничението между P_req и P_cap разделя две задачи, които често се смесват: определянето на мисионните изисквания и оценката на наличните способности. Платформата трябва да притежава функционалния запас, необходим за най-сложните етапи, но конкретната мисия не налага всички автономни способности да се използват постоянно на максимална степен. Полученото съпоставяне може да служи като вход към избора на платформа, модулна хардуерна и софтуерна конфигурация и последващото определяне на архитектурните и алгоритмичните изисквания.

7. Дискусия

Предложеният подход има три основни предимства. Първо, отделя въпроса „каква функция трябва да бъде автономна“ от въпроса „до каква степен трябва да бъде автономна“. Второ, обвързва необходимата автономност директно с мисионните и средовите изисквания. Трето, чрез разграничаването на изискван профил P_req и профил на способности P_cap позволява функционално съпоставяне между мисията и конкретната система. Подходът е съвместим с концепцията на EDA за „автономност като функция“ [1] и с многомерното разбиране на ALFUS [3], но е насочен към формиране на мисионно-зависими профили при ударни БЛА. NATO също поставя акцент върху споделено разбиране на автономните системи, управление на различни степени на автономност и интероперативност на системи от системи [9].

Функционалният профил не трябва да се разглежда като постоянна характеристика на платформата. В динамична среда изискванията към отделните компоненти могат да се изменят според фазата на мисията, качеството на навигацията и комуникацията, промените в заплахите и остатъчния ресурс. Практическата реализация следователно предполага модулна хардуерна и софтуерна архитектура, в която автономните способности се конфигурират според

конкретната задача. Така мисионният анализ се свързва непосредствено с последващото извеждане на архитектурни и алгоритмични изисквания.

Заключение

Предложен е подход, зависим от характера на мисията за определяне на автономността на ударни БЛА. Класифицирани са основни ударни, осигуряващи и групови мисии и са систематизирани факторите, които изменят необходимата функционална самостоятелност. Въведен е функционален профил на необходимата автономност като вектор от степени за отделните функционални класове и е предложена петстепенна скала за тяхното определяне.

Основният резултат е разграничаването между изискван от мисията профил P_req и профил на автономните способности P_cap на конкретния БЛА. Това позволява мисионните изисквания да бъдат съпоставени с реалните способности на системата и формира последователността: мисия и среда -> изискван функционален профил -> съпоставяне със способностите -> архитектурни изисквания -> алгоритмична реализация.

Литература

1. European Defence Agency. (n.d.). Taxonomy: Autonomy as a function. European Defence Agency. Accessed 27 August 2026.
2. European Defence Agency. (2024). EDA Action Plan on Autonomous Systems (APAS). European Defence Agency.
3. Huang, H.-M., Messina, E., & Albus, J. (2007). Autonomy Levels for Unmanned Systems (ALFUS) Framework, Volume II: Framework Models, Version 1.0 (NIST SP 1011-II-1.0). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1011-II-1.0
4. Defense Advanced Research Projects Agency. (2018). CODE Demonstrates Autonomy and Collaboration with Minimal Human Commands. DARPA.
5. Defense Advanced Research Projects Agency. (2019). In the Sky and on the Ground, Collaboration Vital to DARPA’s CODE for Success. DARPA.
6. National Security and Defense Council of Ukraine. (2026). Results of Ukraine’s Defense Industry in 2025: Deep Strike.
7. Bronk, J. (2026). Four Years On: An Update on the Air War Over Ukraine. Royal United Services Institute.
8. Welsch, M., Atalan, Y., Jensen, B., & Tiersten-Nyman, E. (2026). The Geography of Coercion: Russian Missile and Drone Campaigns in Ukraine. Center for Strategic and International Studies.
9. NATO. (2022). Summary of NATO’s Autonomy Implementation Plan. NATO.

TECHNOLOGICAL EVOLUTION OF THE MINE COUNTERMEASURES SHIP SUBSYSTEM: TRANSITION TO INTEGRATED UNMANNED MODULES AND SENSOR NETWORKS

Krasimir S. Angelov

Faculty of Navigation, Nikola Vaptsarov Naval Academy, Varna, Bulgaria, angelov@nvna.eu

***Abstract**: The paper examines the technological evolution of mine countermeasures (MCM) in response to modern naval mine threats. It highlights the critical application of airborne laser and photon-based LiDAR sensors for the rapid detection and classification of drifting mines. Furthermore, the research emphasizes the transition from traditional mine-hunting to a network-centric "Stand-off" concept. Within this architecture, a mother-ship operates safely outside the danger zone while coordinating a multi-domain MCM Toolbox comprising unmanned surface vehicles (USVs), unmanned aerial vehicles (UAVs), autonomous underwater vehicles (AUVs), and remotely operated vehicles (ROVs). The study also analyzes the structural and technological requirements for these platforms, focusing on the utilization of non-magnetic composite materials, acoustic damping, and active degaussing systems to minimize their physical signatures. The main conclusion asserts that achieving high operational efficiency requires the integration of these physically optimized platforms into a cohesive System of Systems (SoS).*

***Keywords**: mine countermeasures (MCM); Unmanned Surface Vehicle (USV); Unmanned Aerial Vehicle (UAV); MCM mother-ship; Remotely Operated Vehicle (ROV).*

ТЕХНОЛОГИЧНА ЕВОЛЮЦИЯ НА КОРАБНАТА ПРОТИВОМИННА ПОДСИСТЕМА: ПРЕХОД КЪМ ИНТЕГРИРАНИ БЕЗПИЛОТНИ МОДУЛИ И СЕНЗОРНИ МРЕЖИ

Красимир С. Ангелов

Въведение

Развитието на минното оръжие води до актуализиране на средствата за борба с него. Съществува ясно изразена корелация, при която почти едновременно с въвеждането на новост, използвана в съвременните морски мини, се търси адекватен начин за нейното неутрализиране. Независимо че в арсенала на страните, разполагащи с минно оръжие, голяма част от образците са от по-старо поколение, не е целесъобразно да се отхвърля вероятността противникът да разполага и със съвременни мини, при които традиционните способи и средства за противодействие са недостатъчно ефективни. В наши дни развитите в сферата на отбраната страни отделят значителен ресурс за търсене на адекватни възможности за минимализиране на риска от подриваване на морски мини. Съществуват различни направления за технологично усъвършенстване на текущото противоминно въоръжение, като най-реалистични в краткосрочен план са изследванията, свързани с лазерно и фотонно базирани сензори, автоматизирани

надводни и подводни апарати и иновации, свързани с изграждането на корпусите на самите плавателни средства за борба с минната заплаха.

1. Лазерно и фотонно базирани сензори за откриване на мини (LIDAR системи)

Въздушният LiDAR (Light Detection and Ranging) представлява една от най-трансформиращите технологии в съвременните отбранителни стратегии. Монтирана на самолети, вертолети или безпилотни летателни апарати, тази активна система за дистанционно наблюдение излъчва бързи лазерни импулси към водната или земната повърхност. Чрез прецизно измерване на времето, необходимо на светлината да се отрази обратно към сензора, въздушният LiDAR изгражда високодетайлни триизмерни модели на околната среда. За разлика от пасивните системи за изображения, които разчитат на околна светлина или видими дължини на вълните, LiDAR прониква през растителност, работи ефективно при условия на слаба светлина и осигурява несравнима точност на данните за височината и пространството. В сферата на отбраната, въздушният LiDAR се е развил от експериментален инструмент в незаменимо средство за разузнаване, наблюдение и оперативно планиране. Способността му да генерира триизмерна геопространствена информация в реално или почти реално време предоставя решително предимство в сложна обстановка. В наши дни разработките на оръжейните компании за откриване на морски мини използват значително по-сложни технологии, които имат своите предимства спрямо използваните досега класически технологии за борба с минната заплаха на море. При радиолокация вълните се отразяват от водната повърхност, докато LIDAR-системите, използвани в противоминните операции, заобикалят това ограничение чрез лазери, генериращи импулси в зеления спектър. Зелената светлина има свойството да прониква през водната повърхност и да достига определена дълбочина (Aviation and Defense Market Reports, 2024). При противоминната концепция с използване на лазер за откриване на мини съществуват следните етапи:

- излъчване на импулс: вертолет или безпилотен летателен апарат-носител на LIDAR-система в рамките на секунда излъчва милиони лазерни лъчи в зеления спектър към водната повърхност.
- проникване: част от светлината прониква в дълбочина, отразявайки се от потопени обекти или от самото дъно.
- регистрация и 3D анализ: сензорите улавят отразените лъчи. Специален софтуер анализира времето за връщане на лъча и интензитета му, изграждайки детайлно триизмерно изображение на обекта в реално време. По този начин мините се разпознават по тяхната специфична геометрична форма (Cowan, 2024).

Най-важната положителна характеристика на лазерните системи е скоростта на обследване на водната повърхност. Докато традиционният кораб-минен ловец използва хидроакустически станции с поискови скорости между 4 и 6 вз., въздушните платформи, въоръжени с LIDAR системи, могат да осигурят оперативност със скорост над 100 вз. Тяхната задача не е детайлна класификация на дънни обекти, а незабавно откриване и локализиране на повърхностни, плаващи

и дрейфащи котвени мини. Система за откриване на мини, базирана на авиационно средство,[45] прелита над района, опасен от мини, открива координатите на мините и предава данните към командния пункт, който управлява други средства за унищожаване на мините (напр. безпилотните надводни апарати).

Доказателство за това, че съществуват значителни предимства на лазерно и фотонно базирани сензори за откриване на мини, са продължаващите изследвания на различни технологични гиганти в областта на сигурността. Най-ясно изразени са:

- Висока скорост на тактическо разгръщане: вертолетите или безпилотните летателни апарати се движат многократно по-бързо от противоминните кораби, което позволява бързо установяване на мини в районите на операцията.
- Безопасност за личния състав: личният състав се намира извън района, опасен от мини.
- Ефективност в плитки води: хидроакустическите станции не са достатъчно ефективни в плитки води поради силното влияние на дънната реверберация, докато LIDAR системите не са възпрепятствани от тези условия.

Основен ограничаващ фактор, въздействащ върху ефективната работа на морски LIDAR системи, е мътността на водата. При силно вълнение, тиня или речни наноси светлината се разсейва бързо, което значително намалява дълбочината на откриване. Поради тази причина е необходимо в дълбоки води или при ниска видимост системата да се използва комбинирано с дълбоководни автономни хидроакустични дронове.

LIDAR следва да се разглежда като основен компонент от противоминното въоръжение. Особено ефективно ще бъде неговото използване в ограничени в навигационно отношение райони, особено при операции, ограничени във времето. В много случаи ще бъде необходимо комбинирано използване на системата с хидроакустически средства или други традиционни методи за борба с минната заплаха.

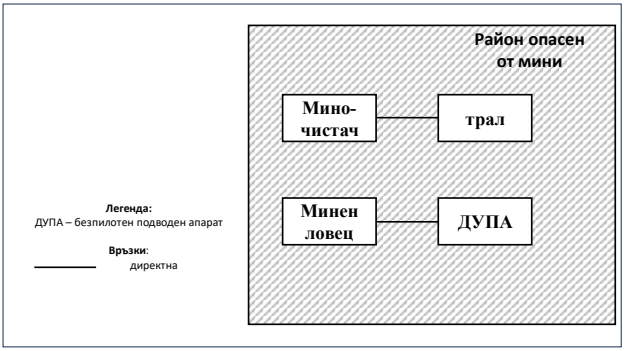
2. Мултифункционални МСМ-дронове

Съвременната концепция за противоминна война претърпява значителна трансформация. Традиционният консервативен подход, разчитащ на специализирани противоминни кораби (миночистачи и минни ловци), които навлизат директно в район, опасен от мини (MCM Stand-in) (фиг. 1), се заменя от концепцията за „извеждане на човека от опасната зона" (MCM Stand-off) (фиг. 2). Тази цел се постига чрез интегрирането на кораб-носител и група от безпилотни автономни системи, опериращи в три физически домейна: въздушен, надводен и подводен.

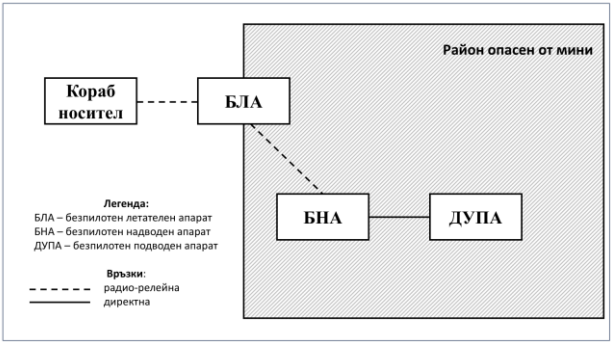
Взаимодействието между тези платформи създава гъвкава, многодомейна и мрежово-центрична архитектура, известна в терминологията на НАТО като противоминен контейнер (MCM Toolbox). Основни елементи на тази система са

[45] В англоезичните научни публикации се среща като ALMDS (Airborne Laser Mine Detection System).

безпилотни надводни апарати, безпилотни летателни апарати, дистанционно управлявани и автономни подводни апарати, които се намират на кораб-носител. Корабът-носител осигурява съхранението на противоминното оборудване, развръщането и обирането му, изпълнението на заложените функции в средата на действие и не на последно място извършването на определени поддържащи операции.



Фигура 1: Функционална схема на противоминна система при концепцията MCM Stand-in



Фигура 2: Функционална схема на противоминна система при концепцията MCM Stand-off

Безпилотни надводни апарати (Unmanned Surface Vehicles – USV)

Безпилотните надводни катери изпълняват ролята на централен тактически хъб и платформи-носители в зоната на противоминната операция. Те се управляват дистанционно от борда на отдалечен от района кораб-носител, който е разположен извън обсега на минната заплаха или от брегови център за управление. Безпилотните надводни катери служат като платформи за пренасяне, развръщане и

прибиране на подводни автономни апарати и дистанционно управлявани апарати. Освен това те често изпълняват и функция по буксиране на специализирани хидроакустични станции. Пример за такава интеграция се наблюдава при френско-британската програма MMCM (Maritime Mine Counter Measures), при която безпилотен катер буксира хидроакустическа станция с висока резолюция SAMDIS[46], което позволява откриване и класификация на дънни мини при висока скорост на движение без риск за екипажа.

Безпилотни летателни апарати (Unmanned Aerial Vehicles – UAV)

Въздушният сегмент от противоминната мрежа осигурява три критични предимства: висока скорост на обзор, автономно оптично/лазерно откриване и надежден ретранслационен канал за данни. Въздушните дронове с вертикално излитане и кацане се оборудват с олекотени оптико-електронни и лазерни сензори за бързо картографиране на плитките крайбрежни води и зоните на прибоя. Тяхната втора, не по-малко важна роля е функционирането им като въздушни комуникационни ретранслатори. Поради физическите ограничения при разпространението на радиовълните над водната повърхност, UAV поддържат непрекъсната високоскоростна тактическа връзка между надводните катери, подводните средства и отдалечения кораб-носител. При първоначалното установяване на противоминната концепция Stand-off съществуваше проблем именно с невъзможността от осигуряване на команден канал на значителна дистанция между кораба-носител и безпилотния надводен катер. С въвеждането в противоминната система на безпилотен летателен апарат този недостатък се преодолява. В бъдеще се очаква апаратите от този тип да осигуряват още по-голяма автономност, което ще осигури значителен времеви ресурс за провеждане на противоминната операция.

Пример за такава интеграция се наблюдава на хибридния сензорен контейнер SMAMD (Single-system Multi-mission Airborne Mine Detection) от BAE Systems върху безпилотния вертолет MQ-8C Fire Scout. Системата комбинира активен лазер и пасивна многоспектърна камера за автоматично засичане и класификация на мини от брега до 10 км навътре в морето.

Дистанционно управлявани и автономни подводни апарати (ROV и UUV/AUV)

Подводният сегмент е този, който извършва непосредствения контакт с минната заплаха на средни и големи дълбочини, където лазерните системи за обследване са неефективни. Установени са две основни подгрупи апарати:

Автономните подводни апарати (Autonomous Underwater Vehicles – AUV), например Remus или Hugin, се програмират предварително и се спускат от USV или от кораб-носител. Те се движат самостоятелно по предварително зададен

[46] Synthetic Aperture Mine Detection and Imaging System (SAMDIS) - специализирана хидроакустическа система от най-ново поколение, разработена от френската компания Thales за нуждите на противоминната война.

маршрут, извършвайки прецизно хидроакустическо сканиране на морското дъно. След качването им на борда (или по време на кратки изплавания чрез акустичен модем) събраните данни се анализират за наличие на миноподобни обекти.

Дистанционно управлявани апарати (Remotely Operated Vehicles – ROV): След като даден обект е класифициран като вероятна мина, на мястото се изпраща ROV. Той е физически свързан с катер (USV) или кораб чрез оптичен/захранващ кабел. Това позволява на оператора да вижда видеосигнал с висока разделителна способност в реално време и да управлява прецизно подводния апарат. ROV се използват за окончателна идентификация (чрез камери и високочестотни ХАС за близък обзор) и последваща неутрализация. Неутрализацията се извършва чрез поставяне на взривен заряд до мината (т.нар. Mine Disposal Systems) или чрез използване на дистанционно управлявани апарати тип „камикадзе" (напр. SeaFox C).

Ключът към високата ефективност на мултифункционалните дронове не е само в индивидуалните им възможности, а в тяхната системна интеграция, осигуряваща висок синергичен ефект. Типичен съвременен сценарий за противоминна дейност може да бъде представен по следния начин:

Фаза 1 (Разузнаване от въздуха): Въздушният дрон прелита над назначен район, извършвайки бързо лазерно сканиране за откриване на плаващи мини и мини, поставени на малко удълбочение.

Фаза 2 (Поиск с използване на хидроакустическа станция): Безпилотен надводен катер спуска подводен автономен апарат, който сканира дъното с хидроакустическа станция, откривайки дънни мини в районите с голяма дълбочина.

Фаза 3 (Идентификация и неутрализация): При откриване на миноподобен обект, USV изпраща дистанционно управляван апарат, който идентифицира визуално обекта и го унищожава.

По време на противоминната операция безпилотният летателен апарат се намира над района, осигурявайки връзка за предаване на хидроакустическата информация и видеопотоците към командния център в реално време.

3. Конструктивно-технологични изисквания към елементите на противоминните системи

Проектирането на съвременни кораби-носители и безпилотни апарати за противоминна борба изисква коренно различна инженерна философия в сравнение с традиционното корабостроене. Тъй като съвременните морски мини използват високочувствителни комбинирани взриватели (реагиращи едновременно на промени в магнитното, акустичното и хидродинамичното поле), платформите в застрашената зона трябва да притежават ниски нива на собствените си физически полета. От друга страна, поради променливата и тежката среда, в която тези корпуси трябва да функционират, съществуващите критични изисквания за якост и устойчивост продължават да са актуални.

Плавният преход, започнал в началото на седемдесетте години на миналия век за изработване на корпусите на противоминните кораби от корабостроителна

стомана към немагнитни материали, е фундаментален. Използването на стъклопласт позволява конструирането на монолитни корпуси без заваръчни шевове, които са немагнитни. Освен това, композитните материали имат изключително високо съотношение на якост към тегло и не корозират в агресивната морска среда. Съществува тенденция при изработване на съвременните корпуси да се използва методът на сандвич-панелите, т.е. два слоя от стъклопласт, между които е затворен лек полимерен слой (пенополиуретан). По този начин значително се намалява теглото на конструкцията, увеличава се плавучестта и се намалява акустичното излъчване на кораба или апарата.

За допълнително намаляване на акустичните полета на системите се прилага комплекс от пасивни и активни конструктивни решения:

Амортизационни платформи и еластично окачване: Всички вибриращи агрегати на борда се монтират върху специализирани виброизолатори, които абсорбират структурния шум и не позволяват на вибрациите да се предадат към корпуса и оттам във водната среда.

Водометни движители и малошумни винтове: При безпилотните апарати класическите винтове могат да бъдат заменени с водометни движители или винтове с оптимизирана геометрия на лопусите (високо дисково отношение), работещи при ниски обороти. Това предотвратява появата на кавитационни процеси, които са основен източник на акустичен шум във водата.

При по-големите платформи (като корабите-носители), където е невъзможно абсолютно всички вътрешни системи (генератори, оръжейни системи, кабелни трасета) да бъдат изработени от композитни материали, се прилагат активни технологии за потискане на магнитното поле:

Надводната платформа се оборудва с размагнитващи устройства, представляващи триизмерна мрежа от кабелни намотки, разположени по целия корпус. Тези намотки генерират контролирано магнитно поле, което е точно равно по сила и противоположно по посока на собственото магнитно поле на кораба. В резултат се получава взаимно унищожаване на полетата.

В обобщение, технологичните решения в архитектурата на корпуса и материалите (композити, стъклопласт, активни системи за размагнитване) трансформират физическата същност на противоминните платформи. Намаляването на акустичните и магнитните полета им позволява да навлизат сравнително безопасно в зони, опасни от мини. Въпреки това индивидуалната пасивна защита на корпуса е само предпоставка за устойчивост на външните влияния на противоминната платформа.

Заключение

Динамиката в развитието на съвременните оръжейни системи, използвани в морския домейн, предявява по-високи изисквания, свързани с безопасното използване на морските фарватери за военни и невоенни цели. Противоминните системи следва да бъдат адекватни на новите минни заплахи. На основата на проведеното изследване могат да се представят следните изводи:

- За достигане на по-висока ефективност на противоминните действия е необходимо новите физически оптимизирани платформи да бъдат софтуерно и командно интегрирани, което води до допълнителен анализ на техния мрежово-центричен капацитет като Система от системи (SoS);
- Изследванията, свързани с оптимизиране на противоминната система на страната, изискват итеративност на процесите, свързани с изследването на морската среда, поради продължаващото развитие на морските мини и нарастващия брой страни, имащи в своя арсенал такъв вид оръжие;
- За формирането на съгласувана национална позиция, свързана с противодействието на минната заплаха на море, е необходимо изучаването на чуждия опит на страни-партньори, притежаващи висок капацитет в сферата на минната и противоминната война.

Източници

1. Aviation and Defense Market Reports. (2024). Airborne LiDAR in defense: Revolutionizing modern military operations. https://aviationanddefensemarketreports.com/airborne-lidar-in-defense-revolutionizing-modern-military-operations/
2. Cowan, G. (2024, April). Mine countermeasures: Search and destroy. In *Maritime UAS Technology Report*. Shephard Media. https://businessinfo.shephardmedia.com/technology-reports/uas-april-2024/mine-countermeasures

CURRENT CAPABILITIES OF THE MINE COUNTERMEASURES FORCES OF THE BLACK SEA FLEET OF THE RUSSIAN FEDERATION IN THE CONTEXT OF MODERN NAVAL CHALLENGES

Krasimir S. Angelov

Faculty of Navigation, Nikola Vaptsarov Naval Academy, Varna, Bulgaria, angelov@nvna.eu

***Abstract**: This paper examines the current capabilities of the Russian Black Sea Fleet's Mine Countermeasures Vessels (MCMVs) in the post-2022 period, focusing on their fleet composition, onboard systems, and effectiveness in combat conditions. The analysis assesses the impact of Ukrainian asymmetric tactics, specifically the employment of Unmanned Surface Vehicles (USVs) and Unmanned Aerial Vehicles (UAVs), which have significantly altered the regional operational environment. Furthermore, the study investigates the integration of traditional minesweeping platforms with modern mine clearance technologies, as well as the consequent evolution of mine warfare tactics.*

***Keywords**: mine countermeasures vessels (MCMVs); Russo-Ukrainian War*

АКТУАЛНИ СПОСОБНОСТИ НА ПРОТИВОМИННИТЕ СИЛИ НА ЧЕРНОМОРСКИЯ ФЛОТ НА РУСКАТА ФЕДЕРАЦИЯ В КОНТЕКСТА НА СЪВРЕМЕННИТЕ ВОЕННОМОРСКИ ПРЕДИЗВИКАТЕЛСТВА

Красимир С. Ангелов

Въведение

Противоминната война е критичен компонент на военноморските операции, особено в полузатворени морски пространства като Черно море. След началото на войната в Украйна през 2022 г. динамиката на морските операции се промени драстично, въвеждайки нови заплахи като безпилотни надводни и подводни апарати, без да се пренебрегва използването на противокорабни крилати ракети. Тези фактори доведоха до значителни загуби за Черноморския флот (ЧФ) и принудиха преразглеждане на традиционните военноморски тактики и процедури. Този доклад цели да оцени състоянието и способностите на противоминните сили на ЧФ на фона на тези промени.

Анализът се основава на публично достъпни данни за състава на руския Черноморски флот, доклади на международни аналитични центрове и военноморски експерти, оценки за въздействието на украинските атаки върху руския флот и информация за модернизацията на руския военноморски флот, включително противоминните кораби. Като общонаучен подход в настоящото изследване е приложен системният анализ. Методи за емпирични изследвания са анализ на информационни източници и ретроспекция. Методи за теоретични изследвания са анализ, сравнение и синтез.

1. Състав и способности на противоминните кораби на Черноморския флот

Независимо от сравнително оптимистичните амбиции, които са декларирани в стратегическите документи за развитие на способностите на Русия в морския домейн, до началото на пълномощабната война на Русия срещу Украйна през 2022 г. противоминните сили на Черноморския флот включват разнообразни по възраст и в качествено отношение надводни платформи. Общият брой противоминни кораби е осем от четири различни проекта (Black Sea Fleet Information Resource, 2025):

- един морски миночистач от **проект 12660 (клас Gorya)**;
- три базови миночистача от **проект 12700 (клас Alexandrit Class)**;
- три морски миночистача от **проект 266М (клас Natya)**:;
- един морски миночистач от **проект 02668 (клас Natya Mod)**.

За адекватно разбиране на състоянието на морските противоминни сили на Черноморския флот количественото определяне не е удовлетворяващо условие, необходимо е осъществяването на качествено-функционален анализ, при който да се съпостави текущото въоръжение със съвременно противоминно оръжие, с което разполагат други водещи морски играчи.

Флагманският кораб на черноморските противоминни сили на Руската Федерация е миночистач **проект 12660**, който е въведен в експлоатация през 1988 г. (RussianShips.info, б. д.; and-kin2008.narod.ru, б. д.-а). Корпусът му е изработен от маломагнитна легирана стомана. Значителна част от въоръжението и техниката също са от маломагнитни сплави. Тези особености са проектирани, за да намалят магнитното поле на кораба и да осигурят защита срещу неконтактни мини.

Тралното въоръжение на кораба е типично и включва дълбоководен контактен трал, електромагнитен трал и акустичен трал. То се „подсилва" от морално остарелите ниско ефективни 4 шнурови заряди „ШЗ-200". В допълнение корабът притежава способност за постановка на 16 котвени мини. Независимо че са миночистачи, корабите пр. 12660 притежават способности, присъщи на минните ловци. Миночистачът е въоръжен със самоходен дистанционно управляем унищожител на мини СТИУ-2 „Кетмен" (Военное обозрение, б. д.). Не е налична информация относно ефективността на този вид оръжие, но може да се направи обосновано предположение, че тази система, а и концепцията за използването ѝ значително наподобява процедурите, които се изпълняват от минните ловци и техните безпилотни управляеми апарати. В допълнение миночистачът разполага с буксируем търсач-унищожител на мини ИУ „Палтус". Този апарат не се използва масово и е ограничен само при двата кораба от посочения проект. Тъй като класът не е продължен и остава само с два кораба, системата не получава широко разпространение и се описва като „неприета" или „експериментална" (Бандурин, 2025). Отрицателна характеристика за този вид противоминно оборудване е остарялата концепция, при която преди системата да премине през минното поле е необходимо надводната платформа вече да е преминала първа, което от гледна точка на безопасността за кораба и екипажа е неприемлива поради високия риск от подриваване на мината. Подводният комплекс за унищожаване на мини „Гюрза"

също може да бъде класифициран като средство за борба срещу подводната заплаха. И при него обаче липсва актуална информация за реалната му ефективност срещу минната заплаха. Траловете, използвани срещу контактни и неконтактни мини, са добре известни в средите на противоминната експертиза. Що се отнася до дълбоководния контактен трал „ГКТ-2", той е създаден в средата на 60-те години на миналия век и е с доказана ефективност (АО „Завод им. С.М. Кирова", б. д.; Gidropribor, б. д.-b). Концепцията за използването на тралове е остаряла и изоставена от повечето държави членки на НАТО за сметка на по-безопасното миноловене, при което противоминното оборудване навлиза в опасната зона преди самата надводна платформа. Миночистачът е оборудван и с 2 броя трално въоръжение за борба с неконтактни дънни мини – електромагнитен трал „ТЭМ-3М" и акустичен трал „АТ-3". Електромагнитният трал има възможност за използване в петлеви или електроден вариант. Акустичният трал „АТ-3" се използва при морски, базови и рейдови миночистачи, с него се неутрализират дънни мини с акустически взриватели (Свободная пресса, 2019). В наши дни използването на трално въоръжение за борба срещу неконтактни мини е дори по-неприемливо отколкото при контактните котвени мини, поради факта, че в този тип морски мини (дори при по-старите образци) се вграждат прибори за срочност и прибори за кратност (Rios, 2005, с. 16). Тези устройства правят неконтактното тралене твърде ненадеждно, съответно рискът от последващо подриваване на плавателен съд, преминаващ през този район, е значителен (Lluy, 1995, с. 18).

Двата морски миночистача **проект 266М** са въведени в експлоатация през 1973 г. и 1974 г. и са изработени от маломагнитна легирана стомана (and-kin2008.narod.ru, б. д.-b). Значителна част от въоръжението и техниката са направени от немагнитни или маломагнитни сплави, като по този начин се намалява вероятността от подриваването на корабите на неконтактни мини с магнитни неконтактни взриватели.

Корабите проект 266М притежават минозаградни способности, като имат възможност да носят на борда си до 10 морски мини. Тралното въоръжение е типично за кораб, конструиран в началото на 70-те години на миналия век: контактен трал, електромагнитен трал и акустичен трал. Дълбоководният контактен трал „БКТ" има голям трален захват (до 420 м), с който се осигурява висока производителност срещу котвени мини. Корабът е въоръжен с петлеви електромагнитен трал „ТЕМ-4" и акустичен трал „АТ-3". В допълнение, противоминните способности са усилени и с 4 комплекта шнурови заряди „ШЗ-200". Съвременната концепция за водене на противоминни действия не прилага използването на такъв тип въоръжение. Корабът не разполага с по-съвременни средства за борба срещу минната заплаха от типа на безпилотни подводни апарати, които да предхождат преминаването през опасни в минно отношение райони, което прави участието му в противоминни операции рисково, особено при наличието на съвременни образци неконтактни мини.

Морският миночистач **проект 02668** е въведен в експлоатация през 2008 г., той е единствен по рода си и е построен на основата на миночистач пр. 266МЭ

(barmacode, 2018). За разлика от предшествениците си, получава съвременни средства за търсене и унищожаване на морски мини, а така също автоматизирана система за управление на противоминните действия (Dogswar.ru, 2022). Корабът разполага с минни пътища, които дават възможност за осъществяването на минозаградна дейност в рамките на до шест дънни неконтактни мини (Gidropribor, б. д.-a). Тралното въоръжение на кораба е в традиционна конфигурация: дълбоководен контактен трал „ГКТ-2", петлеви електромагнитен трал „ТЭМ-3М" и акустичен трал „АТ-6". Акустическият трал е по-ново поколение и има по-голям спектър от възможности за модулирането на акустични импулси.

Най-голям интерес от въоръжението на кораба има към самоходния телеуправляем търсач-унищожител на мини СТИУ-3 „Маёвка" (Быстров и др., 2023, с. 61). Руските специалисти правят аналогия, като сравняват апарата със западни образци. Например размерите, теглото и скоростта на изделията са напълно съизмерими. С по-ниски показатели са дължината на кабел-буксира, който при другите образци варира между 1000 и 2000 м, докато при „СТИУ-3" е едва 850 м, което се отразява на способността за отстояние от кораба (mina, 2014).

За разлика от по-старите противоминни проекти, корабът е оборудван със съвременна подкилна хидроакустическа станция „Ливадия-МЭ", при по-старите руски кораби се използват две хидроакустически станции – за котвени мини и за дънни мини. ХАС „Ливадия-МЭ" е проектирана за търсене, откриване, автоматично класифициране и показване на котвени и дънни мини по курса на кораба. Станцията едновременно открива и класифицира котвени мини на дистанция до 800 м. и дънни мини на дистанция до 560 м. Системата осигурява и управлението на дистанционно управляемия апарат „СТИУ-3". Това надгражда способностите на кораба за действия при сложни в минно отношение условия, така се намалява рискът от подриваване на миночистача и до известна степен се компенсират ефектите от неблагоприятни хидроакустични условия (and-kin2008.narod.ru, б. д.-b). Друга важна стъпка при този проект кораби е въвеждането на информационна система за боен мениджмънт, която руските специалисти наричат „Автоматизирана система за управление на противоминните действия Диез-Э".

Трите базови миночистача **пр. 12700** са въведени най-скоро в състава на Черноморския флот на Руската Федерация. Това става поетапно в началото и края на 2019 г. и в средата на 2021 г. Корпусът на този проект кораби е изработен от монолитно фибростъкло, използвайки вакуумна инфузия. Използването на корпус от фибростъкло му придава повишена здравина в сравнение с традиционния стоманен корпус и се характеризира с по-дълъг експлоатационен живот. Този корпус осигурява подобрена живучест, ниско тегло и минимизиране на физическите полета – фактор от решаващо значение за противоминните кораби (Kchf.ru, б. д.).

Съществена конструктивна новост са две носови подрулващи устройства и две кърмови подрулващи устройства, които осигуряват много висока маневреност на кораба. Миночистачите пр. 12700 „Александрит" разполагат с вече коментираната „Автоматизирана система за управление на противоминните действия Диез-Э",

подкилна ХАС „Ливандия-М". За осъществяване на противоминна дейност на борда на кораба от проекта се намират безпилотни надводни плавателни съдове „Сканда" (модифицирана лодка с надуваеми бордове и твърдо дъно „БЛ-680") и съответните подводни апарати за откриване, идентифициране и неутрализиране на мини. В допълнение корабите имат и класическо трално въоръжение – дълбоководен контактен трал „ГКТ-2" и широколентов акустичен трал „ШАТ-У" (сравнително нов и актуален трал).

След направения обзор на наличните противоминни платформи на ЧФ на РФ и основното им противоминно въоръжение, може да се обобщи, че:

- миночистачът **клас „Александрит" (пр. 12700)** е модерен кораб, проектиран да използва високотехнологични ХАС и дистанционно управлявани апарати за откриване и унищожаване на мини. Към момента на въоръжение в Черноморския флот са три кораба от този клас;
- миночистачът **клас „Натя" (пр. 266М)** е по-старо поколение кораб, разчитащ на традиционни трални системи, адекватни при по-нискотехнологични мини. При необходимост за противодействие срещу съвременни дънни неконтактни мини, корабът ще бъде неефективен;
- миночистачът **клас „Горя" (пр. 12660**) се явява преходен от гледна точка на използваните технологии. Той е ефективен спрямо традиционните контактни мини. Въпреки че разполага с по-модерно противоминно оборудване, не може да се твърди, че е достатъчно адекватен на съвременната минна заплаха;
- миночистачът **клас „Натя Мод" (пр. 02668)** е кораб, проектиран да използва високотехнологични хидроакустически станции и дистанционно управляеми апарати за търсене и унищожаване на морски мини. Черноморският флот разполага с един кораб от този проект.

Ключово предизвикателство е съществуването в технологично отношение на половината от противоминните кораби на Черноморския флот. Те са по-уязвими на модерните мини и актуалните в наши дни асиметрични заплахи. Разнообразието на противоминни платформи с различно въоръжение и техника допълнително поставя на изпитание подготовката на личния състав и вероятността за взаимозаменяемост между екипажите на корабите. В допълнение на това, способностите за отразяване на атаки от въздуха (противокорабни крилати ракети, пилотирани и безпилотни летателни апарати) не удовлетворяват (Bozov, 2023, с. 246-247). За минимализиране на този дефицит е необходимо осигуряването на защита от бойни кораби (фрегати и корвети) и/или въздушно прикритие на морско направление.

2. Влияние на военните действия върху противоминните сили

Конфликтът с Украйна значително промени оперативната среда за военните кораби от Черноморския флот, в частност и тази на противоминните кораби. Първоначалните стратегически планове на Русия, целящи завоюването на морско превъзходство с последващо осъществяване на морска десантна операция, не бяха постигнати (Popa & Learschi, 2025, с. 10). Противоминните сили на Русия следваше да осигурят сигурност на основния боен потенциал и десантните отряди

в противоминно отношение. Украинските безпилотни надводни апарати се оказаха ефективно и евтино средство за атака срещу руски военни кораби, включително маломерни цели (кораби за бойна поддръжка и катери). В допълнение използването на традиционните противокорабни крилати ракети допълнително изложи на риск тактическите плавателни единици на Черноморския флот.

Независимо от дезинформацията от руска и украинска страна, може да се направи обосновано предположение, че Черноморският флот търпи сериозни загуби. Западни анализатори твърдят, че тези загуби достигат 20% до 2023 г. (Cook, E., 2023). Сведенията за осъществени успешни атаки от страна на украинските въоръжени сили срещу противоминни кораби на ЧФ са противоречиви и непотвърдени. Може да се твърди за организирането на една успешна атака от украинска страна с надводни и въздушни безпилотни апарати срещу морския миночистач „Иван Голубец“, базиран във вмб Севастопол на 22.10.2022 г., с последващ шестмесечен ремонт и възстановяването на боеспособността му (Barkhush, 2024; Bickerton, 2022). Непотвърдено от руска страна или независим източник съобщение за друг морски миночистач от пр. 266М – „Ковровец“ и неговото унищожение с използването на тактическа балистична ракета ATACMS на 19.05.2024 г. (Higham, 2024; Povilas, 2024). Множеството успешни атаки срещу военни кораби от Черноморския флот на Русия принуждава руското ръководство да премести значителна част от плавателния си състав от вмб Севастопол във вмб Новоросийск, с цел намаляването на риска от допълнителни загуби.

3. Оценка на актуалните противоминни способности

Оценката на актуалните способности на противоминните сили на ЧФ е комплексна. От една страна, Русия разполага с четири модерни кораба, три от клас „Александрит“ и един кораб от пр. 02668, които предоставят значителни възможности за противодействие на минната заплаха, както срещу класически котвени контактни мини, така и срещу неконтактни дънни мини. Тези платформи значително намаляват степента на риска за кораба, екипажа и материалната част. Въпреки всичко, ако се сравнят с най-актуалните платформи за противоминни действия, например концепцията, която прилагат ВМС на Нидерландия и Белгия “rMCM Program” (Exail, 2025), трябва да се отбележи, че руската платформа започва да остарява в момента на въвеждането ѝ в строя. На съвсем друго технологично ниво е останалата част от противоминните сили на Черноморския флот, които използват по-старата концепция на противоминни действия посредством тралове за контактно и неконтактно тралене, която е много по-уязвима и застрашаваща безопасното използване на корабите и техните екипажи. Освен това, не трябва да се пренебрегва и фактът за намаленото оперативно пространство. Поради заплахата от украински атаки, руските военни кораби действат в по-ограничени зони, което би затруднило осигуряването на различните видове прикрития на противоминните кораби при осъществяването на техните функции на море. В много висока степен следва да се разглеждат и асиметричните предизвикателства, използвани от украинските въоръжени сили. Иновациите при

воденето на морската война с използването на безпилотни надводни и безпилотни летящи апарати създават сериозни предизвикателства, за които традиционните противоминни кораби не са проектирани да действат (Bozov, 2022, с. 116).

Заключение

Актуалните способности на противоминните кораби на руския Черноморски флот са противоречиви. Към момента тече процес на модернизация, при която остарелите кораби се заменят със сравнително актуални платформи, оборудвани с по-модерни средства за противоминна война. Времевите параметри на тази трансформация са неустойчиви поради променливата среда за сигурност. Докато това се случва, значителна част от флота, в това число и противоминните сили, е изправена пред технологично остаряване. Войната в Украйна разкри сериозни уязвимости на руските сили спрямо асиметрични заплахи, което ограничи способностите им за действие. В резултат на това ефективността на противоминните операции на Черноморския флот е поставена под сериозен въпрос, като силите са изправени пред необходимостта от адаптиране към нова, нетрадиционна оперативна среда.

Източници

1. Бандурин, Е. Н. (2018). *Моя военно-морская жизнь*. Самиздат. https://samlib.ru/b/bandurin_e_n/kniga3.shtml
2. Быстров, Б., Маруев, В., Плясов, А., и Черкасов, С. (2023). Противоминное оружие России: Генезис и эволюция (к 125-летию противоминного оружия России). *Морской Сборник*, (6), 54–62.
3. АО „Завод им. С.М. Кирова". (б. д.). *Глубоководный контактный трал ГКТ-2*. https://qai.ke.kz/ru/company/production/1059/
4. Военное обозрение. (б. д.). *Последние противоминные корабли морской зоны Советского Союза*. https://topwar.ru/38189-poslednie-protivominnye-korabli-morskoy-zony-sovetskogo-soyuza.html
5. Свободная пресса. (2019). *Атомные подлодки ВМФ РФ остаются без прикрытия*. Rambler News. https://news.rambler.ru/troops/42117848-atomnye-podlodki-vmf-rf-ostayutsya-bez-prikrytiya/
6. barmacode. (2018, 8 сентября). *Морской тральщик „Вице-адмирал Жуков"*. LiveJournal. https://barmacode.livejournal.com/163794.html
7. Barkhush, A. (2024, July 29). *Black Sea Fleet vessels Russia has lost since the beginning of the full-scale invasion*. United24 Media. https://united24media.com/latest-news/all-the-black-sea-fleet-vessels-russia-has-lost-since-the-beginning-of-the-full-scale-invasion-1445
8. Bickerton, J. (2022, October 29). *Russia says minesweeper hit in 'massive' attack on Black Sea Fleet*. Newsweek. https://www.newsweek.com/explosions-reported-near-crimean-city-russia-drones-shot-down-sevastopol-1755579
9. Black Sea Fleet Information Resource. (2025). *Black Sea Fleet 2025 all surface combatants and submarines*. https://www.kchf.ru/eng/ship/today.htm

10. Bozov, I. Z. (2022). Comparative analysis of the remotely piloted aircraft systems used in the Russia-Ukraine war. In *International Scientific Conference - Defense Technologies DefTech 2022* (pp. 113–117). Faculty of Artillery, Air Defense and Communication and Information Systems.
11. Bozov, I. Z. (2023). Unmanned combat aerial vehicle (UCAV) – weapon of the future. In *International Scientific Conference - Defense Technologies DefTech 2023* (pp. 243–247). Faculty of Artillery, Air Defense and Communication and Information Systems.
12. Cook, E. (2023, December 26). *Fifth of Russia's Black Sea Fleet 'destroyed' in 4 months: UK*. Newsweek. https://www.newsweek.com/russia-black-sea-fleet-crimea-ukraine-landing-ship-1855450
13. Dogswar.ru. (2022, 26 января). *Морские тральщики проекта 266М „Аквамарин"*. http://www.dogswar.ru/voennyi-flot/korabli/8834-morskie-tralshiki-pr.html
14. Exail. (2025, November 4). *First mooring of the Oostende in Zeebrugge, the first mine countermeasures vessel in the Belgian-Dutch rMCM programme*. https://www.exail.com/news/first-mooring-of-the-oostende-in-zeebrugge-the-first-mine-countermeasures-vessel-in-the-belgian-dutch-rmcm-programme
15. Gidropribor. (б. д.-a). *Морскаядонная мина МДМ-2*. http://gidropribor.chat.ru/html/rnuw_r/1/2/minestth1.html
16. Gidropribor. (б. д.-b). *Противоминное оружие*. http://gidropribor.chat.ru/html/rnuw_r/1/aw.html
17. Higham, A. (2024, May 19). *Ukraine destroys Russian Black Sea 'Kovrovets' minesweeper*. Newsweek. https://www.newsweek.com/ukraine-destroys-black-sea-kovrovets-minesweeper-1902259
18. Kchf.ru. (б. д.). *Морской тральщик „Иван Антонов"*. https://www.kchf.ru/ship/tral/ivan_antonov.htm
19. Lluy, P. A. (1995). *Mine warfare: An old threat presents new challenges* (Master's thesis). Naval Postgraduate School. http://hdl.handle.net/10945/31337
20. mina. (2014, 6 июня). Коментар към „Сила России". *Otvaga2004*. https://otvaga2004.mybb.ru/viewtopic.php?id=161&p=8
21. Popa, A., & Learschi, S. (2025). *The strategic collapse of the Russian Navy in the context of the war in Ukraine (2022–2025)*. Maritime Security Forum.
22. Povilas, M. (2024, May 28). *Another win for ATACMS: Ukraine destroyed a large Russian marine minesweeper*. Technology.org. https://www.technology.org/2024/05/28/another-win-for-atacms-ukraine-destroyed-a-large-russian-marine-minesweeper/
23. Rios, J. J. (2005). *Naval mines in the 21st century: Can NATO navies meet the challenge?* (Master's thesis). Naval Postgraduate School. https://hdl.handle.net/10945/1860
24. RussianShips.info. (б. д.). *Морские тральщики проекта 12660*. https://russianships.info/boevye/12660.htm

25. and-kin2008.narod.ru. (б. д.-a). *Морской тральщик проекта 12660*. https://and-kin2008.narod.ru/pr12660.html
26. and-kin2008.narod.ru. (б. д.-b). *Морской тральщик проекта 266*. https://and-kin2008.narod.ru/pr266.html

QUANTITATIVE AND QUALITATIVE ANALYSIS IN CHOOSING OPTIONS FOR DEVELOPING NAVAL MINE COUNTERMEASURES CAPACITY

Krasimir S. Angelov

Faculty of Navigation, Nikola Vaptsarov Naval Academy, Varna, Bulgaria, angelov@nvna.eu

***Abstract**: Evolving naval mine threats in the Black Sea require modernizing Mine Countermeasures (MCM) capabilities. This paper evaluates two Stand-off acquisition strategies: specialized MCM motherships versus converted commercial platforms carrying modular containerized systems. Using a Multi-Criteria Decision Making approach based on the Weighted Sum Model, both options are assessed across four criteria: Deployment Time, Cost and Life Cycle, Operational Effectiveness, and Flexibility. The quantitative evaluation demonstrates that converting commercial platforms is currently the more viable and acceptable option for rapidly mitigating urgent operational capability gaps. Purpose-built MCM vessels remain better suited for long-term strategic force structure planning. This study provides a practical decision framework for naval force planning in dynamic security environments.*

***Keywords**: mine countermeasures (MCM); Multi-Criteria Decision Making (MCDM); Weighted Sum Model (WSM); stand-off MCM operations.*

КОЛИЧЕСТВЕНО-КАЧЕСТВЕН АНАЛИЗ В ИЗБОРА НА ВАРИАНТ ЗА РАЗВИТИЕ НА ПРОТИВОМИНЕН КАПАЦИТЕТ НА ВОЕННОМОРСКИТЕ СИЛИ

Красимир С. Ангелов

Въведение

Анализът на оперативната среда в Черноморския регион чертае динамична обстановка с възможни множество въздействащи фактори, които с различен интензитет влияят върху системата за сигурност. Текущото състояние на противоминните способности на Военноморските сили на страната представлява баланс между способността на страната да поддържа и актуализира системния отбранителен потенциал и устойчивостта на икономическите предизвикателства. Процесът по придобиване на допълнителни минни ловци от клас „Трипарти" затвърждава отчасти способността на страната да е устойчива на съвременните минни заплахи. Въз основа на емпирично установената тенденция сред водещите военноморски сили обаче това не бива да се приема като достатъчно, особено в дългосрочен план. Рискът от използването на нови образци неконтактни мини и критичността на обществото при повишаване на нивото на риск от загуба на човешки и материален ресурс изискват осъществяването на допълнителни и итеративни действия за трайно нарастване на устойчивостта на системата за отбрана в нейния поделемент, поддържащ противоминния баланс на въоръжените сили в морския домейн.

Установено е, че в изграждането на новата противоминна Stand-off концепция водещите страни предлагат два подхода, които не са взаимно изключващи се, а по-скоро са допълващи се в зависимост от критериите за успех, които са посочени пред анализиращите експерти в противоминната област. Първият подход изисква изграждането на система от системи, включваща като системи специално конструиран кораб-носител и автономни надводни, подводни и въздушни апарати. Този подход се наблюдава при реализирането на белгийско-нидерландската противоминна програма - rMCM. Вторият подход при изграждането на противоминна система от системи извежда необходимостта от използването на неспециализиран надводен плавателен съд, който има способността да помества на борда си необходимия брой стандартни контейнери с противоминно оборудване, в това число: оперативна централа, автономни подводни, надводни и въздушни апарати. Във висока степен този подход е установен при реализирането на противоминните програми на Великобритания и Съединените щати.

1 Изложение

За установяване на реална посока за развитие на надводния противоминен капацитет на Военноморските сили на страната е целесъобразно използването на сравнителен анализ между двата възможни подхода. Използването на водещи критерии, по които да се сравнят двете възможности, ще благоприятства организирането на анализа. За целта, конкретно съпоставените тактико-технически параметри (като интеграция на товаро-разтоварни устройства, физически полета и срок за въвеждане в експлоатация) са групирани в четири стратегически критерия: Време за внедряване, Разходи и жизнен цикъл, Оперативна ефективност и Гъвкавост/Адаптивност, чийто синтез определя крайната Приложимост в Черноморския регион.

1.1 Вариант 1 - Специално построен кораб-носител

При първия вариант с използване на специализиран кораб-носител, могат да бъдат представени следните **положителни характеристики**:

- Оптимизирана архитектура за използване на безпилотни системи от различен клас: корабът е проектиран с възможност за оптимално използване на системи за спускане и обиране от борда (кърмови слипове или бордови люкове, кран-балки за безопасно спускане/обиране на безпилотни надводни и подводни апарати[47] при вълнение на морето 4 - 5 бала). Конструктивно е осигурена площадка за излитане и кацане на безпилотни летателни апарати[48], като това е съобразено с оборудването и надстройката на кораба в непосредствена близост до мястото за кацане и безопасното маневриране към зададена точка във въздушното пространство.

[47] Възможните габарити на безпилотен надводен апарат за целите на противоминната концепция са: дължина около 12 м, височина около 4 м, ширина около 4 м, тегло 18 т.

[48] Възможните габарити на безпилотен летателен апарат за целите на противоминната концепция са: дължина около 4 м, височина около 1,30 м, ширина 1,20 м, максимално излетно тегло около 250 кг.

- Контрол над физическите полета: независимо че според противоминната концепция не се планира преминаването на кораба-носител през район, опасен от мини, контролът на неговите физически полета е от първостепенна важност съгласно нормативните изисквания във Военноморските сили. Това включва изпълнението на мерки, свързани с намаляване на риска от детониране на неконтактните взриватели на дънните мини. За тази цел се осъществява контрол за състоянието на магнитното поле на кораба. Използват се щатни размагнитващи устройства, а при необходимост се извършват действия, свързани с фактическото редуциране на това поле. Минимализирането на акустичното поле на кораба също е обект на конструктивни решения по време на строителните дейности, които не са обект на разглеждане при невоенните кораби.

- Интегрирана система за боен мениджмънт: На кораба е обособен специално конструиран боен информационен център[49] за противоминния разчет на дронове, сертифициран съгласно стандартизационните документи на НАТО с висока степен на защита от противникови средства за радиоелектронна война и кибератаки.

- Дълъг жизнен цикъл: Обикновено при планирането на военни кораби се търсят инженерно-конструкторски решения за дълъг жизнен цикъл на въоръжението и техниката, и самия корпус на кораба. Прогнозираният ресурс на специализиран противоминен кораб-носител е от порядъка на над 30 години.

Независимо от предложените положителни характеристики, при варианта с използване на специализиран противоминен кораб-носител, не трябва да се пренебрегват и някои **недостатъци** в проекта:

- Висока цена: Строителството на чисто нов военен кораб от такъв клас изисква значителен финансов ресурс. Актуален пример е белгийско-нидерландската противоминна програма rMCM, при която за въвеждането в строя на дванадесет кораба-носителя и въоръжението към тях е предвидено финансово осигуряване, превишаващо сумата от 2 млрд. евро, т.е. около 160 – 200 млн. евро за един кораб.

- Дълъг срок за реализация: Оптимистичният вариант за реализиране на противоминен проект от концепцията до влизането в строя на корабите следва да се разглежда в рамките от 7 до 10 години, като в този срок не са включени явления, свързани с форсмажорни условия или финансова неустойчивост в бюджетните постъпления на ведомството, които допълнително могат да забавят реализацията на проекта. Главен фактор при срока за реализация остава количеството планирани за придобиване надводни платформи и дали те са били реализирани във времето или се осъществява съвсем нов проект.

- Технологичен риск: Дългият срок на реализация крие риск от морално остаряване на системата за боен мениджмънт, планирана да бъде вложена като интегриращ фактор в противоминната система от системи. Като това може да се осъществи още по време на строежа на кораба или при усвояването от екипажа и привеждането му в оперативна готовност.

[49] Съгласно „Корабен устав на Военноморските сили на Република България" от 2008 г.

1.2 Вариант 2 - Преоборудван надводен плавателен съд

Както при първия вариант, така и при втория вариант с използване на Преоборудван надводен плавателен съд, съществуват предимства и недостатъци. Като положителни характеристики могат да бъдат посочени:

- Бързина при придобиване: при адекватно планиране на ремонтните и конструктивните дейности, периодът от закупуването, трансформирането и въвеждането в оперативен режим на вече изграден и влязъл в експлоатация невоенен кораб би отнело едва 12 - 24 месеца. Например, Кралските военноморски сили на Великобритания се вместват във времевата рамка от 18 месеца с противоминната платформа HMS Stirling Castle. До голяма степен това време ще зависи от проекта на кораба и възможността за адаптиране на неговите системи към очакваните за изпълнение функции на конкретния проект противоминен кораб-носител.

- Значително по-ниска цена: Очаквано първоначалните разходи за придобиване и преоборудване на кораба са неколкократно по-ниски от проектирането и строежа на нов кораб-носител за нуждите на отбранителната система на страната в морския домейн. Като пример може да се посочи, че Кралските военноморски сили придобиват HMS Stirling Castle (бивш търговски офшорен плавателен съд MV Island Crown) за около 46 млн. евро. С преоборудването цената достига сумата от около 52 млн. евро. По този начин реализираният проект на Великобритания е около 4 пъти по-изгоден икономически спрямо реализиращия се проект на Белгия и Нидерландия.

- Голям полезен обем и товароподемност: Невоенните кораби за поддръжка на офшорни платформи (какъвто е Stirling Castle) разполагат с огромни палубни пространства, корабни подемни средства с компенсация на вълнението и системи за динамично позициониране.

- Модулност: Такава надводна платформа позволява качването на стандартни ISO контейнери с поместени в тях безпилотни апарати от различни класове и системи за боен мениджмънт. Корабът лесно може да промени своето предназначение посредством смяна на контейнерите, в които са поместени противоминното въоръжение и оборудване.

При този вариант съществуват и няколко **недостатъка**:

- Компромиси с физическите полета: Корпусите на невоенните кораби са изработени от стандартна стомана, освен това енергосиловата система, както и винто-рулевата група осигуряват много по-високо ниво на акустично и магнитно поле, тъй като към тях не се предявяват изисквания, които са стандартни при конструирането на военни кораби от всички класове. Това значително повишава риска от детонирането на неконтактни мини при преминаване на кораба през минно поле.

- Слабо отбранително въоръжение: Независимо че военните кораби, използвани за противодействие на минната заплаха имат сравнително слабо въоръжение срещу въздушен противник, при невоенните кораби то отсъства

напълно. Възможностите за интегриране на ракетни и артилерийски системи за борба срещу въздушен и надводен противник към невоенни платформи конструктивно, както и хардуерно и софтуерно са крайно ограничени и нецелесъобразни.

- **Ограничен остатъчен жизнен цикъл:** Използването на вече употребяван невоенен надводен плавателен съд ограничава периода на експлоатация, като обикновено той е около 10 - 15 години, което представлява около три пъти по-кратък период в сравнение с новопостроен противоминен кораб-носител.

В обобщен вид резултатите от сравнителния анализ са представени в табл. 1. Данните посочени в таблицата показват висока степен на комплицираност, при която няма възможност за еднозначност на избора и съответно препоръка за реализиране на един от двата варианта. При синтез на данните към приложимостта им в акваторията на Черно море, вариантът с използване на вече конструирана невоенна надводна платформа с интегрирането и адаптирането на модулни контейнерни – противоминни инструменти е най-вероятен при осигуряване на попълването на опе ративни дефицити в ограничение на времето. Вторият вариант с придобиване на нов специализиран противоминен кораб-носител и приложимостта на тази противоминна система от системи е най-благоприятен вариант за дългосрочно из-граждане на отбранителен капацитет.

Таблица 1. Сравнителна таблица за специализиран противоминен кораб и преоборудвана невоенна платформа

Стратегически критерий	**Аналитичен подкритерий (Показател)**	**Специализиран противоминен кораб-носител**	**Преоборудвана невоенна платформа**
1. Време за внедряване	**1.1 Срок за въвеждане**	Дълъг: 7 - 10 г.	Кратък: 1 - 2 г.
2. Разходи и жизнен цикъл	**2.1 Първоначална цена**	Висока цена	Ниска/умерена цена;
	2.2 Времеви ресурс	Над 30 г.	10 - 15 г.
3. Оперативна ефективност	**3.1 Интеграция на подемни системи и безпилотни апарати**	Заложена фабрично (4 - 5 бала)	Частично адаптирана / контейнеризирана
	3.2 Физически полета и защита	Военен стандарт (ниски полета)	Граждански стандарт (високи полета)
	3.3 Отбранителна способност	Слабо артилерийско и/или ракетно въоръжение	Трудно интегриране на оръжейни системи
4. Гъвкавост и	**4.1 Модулност**	Специализирана	Висока

Стратегически критерий	**Аналитичен подкритерий (Показател)**	**Специализиран противоминен кораб-носител**	**Преоборудвана невоенна платформа**
адаптивност		интеграция	(стандартизирани ISO контейнери)
СИНТЕЗ	**Приложимост в Черно море**	За дългосрочно из-граждане на капацитет	За спешно попълване на оперативни дефицити

1.3 Количествен анализ на възможностите с използване на Модела на претеглените суми

За количествено оценяване на двата възможни варианта за придобиване на нови противоминни способности е приложим Моделът на претеглените суми (Triantaphyllou, 2000, с. 6-7) в рамките на теорията за Многокритериалното вземане на решения. За да се спази условието за скаларна еднородност, оценките по отделните критерии са приведени към уеднаквена 5-степенна скала, а относителната им тежест е дефинирана от оперативните приоритети на противоминните сили на страната в акваторията на Черно море. Съществуват три стъпки на всяка техника за вземане на решение, включваща числен анализ на възможностите (алтернативите) (Triantaphyllou, 2000, с. 5-6):

- определяне на съответните критерии и алтернативи;
- прикрепяне на числени мерки към относителната важност на критериите и към въздействието на алтернативите върху тези критерии;
- обработване на числовите стойности, за да се определи класирането на алтернативите.

Моделът на претеглените суми е вероятно най-използваният подход, особено при едноизмерни проблеми. Ако имаме m алтернативи и n критерии, то най-добрата алтернатива е тази, която удовлетворява (в случая на максимизация) следното условие:

$$A^*_{WSM\text{-}score} = max \sum_{j=1}^{n} a_{ij} w_j \text{ , за i } = 1, 2, 3, \ldots, \text{ m.} \quad (1)$$

където: $A^*_{WSM\text{-}score}$ е оценката на най-добрата алтернатива,

n е броят на критериите за вземане на решение,

a_{ij} е реалната стойност на i-тата алтернатива по отношение на j-тия критерий,

w_j е теглото на важност на j-тия критерий.

В текущия казус за многокритериално вземане на решения са установени:

- четири критерия (Време за внедряване; Разходи и жизнен цикъл; Оперативна ефективност; Гъвкавост и адаптивност);
- две алтернативи (Специализиран противоминен кораб-носител; Преоборудвана невоенна платформа).

Относителните тегла на четирите критерия са определени както следва: w_1 = 0,35, w_2 = 0,30, w_3 = 0,20 и w_4 = 0,15. Стойностите на изпълнение (оценките) от 1 (най-ниска) до 5 (най-висока) на двете алтернативи спрямо четирите критерия за вземане на решение са следните:

$$A = \begin{bmatrix} 1 & 2 & 5 & 3 \\ 5 & 4 & 2 & 5 \end{bmatrix}$$

Следователно данните за този проблем за многокритериално вземане на решения са обобщени в следната матрица за вземане на решения:

Алтернативи	**Критерии**			
	C_1	C_2	C_3	C_4
	0,35	0,30	0,20	0,15
A_1	1	2	5	3
A_2	5	4	2	5

Когато формула (1) се приложи спрямо горните данни, получените оценки за двете алтернативи са:

$A_{1 \cdot WSM\text{-}score}$ = 1 . 0,35 + 2 . 0,30 + 5 . 0,20 + 3 . 0,15 = 0,35 + 0,60 + 1,00 + 0,45 = 2,40,

$A_{2 \cdot WSM\text{-}score}$ = 5 . 0,35 + 4 . 0,30 + 2 . 0,20 + 5 . 0,15 = 1,75 + 1,20 + 0,40 + 0,75 = 4,10.

Следователно най-добрата алтернатива (в случай на максимизация) е алтернативата - Преоборудвана невоенна платформа A_2, тъй като тя притежава по-високата оценка: 4,10, спрямо първата алтернатива Специализиран противоминен кораб-носител.

Заключение

Количественият анализ ясно показва, че при настоящата оперативна среда преоборудваните плавателни съдове са препоръчителни, благодарение на критичните си предимства по отношение на времето за придобиване (w_1 = 0,35) и разходите за придобиване (w_2 = 0,30). Разбира се, при промяна на оперативната среда резултатите от изследването ще покажат различни стойности, което би могло да промени общата оценка в полза на придобиването на нови специализирани противоминни кораби.

Литература

1. Triantaphyllou, E. (2000). Multi-criteria decision making methods: A comparative study (Vol. 44). Springer. https://doi.org/10.1007/978-1-4757-3157-6

CIVIL-MILITARY COOPERATION IN NON-MILITARY CRISIS

Anton I. Manchev

Bulgarian Defence Institute "Professor Tsvetan Lazarov", Sofia, Bulgaria
e-mail: a_i_manchev@abv.bg

***Abstract**:Civil-military cooperation very often plays a key role in resolving any non-military crisis. Interaction between the military and civilians should be based on clear and precise rules for the rights and responsibilities of each party. The legal framework in our country shows that civil-military cooperation still does not get the attention it deserves. The existing legal framework is mainly found in the departmental publications of the Ministry of Defense.*

***Keywords:** Civil-military cooperation, crises, non-military crises, disasters.*

ГРАЖДАНСКО-ВОЕННО СЪТРУДНИЧЕСТВО ПРИ КРИЗИ ОТ НЕВОЕНЕН ХАРАКТЕР

Антон И. Манчев

София, Институт по отбрана „Професор Цветан Лазаров" ,
e-mail: a_i_manchev@abv.bg

***Резюме**: Гражданско-военното сътрудничество много често има ключово значение при решаването на всяка криза от невоенен характер. Взаимодействието между военни и цивилни следва да се осъществява на основата на точни и ясни правила за правата и отговорностите на всяка от страните. Нормативната база в нашата страна показва, че все още не се отделя необходимото внимание към Гражданско-военното сътрудничество. Действащата нормативна база е основно във ведомствените издания на Министерство на отбраната.*

***Ключови думи:** Гражданско-военно сътрудничество, кризи, кризи от невоенен характер, бедствия.*

Въведение

В наши дни живеем в условия на непрекъснато нарастване на опасността от кризи от невоенен характер. През последните години България премина през поредица от такива кризи: политическа, икономическа, бежанска, КОВИД-19, инфлационна, водна, засегната беше от редица наводнения, пожари и други бедствия. Всяка от тях оказа своето негативно влияние върху развитието на всички области на обществено-политическия живот в страната.

Зачестилите пожари и наводнения доведоха до огромни материални загуби, промениха живота на много български граждани, а бяха дадени и не малко човешки жертви.

Всичко това постави остро въпроса как да се управляват тези кризи, какво е състоянието на Системата за национална сигурност на Република България и нейните възможности за отговор на всяко предизвикателство от сложния и все по-бързо променящ се свят и каква е ролята на гражданско-военното сътрудничество за минимизиране на негативните последици.

Всичко това изисква да се изследва гражданско-военното сътрудничество при кризите от невоенен характер с цел повишаване на общия капацитет за разкриване на потенциалните заплахи, за адекватното управление на кризите и преодоляването на последствията от тях.

Целта на настоящия доклад е да се разкрият характерните особености на гражданско-военното сътрудничество при възникването, управлението на кризи от невоенен характер и ликвидиране на последствията от тях, да се разкрият основните предпоставки за успешното гражданско-военното сътрудничество и изведат някои проблеми на гражданско-военното сътрудничество, които възникват при кризи от невоенен характер, като се посочат и някои пътища за тяхното преодоляване.

1. Същност на кризите от невоенен характер

В наши дни много изследователи свързват понятието криза със специфични обществени състояния, които са предизвикани от природни явления, големи катастрофи, социални катаклизми и дори дълбоки политически противоречия. Това показва едно разширяване на същността на понятието криза, като в неговите характеристики се прибавят и елементи на неопределеност, което от своя страна още повече затруднява разбирането на същността на кризата като явление, което е свързано със специфични обществени отношения.

В нормативната база в страната няма дадено определение на понятието криза. Според чл. 2, ал. 1. на отменения Закон за управление на кризи „Криза по смисъла на този закон е такава внезапна или очаквана промяна на установеното състояние на живот, предизвикана от човешка дейност, събития или природни явления, при която са нарушени или застрашени животът, здравето и имуществото на големи групи от хора, територията, околната среда, културните и материалните ценности на страната.”[1]

Днес много изследователи свързват понятието „криза“ със специфични обществени състояния, предизвикани от природни явления, големи катастрофи, социални катаклизми и дори политически противоречия. С това същността на понятието се разширява значително, защото в неговата характеристика се добавя и елемент на неопределеност, което от своя страна много затруднява разбирането на същността на кризата като явление, свързано със специфични обществени отношения. На практика във всяка област или сфера на човешката дейност може да бъде нарушен баланса или равновесието и да възникне нестабилност или дефицит на ресурси. Това означава, че в зависимост от средата в която възниква и факторите, които я обуславят, кризата може да има различни определения и съдържание.

Кризите са ситуации, които са определени от изменението на вътрешни или външни фактори на средата и се характеризират със заплаха на основни ценности на обществото, ограничено време за реакция и високо ниво на неопредленост.

През последните години Република България премина през редица видове кризи от невоенен характер които дадоха своето отражение върху обществено-политическия живот в страната, а от там и върху живота на българските граждани. При възникването на всяко бедствие, катастрофа и т.н по места продължава да се разчита на доброволците и армията. Доброволците помагат с финансови средства, действат при спасяването на бедстващите хора, помагат с безвъзмезден труд при отстраняване на последствията. Но какво правят отговорните за това институции? Най-често действат след събитията, като раздават помощи, които често изобщо не могат да възстановят щетите. Постоянно, след всяко бедствие всичко това се повтаря, без да се осъзнава обстоятелството, че трябва да се вземат превантивни мерки, които така и не се взимат, като основното оправдание е липсата на средства.

Дефиниция за понятието „бедствие“ е дадена в чл. 2, от Закона за защита при бедствия - „Бедствие е значително нарушаване на нормалното функциониране на обществото, предизвикано от природни явления и/или от човешка дейност и водещо до негативни последици за живота или здравето на населението, имуществото, икономиката и околната среда, предотвратяването, овладяването, и преодоляването на което надхвърля капацитета на системата за обслужване на обичайните дейности по защитата на обществото ”[2]

Тук трябва да посочим, че кризата е обществено явление, а бедствието е природно. Разглеждайки тези две понятия „криза“ и „бедствие“ е необходимо да отбележим, че в Конституцията от 1991 г. и Закона за отбраната и въоръжените сили на Република България тези понятия липсват, а е използван термина „извънредно положение“.

Кризите от невоенен характер включват спешни и неочаквани ситуации, които изискват хуманитарна и спешна реакция, докато военните кризи включват заплаха или използване на сила и изискват военни и дипломатически реакции.

Управлението на кризите от невоенен характер в Република България е елемент на националната сигурност на страната и съгласно чл. 3 на Закона за защита при бедствия, включва: „1. планиране и превантивна дейност; 2. прогнозиране развитието на кризите; 3. ранно предупреждение; 4. анализ на кризите и определяне на алтернативи за реагиране; 5. подготовка и утвърждаване на планове за управление при кризи; 6. провеждане на операции за реагиране при кризи; 7. връщане към състояние на стабилност.“[2]

2. Гражданско-военното сътрудничество в съвременни условия

Гражданско-военното сътрудничество (Civil Military Co-operation) е нормативно определено само във ведомствените документи и издания на Министерство на отбраната: „Доктрината на въоръжените сили на Република България”[3], „Доктрината за гражданско-военно сътрудничество НП – 3.4.9”[4], „Пособие за специалистите по CIMIC” и „Тактики, техники и процедури ТПП по CIMIC“[5]. Тук трябва да отбележим, че въпросът за гражданското-военно сътрудничество не

се регулира в националните нормативни документи: Актуализирана стратегия за национална сигурност на Република България, Закона за отбраната и въоръжените сили на Република България, Закона за защита при бедствия, Националната стратегия за намаляване на риска от бедствия 2018-2030 г. и Указанията за разработването и готовността за изпълнението на планове за защита при бедствия (разработени от Съвета за намаляване на риска от бедствия към Министерския съвет на Република България).

Гражданско-военните отношения могат да се разглеждат като отношения между две страни. Първата страна на тези отношения са военнослужещите с техните организационни и управленски структури, а втората това са гражданите и организациите, в които те членуват. Съгласно т. 320 от Доктрината на въоръжените сили на Република България ,,Гражданско-военното сътрудничество представлява координация и взаимодействие на командирите с цивилните власти и население, както и с неправителствените и международните организации и агенции в подкрепа постигането на целите на операцията. То е приложимо в пълния спектър от мисии и операции на въоръжените сили в съюзнически или коалиционни операции зад граница, а на територията на страната, се осъществява координация и взаимодействие със силите за сигурност, държавната и местна власт."[3]

Така заложено в тези документи, Гражданско-военното сътрудничесто е основна част от подготовката и провеждането на всяка военна операция и спомага за постигането на политико-военните цели при кризи в мирно време.

Следователно, ГВС следва да се разглежда като комплексна дейност по координация и взаимодействие между военнослужещите и гражданските структури в хода на подготовката, провеждането и след приключване на операциите по възстановяване и подпомагане на населението при кризи от невоенен характер, включително и при природни бедствия.

Какво обаче показва съвременният прочит на състоянието на Гражданско-военното сътрудничесто у нас. Както се посочва в специализираната литература и в редица публикации, а и според нас, съществуват редица проблеми, по-важните от които са:

Първо, липсват достатъчно усилия в отговорните ръководни институции за превенция. Както вече посочихме, все още повечето усилия и средства се разходват за ликвидиране на последствията, а не за превантивни мероприятия. Поради това е необходимо усилията да бъдат насочени преди да са възникнали кризите, най-вече за „…подобряване на взаимните способности в процеса на превенция…."[6, стр. 69].

Второ, липсват единни процедури и правила за координация и взаимодействие между военнослужещите и гражданските структури в хода на подготовката, провеждането и приключване на операциите по възстановяване и подпомагане. Стана дума, че наличните документи са вътрешноведомствени, само за Министерството на отбраната, и за това е крайно наложително да съществуват „… ясни процедури, стандарти и правила за използване на въоръжените сили в подкрепа на граждански екипи и на населението…"[6, стр. 69].

Трето, липсва необходимото законодателство, което да посочи ясно какви са задълженията и отговорностите на отделните министерства, ведомства и организации по противодействие и преодоляване на последствията от различните видове кризи. Има и различни тълкувания, липсва ясна понятийна рамка дори в Конституцията и съответните закони. Дори няма и закон за управление при кризи, каквото е изискването и някои съюзни документи - Доктрината на НАТО за гражданско-военно сътрудничество (Allied Joint Doctrine for Civil-Millitary Cooperation), както и Концепцията на ЕС за ефективна гражданско-военна координация и поддръжка на хуманитарна помощ при бедствия. Крайно време е да има „.. обща правна рамка, която да регламентира правата и отговорностите на различните участници в операцията…"[6, стр. 70].

Четвърто, поради всичко изброено дотук, липсва и единна програма за съвместна подготовка на структурите на МВР, на формированията от МО, на доброволците, на организациите към общини, за неправителствените организации и т.н. От съществено значение да се разработи такава „...национална програма за съвместна подготовка…"[6, стр.70], която да бъде основата на съвместни действия и координация при провеждане на операциите.

3. Гражданско-военно сътрудничество при кризи от невоенен характер – съвременни аспекти.

За успешното гражданско-военно сътрудничество при кризи са необходими редица **основни предпоставки**, каквито са:

На **първо място** това е промяна на действащата в страната нормативна база, като закони, правилници, доктрини, наредби, правила и процедури, които регламентират цялостната съвместна дейност между двете страни: едната - командирите и военнослужещите и другата - цивилните власти и населението, заедно с неправителствените и международните организации и агенции.

На **второ място** е необходимостта да има точни и ясни процедури, протоколи и стандарти и на тяхна основа да се изготвят съвместни планове за действие, общи програми за обучение и тренировки и провеждане на съвместни учения.

На **трето мяст**о е необходимо, с цел осъществяване на бързо и точно взаимодействие между военнослужещите и цивилното население, и двете страни да са запознати и да разбират целите и възможностите на участниците в управлението на кризите. Това се постига чрез разработването на обща национална нормативна база, единни планове и провеждане на съвместни тренировки.

На **четвърто място** е необходимо военнослужещите да разбират целите, задачите и ролята на невоенните участници и цивилните структури, за да може да се осъществи безпроблемно взаимодействие между двете страни. Основна роля в това взаимодействие се изпълнява от експертите по Гражданско-военно сътрудничество от военнослужещи и цивилни служители от въоръжените сили.

На **пето** място екипите от CIMIC и участниците от въоръжените сили не трябва да се стремят да изместват цивилните участници при съвместната им дейност. Те трябва основно да оказват съдействие и да ги подпомагат. Най-важна е ролята на професионалистите от CIMIC в случаите когато цивилните участници нямат

необходимия капацитет за справяне при определени кризи. Това са случаите при които вследствие на бедствия гражданската инфраструктура е значително разрушена.

На **шесто място** екипите от CIMIC трябва да се привличат още при планиране на мероприятията и действията в случай на кризи. Когато се планират мероприятията и действията, целта е да се предотвратят евентуалните бедствия, а когато това не се случи - да започне незабавно преодоляване на последствията от тях.

4. Пътища за подобряване ефективността на гражданско-военното сътрудничество

На **първо** място трябва да бъде усъвършенствана нормативната база. Необходимо е да се приемат нормативни документи на национално ниво, които да регламентират Гражданско-военното сътрудничество, а не да се говори за ГВС само във ведомствените документи на Министерство на отбраната. Задължително е приемането на нова Стратегия за националната сигурност, за да може от нея да се определят задачите и ролята на ГВС. В бъдеще е необходимо при разработване на Национални стратегии за намаляване на риска от бедствия да се определят и ролята и задачите на ГВС.

На **второ място** е необходимо да се повиши ролята на превенцията и да се усъвършенства взаимодействието, чрез изготвяне на съвместни планове и провеждане на съвместни тренировки за тяхното усвояване. Трябва да се спре да се реагира пост фактум след бедствията, а да се повиши ролята на превенцията. Трябва да спре практиката за всички пропуски управляващите да се оправдават с липсата или недостига на средства.

На **трето място** е необходимо изготвянето на правила и стандартни оперативни процедури за взаимодействие между гражданските участници и военните екипи.

На **четвърто** място е необходимо усъвършенстване на нормативната база, като се регламентират правата и задълженията на военните и цивилните участници при съвместните им действия. Необходимо е изготвяне на съвместни планове и провеждане на съвместни тренитовки с цел тяхното детайлно усвояване.

На **пето** място е необходимо разработването на единни стандарти за действие на национално ниво и регионално ниво. На национално ниво те следва да се разработят от Съвета за намаляване на риска от бедствия и аварии към Министерския съвет, от Националния ситуационен център и бъдещия Секретариат към Съвета по сигурност. На местно ниво следва да се разработят от областните и общинските съвети за намаляване риска от бедствия.

На **шесто** място с цел подобряване на взаимодействието и привличането на необходимите сили и средства от въоръжените сили при гражданско-военното сътрудничество е необходимо непрекъснато да се обменя информация за риска от кризи (особено при бедствия и аварии, като пожари, наводнения и други).

Във връзка с Гражданско-военното сътрудничество въоръжените сили на Република България ще продължават при необходимост да се използват за съвместна дейност, за подпомагане и допълване дейността на другите национални

институции. Те ще продължат да поддържат способности за наблюдение и ранно предупреждение от потенциални рискове и заплахи от възникване на кризи от невоенен характер. Ще участват при нужда в защитата на застрашени стратегически обекти и обекти от критичната инфраструктура.

При необходимост ще се включат в противодействие на тероризма и преодоляване на последиците от него. Въоръжените сили ще продължават да неутрализират невзривени бойни припаси и при нужда ще се включат заедно с другите национални институции в подпомагане на населението при бедствия аварии и екологични катастрофи, ще предоставят хуманитарна помощ, и ще участват в оказване на първа и специализирана медицинска помощ.

Въоръжените сили заедно с други национални институции при нужда ще участват в евакуиране на бедстващо население, ще извършват животоспасяващи транспортни дейности, ще участват в овладяване на миграционния натиск и охраната на държавната граница, ще оказват съдействие за контрол на миграцията и приемане на лица, които търсят убежище на територията на страната. С една дума ще съдействат винаги и навсякъде на националните институции, когато има нужда.

Опитът показва недвусмислено необходимостта от сътрудничество на военните командвания с авторитетните международни организации, с органите на централната и местната власт, както и с неправителствените и правителствени организации, извършващи дейности в кризисните райони.

Заключение:

На този етап държавата все още не обръща достатъчно внимание на въпросите на гражданско-военното сътрудничество. Най-точен пример е това, че все още няма национални нормативни документи, в които то да бъде регламентирано. Разчита се само на ведомствените документи и изданията на Министерството на отбраната. Това поражда необходимостта от задълбочена работа на специалистите в областта на сигурността и отбраната, за да се подготвят проекти на тези нормативни актове, а на политиците да приемат тези документи.

Гражданско-военното сътрудничество се явява неизбежна необходимост при възникването на кризи от невоенен характер. Това изисква след приемане на нормативна база да се изготвят планове за осъществяване на гражданско-военното сътрудничество, да се осигурят необходимите средства и да се проведат тренировки за усвояване на тези планове.

Усъвършенстването на гражданско-военното сътрудничество при кризи от невоенен характер в Република България изисква изграждане на интегрирана система за координация, подобряване на взаимодействието, дигитализация на процесите и разширяване ролята на въоръжените сили, като ключов елемент в реагирането при бедствия и аварии.

Литература:

1. Закон за управление на кризи, Обн. ДВ бр. 19 от 2005 г., отменен с § 2, т. 3 от преходните и заключителните разпоредби на Закона за отбраната и

въоръжените сили на Република България, обн. ДВ бр. 35 от 12 май 2009 г., в сила от 12.05.2009 год.
2. Закон за защита при бедствия, Обн. ДВ бр. 102 от 19 декември 2006 г.
3. Доктрина на въоръжените сили на Република България, Издание (Б), С., 2025.
4. Доктрината за гражданско-военно сътрудничество НП – 3.4.9. С., 2014.
5. Тактики, техники и процедури (ТТП) по CIMIC. С., 2007.
6. Иванов, В., Гражданско-военното сътрудничество в помощ на населението при извънредни ситуации, статия в Научно списание „Сигурност и отбрана", брой 1, 2022 г., Издателски комплекс на НВУ „Васил Левски", гр. В. Търново, ISSN: 2815-388X – печат, стр. 59-72, (14 стр.).
7. Ivanov, V., Kisiov, M., "Opportunities to Improve the Civil-Military Cooperation in Emergencies", доклад на годишна научна конференция на НВУ „В. Левски", гр. В. Търново, 08-09 юни 2023 г., ISSN 2367-7481 (ел. издание), с. 753-764, (12 стр.).
8. Иванов, В., Кисьов, М., „Гражданско-военно сътрудничество в извънредни ситуации", доклад на международна научна конференция „Хемус-2022", 2-3 юни 2022 г., Международен панаир, Пловдив. Сборникът с доклади е с ISSN 1312-2916 (print) и е регистриран под № 2318 в Националния референтен списък на съвременни български научни издания с научно рецензиране (под печат), (13 стр.)
9. Allied Joint Doctrine for Civil-Military Cooperation, (AJP-3.19), Edition B (promulgated in June 2025).
10. EU Concept on Effective CIVMIL Coordination in Support of Humanitarian Assistance and Disaster Relief, 2019.

BULGARIA AND THE BLACK SEA DIMENSION OF REGIONAL SECURITY THROUGH THE PRISM OF THE MILITARY SPHERE OF THE TURKISH GEOSTRATEGIC PROJECT `BLUE FATHERLAND` AND THE RUSSIAN `NEUTRAL UKRAINE`

Michael P. Kozarski

Bulgarian Defence Institute `Professor Tsvetan Lazarov`, Sofia, Bulgaria,
e-mail: m.kozarski@di.mod.bg, ORCID № 0009-0003-8623-9855

Abstract: *The global change in the geopolitical and geostrategic security environment as a result of the escalation of conflict in the Middle East, Latin America and Eastern Europe in 2026 contributed to the faster transformation of the unipolar into a multipolar world. At the regional level, new centers of power are taking shape in the world, and one of these regions is the Balkans, and in particular the Black Sea adjacent to it. And it is here that the military-strategic, economic, political, social, demographic and other interests of two Great Powers of the old generation – Turkey and Russia – clash most strongly, and the projections of the geostrategic projects `Blue Fatherland` and `Neutral Ukraine` reflect most strongly on the entire National Security System of the Republic of Bulgaria. Therefore, the aim of the report is to analyze the potential negative effects on some of the segments of the Bulgarian Security System resulting from the two geostrategic projects.*

Keywords: *Geopotics, Balkan peninsula, Blue Fatherland, Neutral Ukraine, Russian-Turkish relations, Regional and National Security*

БЪЛГАРИЯ И ЧЕРНОМОРСКОТО ИЗМЕРЕНИЕ НА РЕГИОНАЛНАТА СИГУРНОСТ ПРЕЗ ПРИЗМАТА НА ВОЕННАТА СФЕРА НА ТУРСКИЯ ГЕОСТРАТЕГИЧЕСКИ ПРОКЕТ „СИНЬО ОТЕЧЕСТВО“ И НА РУСКИЯ „НЕУТРАЛНА УКРАЙНА“

Михаел П. Козарски

Институт по отбрана „Професор Цветан Лазаров“,София, България,
e-mail: m.kozarski@di.mod.bg, ORCID № 0009-0003-8623-9855

Резюме: *Промяната в глобален план на геополитическата и геостратегическата среда за сигурност, в следствие на ескалацията на конфликите в Близкия Изток, Латинска Америка и Източна Европа през 2026 година, допринесе за по-бързото трансформиране на еднополюсния в многополюсен свят. На регионално ниво се оформят новите центрове на сила в света, а един от тези региони е на Балканите, и по-специално на прилежащото към него Черно море. И именно тук се сблъскват най-силно военно-стратегическите, икономическите, политическите, социалните, демографските и други интереси на две Велики сили от старото поколение – Турция и Русия, а проекциите на водените от тях геостратегически проекти „Синьо Отечество“ и „Неутрална Украйна“ рефлектират най-силно върху цялата Система за национална сигурност на Република България. Ето защо целта на доклада ще бъде анализа на потенциалните негативни ефекти върху някои от*

сегментите на българската Система за сигурност, произтичащи от двата геостратегически проекта.

Ключови думи: *Геополитика, Балкански полуостров, Синьо Отечество, Неутрална Украйна, Руско-турски отношения, Регионална и национална сигурност*

Увод

Настъпилите промени в геополитическото и геостратегическото направления и през изминалите две години (2025-2026г.) по различните ключови региони на планетата, на практика зачеркнаха и останалите все още принципи и ценности от несъществуващият архитектурен модел на международен ред и глобална сигурност, наложен след края на Втората световна война, и доведоха до окончателното разбиване на Ялтенско-Малтийската система на международните отношения.

Оформиха се няколко по-големи макрорегиона в света – Китай, Русия, САЩ (които все още удържат някакви части и позиции на влияние), Великобритания (без дори да е член на ЕС), както и често подценявани или пренебрегвани държави като Египет, Иран, Саудитска Арабия, Турция, Пакистан, Индия, Републиика Южна Африка, Алжир и други се утвърдиха като макрорегионални лидери със своите сфери или орбити на влияние.

Китай продължава да разгръща своя пълен потенциал в глобалното пространство, основно акцентирайки на икономическото, технологичното, информационно- комуникационното и енергийното нива, като едновременно с това задълбочава двустранните и многостранните отношения в различните организации, в които членува и има едно от ръководните мяста в тях. Също така Китай ускорява вплитането на света все по-силно в геоикономическата интеграционната мрежа на новия модел на глобална сигурност и международен ред чрез своя мегапроект „Един пояс, Един път“. И макар че към момента проекта да е с множество блокирани транспортно-комуникационно-търговско-енергийни и други коридори по суша, море и въздух в регионите на Близкия Изток, Персийския залив, Черно море и Източна Европа, то същия проект бива пренасочен на север през Беринговия проток и към Северният ледовит океан чрез т.нар. „Леден път на коприната“ или Северният морски път на коприната. [1] А оттук алтернативен маршрут за свързване на глобалното пространство – предимно по въздух море през трасетата на северните морета и Атлантическия океан. И разбира се с допълнителен акцент върху космическото пространство. А по тези начини Китай къде пряко-къде косвено променя завинаги съдбата на света на геополитическо, геостратегическо, геоикономическо и други равнища.

САЩ от друга страна преориентрират своите интереси и желание за влияние в различни региони по света – с предимство са Южна Америка, Близкия и Средния Изток и акваторията на Тихия океан. Едновременно с това се опитват да блокират всякаква нежелани от тях действия от страна на Пекин и да го държат в шах и едновременно с това далеч от морските ширини на прилежащите му морета и най вече от откритите води на Тихия океан. И за разлика от Китай, акцентриа основно

върху военно-стратегическото, продоволственото, енергийното и не на последно място на технологичното измерение на сигурността. Открито вече от Вашингтон считат, че политиката на силата и принципа на „тоягата и морковът" е в основата на изповядваната от САЩ концепция за американското превъзходство в света. В допълнение към това, Вашингтон се опитва да възроди „Доктрината Монро", като към нея добави и някои експанзионистични моменти от т.нар. „Американски век" (XIX век) след края на Гражданската война и последвалият стремеж към глобална доминация. И в допълнение към това се усланя на концепцията за месианизма, както и високомерието, което те разпространяват из целия свят след края на Студената война и разбиването на двуполюсния модел на международната политика.[2] С други думи тя реши да се преформатира като нещо по-голямо, а именно „Глобална Америка", геостратегически проект с който да се противопостави на държавите членки на БРИКС и ШОС, и най вече на Китай и Русия. Но най-важното в цялата ситуация е, че и САЩ, и Китай, а също така Русия и още няколко велики сили са пренасочили своето внимание с по-голяма степен на интерес към Северното полукълбо (и по-точно към топящите се ледници на Ледовития океан и на Арктика).

И следователно най-нормалното, което се очаква да видим като проявление на конфронтацията между две от трите суперсили в света днес е т.нар. „Тукидидов капан", в който редица международни изследователи и специалисти по китайско-американските билатерални и мултилатерални отношения на държавно, частно и смесено отношение.[3] В това число и на все още изследваният от редица утвърдени и нововъзникващи изследователи въпрос за взаимодействието във военното дело между държавите и частните транснационалните компании.

След това очертаване на по-глобалните факти, ще поставим фокус върху двете Велики сили, които и до ден днешен оформят настоящето и бъдещето за нашия регион (Балканският полуостров) – Русия и Турция. Ето защо, за целта на доклада ще обърнем внимание на регионалната и националната сигурност на Република България в контекста на двата геостратегически ключово важни геостратегически проекта на Русия и Турция, засягащи пряко Балканския регион, Черно море и самата България, а именно „Неутрална Украйна" и „Синьо Отечество".

1. Генезисът на геостратегическите проекти „Неутрална Украйна" и „Синьо Отечество"

Русия и Турция са двете най-важни и същевременно ключови Велики сили когато се отнася до регионите на Балканския полуостров, Източна Европа, Кавказ, Черно море, Каспийско море, Близкия Изток и макрорегиона на бившата Персийска империя (ИР Иран). И двете са бивши мега държави, империи, които след разпада си се преформулират спрямо настоящия момент, но никога не се отказват от имперското си минало и дори продължават да изпълняват своите геостратегически идеи за реализирането на ребрандирания образ на империята, както и за популяризирането на същия имидж пред бившите подчинени народи. Сега ще разгледаме в най-общи щрихи двата предимно военно-стратегически проекта на Русия и Турция.

Геостратегическият проект ***„Неутрална Украйна“*** е военното отражение на по-големият, и с право можем да го наречем глобален проект на Русия за ребрандирането ѝ като модерна и все още влиятелна сила в сегашния свят – ***„Руски свят“***. Той е пряк отговор на настоящия свят в следствие на провала на комунистическата идея на разпадналия се в края на 1991 г. СССР, а след провала и на демократичното му ребрандиране като Общност на независимите държави (ОНД) в началото на 1992 г., това желание за противопоставяне с останалия свят единствено се засилва.

Последвалите този съвсем кратък период на турболентни свръхинфлационни, застрашаващи сигурността и единството на страната, застоят в космическата ѝ програма, концесиите които дава на Казахстан (полигоните Семипалатинск (за ядрени изпитвания) и Байконур (за космически полети и изследвания)) и Украйна (полуостров Крим и арендата на военноморската база Севастопол), както и пагубните за Военно-промишления ѝ комплекс загуби от липсата или пък закриването на традиционните пазари и свързаните с тях логистични връзки за тяхното снабдяване с модерни въоръжения и техника допълнително оказват натиск върху най-твърдолинейните политически фракции в страната. Сред тях са и евразийците на „Мозъкът на Путин“ Александър Дугин, на „Готвачът на Путин“ Александър Пригожин, Сергей Наришкин, Алексей Собчак, Дмитрий Медведев и много други. Необходимостта от търсенето на нови алтернативни предприятия, в това число и чрез опит за реинтеграция със Запада, и по-точно с евро-атлантическия свят също завършват с противоречив резултат за Москва. В един момент Русия дори е готова да влезе в НАТО и ЕС, още в края на 1990-те години, но поради една или друга причина това никога не се случва и тя се пренасочва към евразийската идея за „Руски свят“ на Дугин и неговите предшественици от ранните 1920-те години, или за по-лесно „ранните евразийци“ от поколението на Гумильов и Трубецкой, които обаче влизат в пряк разрез на официалната политика на тогавашния новообразувал се СССР.

Ето защо Мосвка с основание започва да търси първоначално скрит, а след 2022 г. и явен реванш срещу Запада, особено след идването на власт на настоящия президент Владимир Путин в последният ден на 1999 година. Този реванш се проявява най-силно на военно-стратегическо, технологично, продоволствено, суровинно-енергийно, туристическо и икономическо отношения. Това противопоставяне продължава и към днешна дата (4 години от началото на войната/Специалната военна операция с Украйна).

В най-общи линии военното измерение на „Руския свят“, а именно „Неутрална Украйна“ цели да предпази Русия от заплахата Украйна да се превърне в бастион, хъб или основна база за военно-стратегическо, логистично, продоволствено, енергийно и географско равнище. Русия иска да превърне Украйна в безопасна зона и буфер срещу НАТО и от 2025 година и на ЕС, като отдалечи двете конкурентни организации от границите си. Москва иска от Украйна декларация и явни действия по преустановяване на желанието на Киев да членува в редиците и да се признае за неутрална държава, по подобие на Швейцария, Лихтенщайн, Финландия и Швеция до 2022 г. и разбира се Австрия. Естествено Украйна отказва

да предприеме тази крачка и продължава в посока евро-атлантическото си интегриране, в следствие на това пряко застрашава сигурността на целия европейски континент чрез насърчаването на конфронтацията между Москва и Брюксел, а оттук и дискредитира имиджът на ЕС като мироподдържаща и миро насърчаваща организация пред целия свят. А изходът от войната/операцията така и не се вижда на този етап.

След разпадът на СССР в много шокиращ и почти блицкриг момент в края на 1991 г., Турция вече се оказва, че притежава най-дългото крайбрежие на Черно море и се превръща в своеобразен хегемон в този географски ареал. Но тогавашното все още светско и кемалистко управление на страната, което условно ще наречем кабинетът „Демирел-Йозал-Чичек-Ялмаз" предпочита да капитализира до максимума и с допълнителни дивиденти тази новообразувала се ситуация, като предприема следните три ключови важни за нея и нейната национална и регионална сигурност действия:

Първо: предлага донякъде приятелска ръка на доскорошния си смъртен враг (визирайки едновременно Руската империя и бившият СССР) и му предлага кооперация на следните равнища – икономика, търговия, туризъм, инфраструктура, обмяна на ценни предмети, културни мероприятия, стоки и услуги, и едновременно с това възползване в максимална степен от предимствата в търговията във волатилна валута, както и много други неща на социално-икономико-инфраструктурно-политическо и културно нива;

Второ: едно от водещите места в новообразуваната от нея Организация за Черноморско икономическо сътрудничество (ОЧИС – още през далечната вече 1992 г.), както и облекчен режим на филтрация на руските туристи в Истанбул и турските черноморски и средиземноморски курорти. Предимно, благодарение на руските инвестиции турците акцентират върху развитието на някогашните си дълбокопровинциални села Кушадасъ, Мармарис и Анталия. Едновременно с това Турция възприема политиката на наречената от нас в рамките на доклада „прехвърляне на волейболната топка" с Русия, като успява да я убеди да започнат съвместна политика за привличането на бившите общи владения в редиците на ОЧИС. Не случайно, с много малки изключения – всички бивши руски и турски подвластни територии са страни членки на ОЧИС, от което може да заключим че може би в кабинетът Демирел-Йозал-Чичек-Ялмаз е имало наченки за съвместно попечителство или кондеминиум между Русия и Турция, с повече роля на Турция, по линия на сътрудничеството Москва-Анкара;

Трето: намалява в значителна степен американското присъствие в платото на Анадол, като единствено базата Инджирлик остава в предимно американско влияние, а едновременно с това започва да гледа във всяка една посока на света и спира да се чувства като авантпост срещу потенциална война между СССР-САЩ и ОВД (Организацията на Варшавския договор) – НАТО и акцентира върху акумулацията на колкото е възможно повече енергийни носители от близките (в това число и в съседен Азербайджан) и по-далечните географски ареали на света. С други думи акцентра върху енергийното измерение на сигурността, като си сътруднчи с Русия не само на това, но и на икономическо, туристическо,

продоволствено и някои други такива. Приоритет за нея остават да „открадне" на най-високите цени и най-висококачествени въглеводородни продукти и да предложи територията си по изграждането на най-модерните инфраструктурни горивни пътища и коридори по коридора Север-Юг, а именно ТАНАП, ТАП, Южен поток, Син поток и други. Някои от тези проекти са и с руски произход (Южен поток и Син поток). От което пък да си подсили позициите за по-близкото и по-далечното бъдеще на страната и да начертае своята геостратегическа империалистическа визия в рамките на Балканите, Централна Азия, Черноморско-Каспийския регион и дори Синдзян (Китай). А защо не и да развие свой собствен геостратегически проект, като например ***„Синьото Отечество"***.

Турският геостратегически проект, с предимно военно-стратегическа насоченост **„Синьо Отечество" (Mavi Vatan)**, представлява най-новият и най-актуален опит на Турция да възроди духът на „прогресивната" Османска империя и да превърне Анкара в една от водещите навални (морски) сили в света. Създаден първоначално като военна концпеция или доктрина от Военноморските сили на Турция, тази идея скоро се превръща в реален геостратегичекси проект за придобиване на вярност сред народите в бившите османски вилаети и своеобразното ребрандиране на Република Турция в положителен образ на бившата Османска империя, акцентирайки върху военноморското превъзходство на Анкара в Медитаранът (Средиземно море), Черно, Йонийско море и разбира се желание за потенциална експазия в Атлантическия океан, Червено море, а оттам и по целия Световен океан. [4]

Естествено този проект има своите корени в прословутата книга на Ахмет Давутоглу „Стратегическа дълбочина". И едновременно с това представлява пряка конфронтация с Русия на по-късен етап по суша и море – по-специално в Сирия (цели да изгони завинаги руснаците от доминиращите им позиции във военноморската база Тартус в Източното Средиземноморие и от военновъздушната им база Хмеймим в провинция Идлиб) и на полуостров Крим (тъй като Турция така и не можа да възприеме идеята, че Крим е съставна част от Русия и не принадлежи вече на Украйна). Поради което постоянно си търсеше поводи за конфорнтация и унижение или поне дискредитиране на имиджа на Русия в глобалното пространство. Не случайно, скорошните действия на Турция (по-специално в периода 2020–2026 г.) в Нагорни Карабах срещу арменците, Северна Сирия срещу ИДИЛ и Израел, Западна Либия срещу войските на фелдмаршал Хафтар Халифа, фортификацията на Северен Кипър и насърчаването на новото му ръководство за противопоставянето с фициален Кипър (Южен, както го наричат официално турските политици, военни, експерти и специалисти в различни области на цялата Система за национална сигурност), търсенето на енергийни ресурси и други суровини в синьото пространство на мегаконтинента Евразия, както и решаваща ѝ роля в създаването на „Мюсюлманското/Ислямското НАТО" или Меканското споразумение между нея, Саудитска Арабия и Пакистан в контекста на продължаващата вече шест месеца война на изтощение между САЩ и ИР Иран, доказват релевантността и жизнеспособността на „Синьото Отечество" на Турция в многоизмерен план.

Синьото Отечество има и още един аспект, а именно – окончателното психическо смазване на морала на балканските, и по-специално на Гърция и Южен Кипър, близкоизточните и кавказките народи и нации, които продължават да разчитат на външна намеса на Великите сили за задържането на турската многоизмерна експанзия спрямо техните земи, ресурси, богатства, речни, морски и въздушни пространства. И както личи, особено след намаляването на паритета на военноморска сила на Русия в Черно море след началото на украинската война и загубата на някои от най-силните военноморски съдове нв Русия, влиянието и силата на Турция в това море нарастват с всяка изминала година. А оттук и реалната опасност за България да се превърне в абсолютният маргинал на по-обширния Балкано-Черноморския регион.

И по подобие на руския геостратегически проект „Неутрална Украйна" или по-големият „Руски свят", така и при турският „Синьо Отечество" България и целият регион отново се намират в окото на геополитическата, геоикономическата и геостратегическата буря. Ще обърнем внимание на пет проблема или негативни геостратегически ефекти за двата геостратегически проекта.

2. България в позицията на „Чукът и Наковалнята" през проекта „Неутрална Украйна"

България и Русия имат традиционно много добри взаимоотношения, като техният най-нов етап датира от Освободителната война между Русия и Турция, след погрома на Априлското въстание и неуспешната за коалицията Сърбия-Черна гора тройна война Сърбо-черногорско-турска или Сръбско-турската от лятото на 1876 г. И именно героизмът на априлските въстаници, както и безкрайната смелост на първообраза на Въоръжените сили на Република България (Опълченците на Шипка) допълнително скрепяват нерушимата общославянска връзка между Русия и България поне до ранната 2022 година.

Разбира се, не винаги обстоятелствата на билатерално ниво са били такива – Русия (и по-точно Киевска Рус) и двете Българии (Волжка и Дунавска) са били в меко казано обтегнати отношения през целия период на Средновековието, но след като Москва превзема последният бастион на Волжка България – град Казан, а пък само век по-рано Турция превзема България на Дунав, то Русия определено цели да постигне нова цел в своето геополитическо и геостратегическо съществуване – прекършване на гръбнака на Исляма (разбивайки Турция и Иран (тогава наричана още Персия) на дипломатическо и на военно ниво), подчинявайки неговите бастиони в двата края на Европейския полуостров, а оттам и разширение по цялото протежение на мегаконтинента Евразия. По този начин легитимирайки се като Бастион на Православието и покровител на цялото Християнство. В последствие тази мисия бива разширена с окупирането за вечни времена на Истанбул (бивш Константинопол), излизането на бреговете на пристанището Бендер Абас на Персийския залив и едновременно с това да получи достъп до бреговете на Средиземно море и . С други думи да направи своя прототип на съвременните понятия „мегаимперия" и „мегадържава", или „Глобална Русия". Но за тази цел е необходимо първо да спечели симпатиите и доверието на балканските народи. Ето

защо през вековете на османското робство, Русия гледа да спечели доверието най-вече на народа на Дунавска България, като същевременно използва него и идеята му за обединена национална държава едновременно като инструмент, на братски народ, а също така и на безпристрастен плацдарм и военен полигон за разширение на влиянието си отвъд ареалите на Черно море. [5]

След Освобождението има няколко кратки периода на неразбирателство между България и Русия по различни външнополитически въпроси на Балканите (Съединението, Независимостта, Междусъюзническата и разбира се последвалите я две на брой световни войни), но все пак двете успяват да намерят общ език, ценности, интереси, търговия, култура, социални и ценности (поне в периода на Студената война 1944-1989г.) и в крайна сметка да се обединят по линия на социализма и комунизма срещу тогавашният общ враг на империализма и капитализма, с главни центрове САЩ и Великобритания, както и срещу Турция и тогава все още родило се и прохождащото НАТО. Но след разпада на СССР и края на Студената война, както и с временното инсталиране на свръхмодерният и „непогрешим" за онова време еднополюсен модел, Русия и Турция започват да се сближават в икономическо, туристическо, енергийно, продоволствено и в други отношения, а от идването на Реджеп Ердоган на власт, Анкара се стреми да се наложи като регионален, а в последствие и глобален лидер, възползвайки се от евтините горива и суровини идващи от Русия и бившият СССР. Но едновременно с това да се разшири и да изтласка Москва от бившата съветска орбита на влияние. По-точно става въпрос за регионите на Централна Азия, Кавказ, Балканите и Източното Средиземноморие.[6]

В следствие на постепенното руско изтегляне от зоната на Балканите и Черноморието, България се оказва буквално в позицията на „чук и наковалня" не само за Русия и нейните последващи геостратегически проекти – вариращи от ОНД до Евразийски икономически съюз (ЕАИС), но и спрямо Турция и нейните геостратегически проекти „Зелена дъга"/„Диамант" и „Синьо Отечество". За последният ще стане дума в следващата подточка, тук обаче ще разгледаме техният антипод „Руският свят" или по-точно неговото военно измерение „Неутрална Украйна".

Парадоксът тук е, че България нито на официално, нито на неофициално ниво желае да бъде част от руската сфера на влияние, нито пък да участва в руско-китайките (БРИКС, ШОС и други които вероятно вече се изграждат) и самостоятелните руски евразийски геостратегически идеи, доктрини и проекти. Тя твърдо е заявила своята евро-атлантическа принадлежност и не желае да замени ЕС за ЕАИС, НАТО за ОДКС (Организацията на договора за колективна сигурност) и въобще да замени евро-атлантизма за сметка на многопластовата идея на Москва за изграждането и усъвършенстването на „Руския свят". Поради което още през 2022 г., София беше обявена за „неприятелска държава" наравно с целият ЕС, Швейцария, Великобритания и някои други държави. [7]

Поради всичко това, може да кажем че от началото на 2022 г. България е в епицентъра на реализирането на военното направление на геостратегическия проект „Руски свят", който ще наречем „Неутрална Украйна".

Потенциалните негативни ефекти, които този проект нанася върху нашата целокупна Система за национална сигурност, пречупени през военното измерение на сигурността са следните:

Първо: умиротворяването на Украйна. В началото Русия изиска от Украйна да се признае за неутрална и да не участва във военни съюзи и най-вече НАТО. По тази причина Русия гледа да направи Северното Черноморие едновременно в демилитаризирана зона и да лиши Украйна от Черноморското крайбрежие, за да си обезопаси морската сигруност и да отреже напълно достъпа на Киев до тези инфраструктурни коридори и пътища към останалия свят.

Второ: самата милитаризация на Черно море, която ще се прояви с евентуалното отваряне на Проливите и конфронтацията между Русия и целият Северноатлантически съюз. А това означава и смъртоносна опасност за България във всяко едно направление, в това число и туризмът по Черно море.

Трето: продоволствената криза, която ще настъпи в следствие на продължаващата война, както и обстрелът на морските плавателни съдове от цивилно и военно естество.

Четвърто: българските ВМС, както и морските съдове на МВР ще бъдат най-уязвими, защото ще бъдат въвлечени в започнето на умишлено обстрелване както от Украйна, така и от Русия, а не е изключено да се стигне и до по-голяма черноморска криза, която да обхване продоволствената, енергийната, икономическата, финансовата сфера на страната, а оттам насетне и до политическа криза в България.

Пето: мигрантска криза след разминирането на определени коридори от морето и създаването на предпоставки за мигрантски натиск от морето към сушата. И следователно невъзможност за справяне с тази настанала ситуация.

3. България в Сянката на турския полумесец или Геостратегическият проект „Синьо Отечество" на Турция и потенциалните негативни ефекти върху нейната и регионалната СНС

Абстрахирайки се от негативното общо минало в двустранните българо-турски отношения в периода на Междувоенния период и на Студената война, както и отрицателното възприятие на голяма част от българското население спрямо Турция, когато все още е ядрото на не съществуващата вече Османска империя. Сега над България съществува съвсем нова, пълзяща на бързи обороти спрямо нея и в морското пространство на цяла Евразия опасност – реанимацията на Османската империя чрез икономическата, военната, продоволствената, енергийната, комерсиалната и стратегическата мощ на Турция в морското пространство. А именно успешното реализиране на геостратегическия проект „Синьо Отечество" и излизането на Турция в морското пространсто, точно както Османската империя през XV-XVI век. А оттук и превръщането ѝ не само в навална сила, но и в една от новите глобални сили в многополюсният свят.

Някои от потенциалните по-негативни ефекти, които ще се проявят пряко върху СНС на Р България и оттам върху цялата държава, в следствие на

засилването на навалното военно присъствие на Турция в Черно море и временното отслабване и понижаване на руското такова, са следните:

Първият от тях е усилването на военното присъствие на Турция и изпращането на нови военни кораби да патрулират не само в южната, но и в северната половина на морето, а оттам и да проектира нейната хегемония в акваториите на Черно и Средиземно море, а в последствие и на останалата инфраструктура на Апенините, Балканите, Кавказ и в Източна Европа. Оттам влиянието ще се прехвърли и върху Централна Азия, Каспийско море и разбира се Синдзян-Уйгур, което не е изключено да се свърже и с по-старата доктрина за създаване на митологичната общотюркска държава Велик Туран, от което да последва нова конфронтация с всички регионални и глобални играчи в тази част на света – Китай, Иран, Индия, Пакистан и Русия именно за тези апетитни откъм природни наземни и подземни ресурсири региони на света.

Вторият ефект е увеличаването на финансовия, икономическия, културният, промишленият, инфраструктурният и енергийният натиск върху всички нейни конкуренти, в това число и чрез разтурването на старите организации от страна на Турция – по-точно на НАТО и ОЧИС, както и допълнителното смазване на геоикономическо ниво чрез различни инструменти (демография, икономика, преки чуждестранни инвестиции, военно-стратегическо присъствие, обявяване на митническа война (възприемане на политиката на протекционизъм), миграция и други) на ЕС (дори и чрез сценарий „Брекзит", в случай че тя все пак един ден влезе в неговите реидици), и преориентирането ѝ към новите такива (Мюсюлманското НАТО/Споразумението от Мека, някой нов потенциален военен съюз от регионите на Близкия, Средния или Далечния Изток, БРИКС, ЕАИС, ОДКС и ШОС).

Третият ефект е самата милитаризация на Черно море, при която може Турция максимално да се възползва от своето географско положение и окончателно да отвори, или пък за постоянно да затвори двата пролива.

В първият случай ще предизвика пряк сблъсък на всички държави от НАТО (особено онези от „Коалицията на Желаещите"), които желаят да водят война с Русия, да застраши териториите на държавите участнички, превръщайки техните пространства в легитимни цели за Въоръжените сили на Руската федерация и да ескалира конфликта между нея и Украйна на едно съвсем ново по-високо ниво. Не е изключено дори и да се достигне до ядрен отговор. И всичко това ще застраши във всяко едно отношение най-пряко именно България, защото е най-близко географски до конфликтната зона и е заела твърда евро-атлантическа и проукраинска позиция, а също така не е способна да лавира на различните нива на двустранните и многостранните отношения между Русия-САЩ, Русия-НАТО и Русия-ЕС и в по-големият им еквивалент Изток-Запад или Глобален Юг-Колективен Запад.

Във вторият случай Турция ще предизвика енергийна и продоволствена криза, примесена със самата милитаризация на морето. Оттук нататък България и Черноморските държави ще претърпят редица съпътстващи вторични и третични загуби, които ще засегнат целите СНС на тези държави. Сред тези загуби ще

бъдат – невъзможност за износ на свежи продукти, храни, течности и лекарства, чийто срок на годност ще изтече и ще се превърнат в ликвидни продукти. Прогресивно, но в геометрична прогресия, ще започне и повишаването на нивото на инфлацията, а след това и съпътстващата я свръхинфлация, ще последва и допълнителна повишена цена на горивата, а оттам нататък и на всички хранително-вкусови, напитки, индустрии за преработки на суровини и на стоки от първа необходимост. И разбира се ще постигне желаният ефект – допълнителна дискредитация на евро-атлантическата общност, в това число и на общата европейска валута (еврото) в очите на всички европейски народи. Сферата на услугите също ще бъде перманентно парализирана (и в последствие ще бъде доведена до окончателен фалит), същата съдба ще последва и банковият сектор, и всички структури на частния сектор, ще се ударят индустрията и енергетиката и ще доведат до окончателния фалит и закриването на множество държавни, частни и смесени предприятия, както и на изтеглянето на всички ликвидни налични капитали от България и регионите на Балканите и Черноморието, и ще ги премести на по-сигурни и спокойни развиващи се и развити региони на света. И в последствие сегашните инфраструктура и функциониращите към момента логистични вериги ще бъдат окончателно прекършени и изобщо ще спрат да функционират по сегашните им механизми.

Четвърто е екологична катастрофа – все пак Турция все още иска и не се е отказала да прокара алтернативен канал, който да бъде използван за лост за лавиране между Великите и Супер силите в света, като също така ѝ позволява да заобикаля и когато си пожелае напълно да пренебрегва Конвенцията от Монтрьо. Оттук ще се образува и прилив на допълнителни количества води от Средиземно в Черно море, а това ще доведе до промяна на екологичната обстановка в нашия регион завинаги.

В допълнение към това ще предизвика сблъсък между луксозните пътнически кораби или на военноморски такива с по-старите, или излизащи вече от употреба кораби за пренос на горива и други видове стоки, а оттук и ще последва и предизвикването на екологична катастрофа – разливи и изгаряния на горива в Мраморно, Черно, Йонийско и/или остатъка от Средиземно море.

Не бива да изключим и умишленото стълкновение и дори обстрел на танкерите и лайнерите от военните кораби и дори допълнително миниране на морето от страна на воюващите страни и посредничащата им Турция, по подобие на случващото се в Ормузкия проток и островите от двете страни на протока от февруари 2026 г. между Иран и САЩ + Израел във войната им срещу Техеран. И оттук се наблюдават всички аспекти военно-стратегически, технологични, ресурсни и технически параметри на асиметричната война. Нещо като библейският разказ на битката между Давид и Голиат в долината Илам. Същият сценарий не е изключен да се повтори и в акваторията на Черно и Мраморно морета, и по-точно на входа/изхода на протоците Босфор и/или Дарданели.

Петото е инфраструктурният колапс, което е примесено между две или повече от изброените проблеми, които Турция може да причини на Балканско-Черноморският регион . От което ще последва възходът на всичко, което се намира

на Изток от Константинопол (Истанбул). Или с други думи България да падне под Сянката на „Синьото Отечество“ и да бъде включена в турската орбита или сфера на геополитическото, геостратегическото и геоикономическото влияние и под пълната многостранна зависимост на Анкара.

Заключение

Анализът на геополитическите процеси на Балканите и в Черноморския регион показва, че динамиката на сигурността вече не се определя от мирно съвместно съществуване, а от сблъсъка на ревизионистки и геостратегически проекти. От една страна, турският проект „Синьо Отечество“ (Mavi Vatan) си поставя за цел разширяване на морския суверенитет и доминиране в Източното Средиземноморие и Черно море, превръщайки Анкара в незаобиколим регионален център на сила. От друга страна, руският проект за „Неутрална Украйна“ цели пълно блокиране на евроатлантическата интеграция на Киев, демилитаризация на северния черноморски бряг и превръщането на Черно море в руско езеро за проекция на сила. За Република България този геополитически натиск поставя пряка заплаха пред критичната инфраструктура, Изключителната икономическа зона (ИИЗ), корабоплаването и националния суверенитет. Страната се намира в ситуация, в която сухопътната и морската ѝ сигурност изискват не просто пасивна интеграция в НАТО, а изграждане на реален възпиращ потенциал срещу тези и други бъдещи потенциални геостратегически проекти и на други регионални и световни Велики сили.

Литература

1. Илиев, Аспарух, Новият етап на "Един пояс, един път" демонстрира как Китай се адаптира геополитически, Investitor.bg, 16.02.2026 г., достъпно на: https://www.investor.bg/a/516-politika/426570-noviyat-etap-na-edin-poyas-edin-pat-demonstrira-kak-kitay-se-adaptira-geopoliticheski
2. Кирилова, Цвета, „Един пояс, един път”: националната кауза на Китай през XXI век, списание „Геополитика, 25.09.2023 г., достъпно на: https://geopolitica.eu/2023/206-broy-4-2023/3791-edin-poyas-edin-pat-natsionalnata-kauza-na-kitay-prez-hhi-vek
3. Инджов, Момчил, Клуб Z, Американското нахлуване във Венецуела е спорно. Но трябва ли да жалим за режима в Каракас?, 04.01.2026 г., достъпно на: https://clubz.bg/169602
4. Караколева, Мартина, “Капанът на Тукидид”: Повтаря ли се историята… или я разказваме погрешно?, 22.04.2025г., достъпно на: https://lider.bg/kapanat-na-tukidid-povtarya-li-se-istoriyata-ili-ya-razkazvame-pogreshno/
5. Maritime.bg, Ердоган постави доктрината „Синьо отечество“ в центъра на морската отбрана, 01.09.2025г., достъпно на: https://www.maritime.bg/129269/
6. Fakti.bg, Турция заплаши Гърция: Никога няма да се откажем от суверенните си права в Синьото отечество, 15.01.2025г., достъпно на:

https://fakti.bg/world/941745-turcia-zaplashi-garcia-nikoga-nama-da-se-otkajem-ot-suverennite-si-prava-v-sinyoto-otechestvo

7. България / История // Васил Гюзелев. „Голяма енциклопедия БЪЛГАРИЯ“. Т. 2 (БЪЛ – БЪЛ). София, БАН, Труд, 2011. ISBN 978-954-8104-23-4
8. Златарски, Васил. История на Българската държава през Средните векове, т.1, ч.1. Второ фототипно издание. София, Академично издателство „Марин Дринов“, 1994, [1918]. ISBN 954-430-298-0
9. Каменаров, Стефан, Неутралният статут на Украйна: решение или „замразяване” на проблема?, сп. Геополика, 19.06.2022г., достъпно на: https://geopolitica.eu/2022/199-broy-3-2022/3582-neutralniyat-statut-na-ukrayna-reshenie-ili-zamrazyavane-na-problema

CHALLENGES ENCOUNTERED IN EMERGENCY MANAGEMENT INVOLVING THE ARMED FORCES OF THE REPUBLIC OF BULGARIA

Ivan K. Vladov

Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, ivankvladov@abv.bg

***Abstract**: The report examines the means and methods by which the army supports state agencies involved in emergency situations, as well as the mechanisms for coordinating actions among these agencies.*

***Keywords:** Emergency situation, Bulgarian army,*

Introduction

In the current conditions of increasing natural, man-made and other risks, the protection of the population and the limitation of the consequences of emergencies are an important task for the state. Floods, forest fires, earthquakes, industrial accidents and other disasters can lead to significant human, material and economic losses and require a timely and well-coordinated response from the competent institutions. In this context, the participation of the Armed Forces of the Republic of Bulgaria in activities to prevent and overcome the consequences of emergencies is of particular importance. In addition to its main function of ensuring national security and the defense of the country, the Armed Forces possess significant human, technical and organizational potential, which can be used to assist the population and state bodies in the event of large-scale disasters and accidents. The participation of military personnel and military formations in such situations is carried out under certain regulatory conditions and in coordination with the state and local authorities, as well as with other structures of the disaster protection system. It may include rescue and emergency recovery activities, population evacuation, engineering and logistical support, firefighting, transportation of people and materials, as well as detection and disposal of unexploded ordnance. The relevance of the topic is determined by the need for effective use of the available national capabilities for responding to emergency situations and the importance of inter-institutional interaction to limit their consequences. That is why the role, tasks and capabilities of the Armed Forces of the Republic of Bulgaria in emergency situations have both theoretical and practical significance.

1. Emergency situations

An emergency is a condition or circumstance that arises suddenly, differs from the usual, normal situation or condition and requires rapid, coordinated action to prevent or limit damage to people, property, the environment or public order.

The term "emergency situations" on the territory of the Republic of Bulgaria covers various complex or dynamic events and circumstances that seriously threaten the life, health, security of citizens, the environment, infrastructure or public order, and require special, urgent measures by the state and society. These events can be classified

according to various characteristics according to their origin, the affected area, or the degree.

The main categories of factors that can lead to emergency situations can be diverse in their origin, considering their nature, origin and potential impact.

14. Natural factors (They are the result of natural phenomena and are often uncontrollable by humans):Земетресения;
    15. Floods;
    16. Hurricanes, typhoons, tornadoes;
    17. Snowstorms and avalanches;
    18. Droughts;
    19. Fires (forest or lightning);
    20. Volcanic eruptions;
    21. Landslides and collapses;
22. Man-made/technological factorsАварии в промишлени предприятия;
    23. Leakage of hazardous chemicals or gases;
    24. Nuclear accidents;
    25. Urban fires
    26. Vehicle disasters (train, plane, truck with dangerous goods);
    27. Collapse of buildings, bridges, tunnels;
28. Biological factors
    29. Epidemics and pandemics (e.g. COVID-19, influenza);
    30. Biological attacks or terrorism;
    31. Mass spread of pests or diseases in plants and animals;
32. Social factors
    33. Wars and armed conflicts;
    34. Terrorist attacks;
    35. Mass riots, protests, riots;
    36. Mass migration or refugee crises;
37. Economic and infrastructure factors
    38. Economic collapses;
    39. Power, water or communications outages;
    40. Transportation system collapse;
    41. Cyberattacks on critical infrastructure;

This knowledge is key not only for specialists in the field of civil protection and crisis management, but also for the general public, as it raises awareness and helps build a culture of safety.

2. Ways and means of the Bulgarian Army for participating in emergency situations

The main role of the army is to protect the sovereignty and territorial integrity of the state. To achieve these tasks, the Bulgarian army must be well prepared to have the necessary technical capabilities to have a timely reaction on its part in the event of a threat. In addition to the main role of the army, it has another task: supporting the

population in peacetime by taking part in emergency situations that arise on the territory of a state, providing support through:

- Sending personnel or equipment to the areas where an emergency situation has arisen and cooperating with representatives of other ministries involved.
- Assists the state or other structures of the state, local or regional authorities with transport and logistical capabilities
- The army's medical structures can support state hospitals
- The army's specialized capabilities and capabilities come into play in the transportation, evacuation and removal of the population from the affected areas or infrastructure.
- Engineering capabilities can be used to clear the destruction or build temporary facilities and help restore the infrastructure.

It is the armed forces that are the bearers of such capabilities, as they combine discipline, flexibility, high operational capacity and strategic planning, which makes them a key tool in managing complex and multi-layered emergency situations. Examining their participation through the prism of institutional resilience shows that the army should not be perceived only as a reserve resource, activated when the capabilities of civilian structures are exhausted, but as an organically integrated element of the prevention, preparation, response and recovery model. With its ability to maintain constant readiness, to react in conditions of a highly degraded environment, to provide logistical, engineering, medical and communication support and to contribute to the restoration of critical infrastructure, the army becomes a guarantor of the functionality of the state in extreme events. This is especially important in the context of growing climate risks, digital dependence and the vulnerability of society to strategic shocks.

3. Problems and challenges in emergency response

The problem of the participation of the Bulgarian Army in emergency management is considered mainly through the prism of national security, civil-military cooperation, crisis management, population protection and the development of disaster response capabilities. We are gradually observing a change in the understanding of the role of the armed forces. The army is no longer considered solely as an instrument of military defense, but also as a resource of the state in large-scale disasters and crises. Military support in complex emergency situations can be defined as a key component of national resilience. The effectiveness of this support depends on the coordination between military and civilian structures, trust between institutions, joint training between internal and external security structures and representatives of territorial and local authorities and the development of the regulatory framework.

The main difficulty encountered in the presence of an emergency is a clear and precise mechanism for managing the structures taking part in it, and thus problems arise related to:

- Do the structures that need the support of the army in an emergency situation know when and how to request its participation?
- What are the resources that it can allocate (such as personnel and equipment)?

• Who carries out the unified coordination of actions between the various structures taking part?

• Who collects, processes and exchanges information between the participating structures?

• How are the achieved results evaluated?

Other obstacles that may arise arise from the insufficiently developed programs for preparation, education, training and exercises between ministerial and civilian structures.

The development of a national program for joint training and the annual conduct of joint exercises under a unified scenario will help to clarify the interaction between the structures of the army, police, fire brigade, medical teams and representatives of local and regional authorities.

A problem related specifically to command and coordination arises from the possibility of a situation getting out of control and the scale of the emergency requiring the presence of:

- Fire brigades;
- Police;
- Medical teams;
- Volunteer formations;
- Local administration;
- Regional administration;
- Military formations;
- Emergency teams (private sector on-duty teams);
- Engineering teams;
- Other private or state structures with specific goals and tasks;

Difficulties encountered with the personnel situation in the Bulgarian Armed Forces is one of the problems that also limits their ability to perform defense and civilian tasks in parallel. In recent decades, the size of the army has been reduced many times, which inevitably leads to a decrease in the available personnel that can be deployed in emergency situations. An additional complication is the competition between different missions - participation in international operations, guarding state borders and maintaining combat readiness. In addition to human resources, the logistics system also creates a problem. Some of the equipment is outdated or insufficient, especially in areas where off-road vehicles, specialized equipment for rescue activities or means for mass evacuations are needed. In the case of major disasters, this leads to situations in which the army has the desire and readiness to get involved, but lacks appropriate technical resources.

Conclusion

The summary of the theoretical, conceptual aspects of emergency management with the participation of the armed forces shows a profound transformation in the understanding of modern risks, threats and response mechanisms. Within the dynamically changing global environment, security is becoming a multi-layered and interdependent process in which natural disasters, man-made accidents, hybrid attacks, cyber threats and social crises form a complex system of interacting factors. This requires

not just improvement, but a fundamental rethinking of the role of state institutions, their operational connectivity and the place of the armed forces in the architecture of national resilience. The conclusions unequivocally show that emergency management cannot be thought of as a linear and reactive activity, but as a continuous, cyclical, predictive and scientifically based process that integrates prevention, preparedness, response and recovery into a single strategic model. In this model, the armed forces acquire key importance not because of institutional tradition, but because of their unique ability to act in conditions of uncertainty, to provide critical infrastructure and to support civil systems where their capacity is exhausted or structurally insufficient. The army stands out as a factor of stability, reliability and operational discipline in moments when the reaction time is minimal, events develop uncontrollably, and the available resources of civil institutions cannot absorb the load. The ability of the armed forces to deploy operational formations, engineering resources, communication systems, medical teams, transport vehicles and logistical support within hours is a strategic advantage that no other institution in the state possesses on a similar scale and synchrony. However, this does not mean that the army should become a universal performer of all tasks, but that its role should be clearly defined, normatively regulated and integrated into the civil protection system.

References

1. НП-3.4.9 - Доктрина за гражданско-военно сътрудничество, МО, София, 2014.
2. Национален план за защита при бедствия, Министерски съвет, С., 2010.
3. Националната стратегия за намаляване на риска от бедствия
4. 2018 - 2030 г., Министерски съвет, С, 2018 г.
5. Кертиков, П. (2015). Системи за командване и контрол (С3) при кризи. София.
6. Дерменджиев, К. Роля на въоръжените сили при бедствия и аварии. София: НБУ, 2018.
7. Ангелов, В. (2019). Ефективност на взаимодействието на институциите при бедствия. Национална сигурност и бъдеще, 1(2), 44–57.
8. Allan, S. (2020). Military support to civil authorities in extreme situations. Routledge.
9. NATO. Allied Joint Doctrine for Civil-Military Cooperation (AJP-3.19).
10. NATO. Allied Joint Doctrine for Countering Chemical, Biological, Radiological and Nuclear Threats (AJP-3.8).
11. NATO. (2021). NATO crisis response system manual (NCRS). NATO HQ.
12. Drabek, T. (2013). Human system responses to disaster. Springer.
13. Burkle, F. M. (2011). Military–civil cooperation in disaster response. Springer.

ANALYSIS OF ATTITUDES AND MOTIVATION FACTORS IN CHOOSING HIGHER MILITARY EDUCATION

Ivaylo Zh. Bozov

Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, bozovfakultet@abv.bg,

Abstract: *The personnel composition of the Armed Forces is leading in maintaining capabilities and protecting the sovereignty and territorial integrity of the country. That is why the admission of cadets to higher military schools is mainly important to fill the shortage of officers. In order to increase the results of the candidate cadet campaigns, a survey was conducted among already admitted cadets in order to analyze their preliminary attitudes when choosing a military profession.*

Keywords: *higher military school, admission, advertising campaign*

АНАЛИЗ НА НАГЛАСИТЕ И МОТИВАЦИОННИТЕ ФАКТОРИ ПРИ ИЗБОРА НА ВИСШЕ ВОЕННО ОБРАЗОВАНИЕ

Ивайло Ж. Бозов

Факултет „Артилерия, ПВО и КИС",
Национален военен университет, Шумен, България, bozovfakultet@abv.bg

Резюме: *Комплектоването на Въоръжените сили с личен състав е водещо при поддържане на способности и защитаване суверенитета и териториалната цялост на страната. Ето защо приемът на курсанти във висшите военни училища е от особена важност за попълване недостига от офицери. За повишаване резултатите на кандидаткурсантските кампании е проведена анкета сред вече приети курсанти с цел да се анализират техните предварителни нагласи при избора на военната професия.*

Ключови думи*: висше военно училище, прием, рекламна кампания.*

Увод

В контекста на динамично променящата се среда за сигурност в глобален и регионален план, въпросът за кадровото обезпечаване на Въоръжените сили на Република България придобива критично значение. Висшите военни училища са основният стълб за изграждането на бъдещия офицерски състав, който трябва да притежава не само висока тактическа подготовка, но и лидерски, технологични и управленски умения. През последните години обаче се наблюдава трайна тенденция на спад в броя на кандидатите за курсанти. Настоящият доклад има за цел да анализира нагласите и мотивационните фактори на младото поколение при избора на военната професия, и да очертае възможни решения за преодоляване на кризата в приема.

1. Мотиви за кандидатстване във висше военно училище.

Мотивацията е вътрешна или външна движеща сила, която ни кара да действаме, да постигаме цели и да променяме своето поведение. Тя определя посоката, силата и постоянството на нашите усилия.

Мотивацията за военна кариера е комплексна, като традиционните ценности - патриотизъм все по-често се съчетават с прагматични очаквания - сигурност и кариерно развитие.

Вътрешната мотивация е свързана с призвание, дълг, чест. Тук водещи са ценности като себедоказване**,** нужда от структура и ред, както и усещането за принадлежност към нещо по-голямо от отделния индивид.

Външната мотивация от своя страна е насочена към безплатно обучение и издръжка, гарантирана работа, добър социален статус. Това е мощен стимул за кандидати от по-малки населени места или семейства с по-ниски доходи.

Основните мотиви, които са движещи при избора на военна професия са:

- Сигурност - в свят на икономическа несигурност, държавната работа с гарантирано заплащане е голямо преимущество.
- Технологии - модернизацията на армията (дронове, нови оръжейни системи, киберсигурност) привлича младежи с технически интереси.
- Динамика - активния начин на живот, стрелби, тактически учения и др. са привлекателни за тези, които не желаят „офис работа".
- Естествено това не изчерпва дългия списък с мотиви, но е водещо що се касае до нагласите на потенциалните кандидати.

2. Предизвикателства пред привличането на кандидати за висше военно училище.

Привличането на кандидати за обучение във висше военно училище е процес, който има за цел не само попълването на заявения брой места за обучение по различните специализации, а създаване на конкурентна среда и привличане на най-подходящите, подготвени и мотивирани кандидати. Основните предизвикателства са свързани с:

- конкуренция от страна на гражданските университети и частния сектор (IT специалисти), които предлагат по-бърза реализация без ограничения на личната свобода.
- демографска криза и намаляващ брой потенциални кандидати
- нестабилна геополитическа обстановка в региона
- ниска начална мотивация - младото поколение отдава голямо значение на гъвкавото работно време и баланса между работа и личен живот
- психологическа бариера - страхът от „казармения" режим, строгата дисциплина и откъсването от близката среда за дълъг период от време.
- влияние на социалните медии върху имиджа на армията.

- През последните години се наблюдава сериозна флуктуация при броя на кандидатите за обучение във ВВУ.

През 2023 г. е отчетен спад от над 35% в броя на кандидатите спрямо 2022 г. (за факултета 78/27), което доведе до запълване на едва 1/4 от местата в някои направления.

Не са много по-добри и данните от приема през 2024 г.

Актуалните данни от 2025 г. сочат към ръст на кандидатите, стимулиран от финансовите възнаграждения, ранния прием и повишената рекламна активност. Въпреки това броя на явилите се кандидати е далеч от желаните стойности.

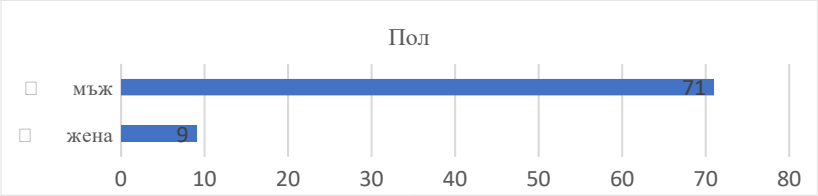
Данните свързани с приема на курсанти през 2026 е обнадеждаващ от гледна точка на броя на кандидатите спрямо обявените места, но ако се погледне цялостно ситуацията не е много по-различна тъй като:

- броя на обявените места е по-малък спрямо предходните години и напълно не покрива нуждата от офицери във Въоръжените сили;
- за не малка част от специализациите за едно място се явява един кандидат, което води до липса на конкуренция и прием на най-подходящите кандидати.

3. Анализ на проведена анкета.

Във връзка с казаното дотук е изготвена анкета с цел даване на насоки за повишаване на броя на кандидатите за обучение във ВВУ.

- Анкетирани са общо 80 курсанта от 1-ви и 2-ри курс сред които:



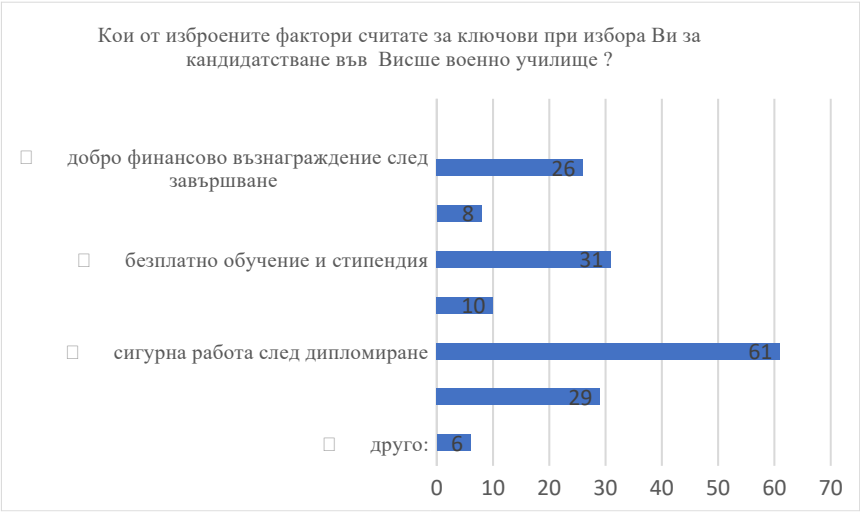
На първи въпрос резултатите показват следното:



Тук повече от 50 процента от участниците посочват, че първоначална информация/насока за кандидатстване във ВВУ са получили от близки/роднини. Това вероятно се дължи на факта, че времената на многобройната българска армия не са толкова далечни и наследниците/познати/съседи на хора служили (и служат) в нейните редици са решили да поемат по техния път.

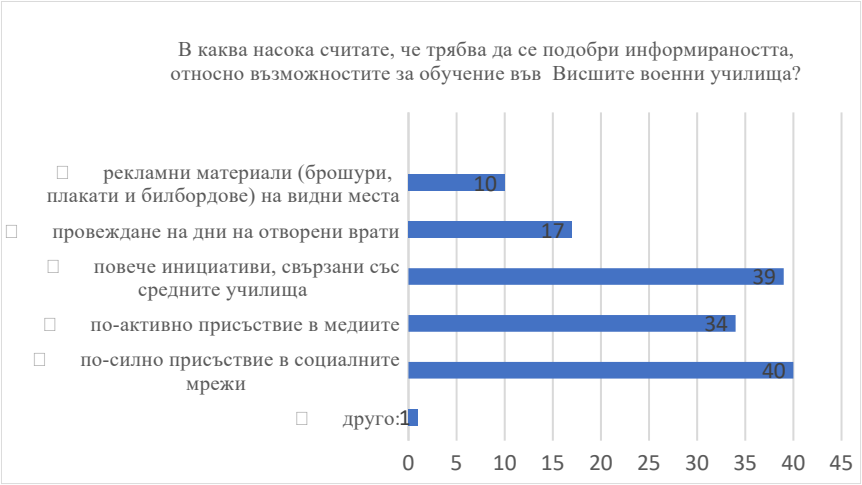
Ниският процент на информираните чрез медии, плакати, брошури и др. показва, че или така организираната рекламна кампания е слаба или не е това пътя към вниманието на потенциалните кандидати. Поради това трябва да се търсят други начини за рекламиране на военната професия.

На следващия въпрос данните показват следното:



Анализа на резултатите от този въпрос показва, че външната мотивация е водеща сред младите (1,3 и 5). Прави впечатление, че според 1/3 от тях военната професия все още се счита за престижна.

На трети въпрос, резултатите са:



Както се вижда, тук препоръките са насочени основно към по-силно присъствие в социалните мрежи и организиране на съвместни инициативи с учениците в заключителния етап на обучението си. Не е малък процента и на тези които считат, че рекламата в медиите трябва да се повиши.

На последния въпрос, отговорите са:



Тези данни са ключови в направление „Предизвикателства“, тъй като показват, че не само липсата на желание, но и високите стандарти са пречка.

Тъй като анкетата е направена сред вече приети курсанти, посочилите отговор 2 са много малко.

Високият брой отговори свързан с медицинските прегледи най-вероятно се дължи на неудобството при пътуването и настаняването при тяхното извършване.

Извън контекста на анкетата, психологическа пригодност, се оказва „препъни камък“ за приблизително 30% от кандидатите (особено последните 2-3 г.). Това подчертава разминаването между личностния профил на съвременните младежи и специфичните изисквания на военната професия.

При физическа годност резултатите показват, че около 15-20% отпадат по медицински причини или на физическите изпити. Това показва, че хронични здравословни проблеми, свързани със заседналия начин на живот на поколението Z, са сериозна пречка за не малък процент от желаещите.

4. Пътища за повишаване резултатите от рекламни кампании.

Въпреки, че използваните към настоящия момент методи, начини и средства за привличане на кандидати дават резултат, е необходимо използването на допълнителни такива, с цел повишаване на проя на кандидатите и създаване на конкуренция сред тях при приема във ВВУ. Такива може да са:

- залагане в по – голяма степен на „дигитален маркетинг“ и представяне на модерното лице на офицерската професия – като лидер и мениджър, а не само като изпълнител на заповеди.
- представяне на професията от курсанти-инфлуенсъри. Младите хора вярват на свои връстници и кратка видеопоредица в TikTok, Instagram и т.н. би показала армейския живот в друга светлина. Традиционните плакати и брошури вече не достигат до целевата аудитория.
- интегриране на VR симулатори в мобилните информационни центрове. Вместо само да получават информация под формата на заучени фрази, потенциалните кандидати трябва се „докоснат“ до военни технологии - да „управляват“ бойна машина или дрон, да „летят“ на изтребител и т.н. по време на кандидатстудентските борси.
- организиране на съвместни дейности между ученици и курсанти
- представяне на IT и инженерни специалности като „държавна кариера“ в същото направление (подчертаване на факта, че се работи със специализирана техника, до която частният сектор често няма достъп). Военната професия е тясно свързана с технологиите, което също е мотиватор за съвременните младежи.

Заключение

Анализът на процесите по привличане на кандидати за висшите военни училища показва, че проблемът с недостига на курсанти не е изолирано явление, а резултат от дълбоки структурни промени в българското общество и ценностната система на новото поколение. Традиционните методи за подбор и реклама вече не дават необходимите резултати в условията на силна конкуренция от страна на цивилния сектор. За да остане привлекателна, военната професия трябва да бъде представена в съзнанието на младежите не като система от ограничения, а като елитна платформа за технологично, кариерно и личностно развитие.

Преодоляването на тези предизвикателства изисква координирани усилия между държавата, Министерството на отбраната и академичното ръководство на военните училища, насочени към модернизация на обучението, подобряване на битовите условия и дигитализация на рекламните кампании.

Литература:

1. Заповед № ОХ-41 от 19.01.2026 г. на министъра на отбраната, относно обявяване на заявения брой места за прием на курсанти и военнослужещи във висшите военни училища (ВВУ) през учебната 2026/2027 година и графици за кандидатстване във ВВУ;
2. Заповед № ОХ-32 от 14.01.2025 г. на министъра на отбраната, относно обявяване на заявения брой места за прием на курсанти и военнослужещи във висшите военни училища (ВВУ) през учебната 2025/2026 година;
3. Заповед № ОХ-70 от 19.01.2024 г. на министъра на отбраната, относно обявяване на заявения брой места за прием на курсанти и военнослужещи във висшите военни училища (ВВУ) през учебната 2024/2025 година.

INFLUENCE OF ATGMS IN COMBAT OPERATIONS

Ivaylo Zh. Bozov

Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, bozovfakultet@abv.bg,

***Abstract**: Anti-tank guided missile systems are constantly evolving and with unmanned aerial vehicles, are a key means of destroying the armored vehicles of opposing forces. This continuous and rapid development requires a review of the tactical approaches to their use and impact in contemporary combat operations.*

***Keywords**: Tactics, ATGM, fire support*

Introduction

In the evolving landscape of warfare, some analysts have questioned the role of tanks as drones and missiles dominate the battlefield. However, the analysis reveals that while tanks are declining in importance, they remain crucial where terrain permits. Newer anti-tank guided missile (ATGM) systems offer increased mobility and protection, shifting the balance in their favor. Yet the essence of the tactic remains the same, with neglecting the basics leading to costly consequences.

1. Development of ATGM

The development of ATGMs can be divided into up to five generations (figure 1), each defined by the advancement in technology used. It is important to note that the different generations of anti-tank guided missiles cannot be strictly distinguished from each other. Rather, the differences overlap to some extent; thus, making a clear distinction is very difficult. The first generation ATGMs, introduced in the 1950s, operated on manual control principles, such as MCLOS (Manual Command to Line of Sight). Here, the operator had to manually guide the missile to the target by visual observation using a wire (one-way control) .

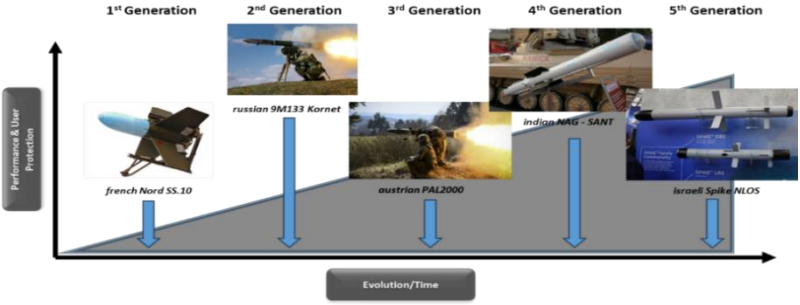


Figure 1: Generations of development of ATGMs

Second-generation ATGMs are equipped with more sophisticated guidance and targeting systems that significantly improve their performance – second-generation missiles use constant flight correction by both the operator and the system (two-way control) through SACLOS (semi-active command and control line of sight) guidance systems .

In third-generation anti-tank missiles, attention has been paid to the vulnerability of the operator by introducing the ability to fire and cover – working on the “fire and forget” principle . They use passive homing heads are used to guide the missile to the target without operator intervention. The effectiveness of these systems has been improved by the introduction of the "top-down" attack method.

In the case of the fourth generation, precise categorization is even more challenging. Some of these systems use the ability to operate in “Fire and Forget”, “Fire, Watch and Update” and “Predicted Line of Sight” modes . Line Of Sight) / are anti-tank missile systems of the 4th generation and rely on a combination of targeting markers. They use a dual configuration of the homing system with an electro-optical thermal imager and millimeter-wave active radar homing with pre-launch and post-launch lock-on capabilities. The development of these systems began in the early 21st century and are technologically advanced systems in which the soldier has the ability to change the flight parameters after launching the missile, as well as the ability to fire the missile at hidden targets, outside the line of sight. Compared to systems of older generations, it has significantly greater firing ranges and the ability to "Attack from above" than the third generation.

Fifth-generation anti-tank missile systems are the most sophisticated weapons, possessing features such as Lock-on-Fire mode . On Before Launch), Beyond Line of Sight mode (Beyond Line Of Sight), Lock -on after launch) and using a third-party target designation mode, in which the target is locked during the missile's flight using the GPS coordinates of the target that is not visible from the firing position, etc. These systems have a new generation infrared seeker, including artificial intelligence.

A notable aspect of the generational transition is that the first two generations required overcoming the technical hurdle of accuracy and effectiveness in terms of the likelihood of enemy fire. Operator protection has been improved starting with the third and subsequent generations. In general, it is obvious that as technology advances, these weapons also evolve - they become more mobile, more precise, and their range of action is constantly increasing.

2. Tactical evolution of ATGM

The last 20 years have seen limited use of tanks, as the combination of anti-tank guided missiles and armed unmanned aerial vehicles (UAVs) results in high casualties, especially when interaction with infantry is poor and artillery fire support is limited .

The saturation of the combat space with reconnaissance assets (mainly UAVs) has changed the tactics of fighting. Conducting powerful fire support from artillery, followed by the attack of armored vehicles and infantry in a narrow area is no longer so effective.

The use of battalion combat groups of 600 to 800 people is in theory highly effective and key to achieving success over the enemy. However, experience in Ukraine shows

them to be impractical due to the lack of sufficient infantry support. Combat zones defended by sufficient forces are characterized by heavy fire support from artillery and UAVs and rare close combat of mechanized and tank formations. Combat is inevitably conducted with mobile, small forces using various forms of transport, including motorcycles, buggies, pickup trucks, etc.

All of this requires a review and analysis of the use of ATGMs and their impact on combat.

The use of anti-tank guided missiles is dictated by three interrelated factors: **firepower**, **space**, and **time**. Their synergy determines tactical effectiveness on the modern battlefield.

- **Firepower** depends on what anti-tank weapons are used, the number of systems deployed in a given direction, the possibility of using a combination of several different weapons, etc.

The firepower of ATGMs goes beyond simply inflicting damage, it changes the balance of power between light infantry and heavy armored vehicles. It is characterized by:

42. High armor penetration: The use of tandem shaped charges neutralizes the dynamic protection (ERA) of modern tanks.
43. High accuracy: The guidance (laser, optical or thermal imaging head) guarantees hitting the target with the first shot.
44. Top - attack: Systems like Javelin attack the thinnest armor of a tank or ABM – namely the turret.
45. Psychological effect: The presence and use of ATGMs deprives opposing forces of the large-scale use of armored vehicles and slows down their pace.

- **Space -** the spatial factor encompasses the geometry of the battlefield, the terrain, and the distance of the collision.

46. Distance control: ATGMs expand the defense security zone by being able to be deployed in the first or second echelon, allowing for the engagement of targets from 2 to 5 kilometers and beyond (before the tank reaches effective firing range).
47. Tactical Camouflage: Squads require minimal cover, allowing them to perform missions from urban environments, forests, or trenches.
48. Terrain limitations: Terrain has a significant impact on the deployment and use of PTS, dense vegetation or hilly terrain can block line of sight (LOS). This necessitates the use of "fire and forget" systems or missiles with NLOS (non-line of sight) capabilities.
49. Dispersion of forces: The long range allows for the execution of tasks from several separate positions, thus concentrating fire on one key point (ambush zone).

- **Time** – in context, it is related to the speed of response, flight duration and survivability dynamics of the estimate. Regarding time, two main factors significantly contribute to the success or failure of military operations. First, the time required to deploy a capability (assets and personnel) to a sufficient extent in a given direction. Second, the time required to reach a sufficient condition for the inclusion of the PTS in combat. It is characterized by:

50. Reaction and deployment time: Modern light ATGMs are brought into combat readiness in seconds, which is extremely important in the event of a sudden enemy appearance.

51. Flight time (Time of flight): At maximum range, the missile flies for between 10 and 20 seconds. In semi-automatic guidance systems (SACLOS), the operator must remain stationary during this time, which puts him at risk.

52. "Fire and forget" principle: Reduces the time of vulnerability of the calculation. Immediately after the launch, the operators can change their position.

53. Battle Dynamics: The massive use of ATGMs slows the advance of opposing forces, buying valuable time for friendly troops to regroup or deliver artillery strikes.

Analysis of the factors shows that the defending troops successfully resist the concentrated use of tanks and ABMs by using long-range anti-tank guided missiles, as this allows the deployment of the systems further back in the battle formation (for protection purposes) and hitting targets at a greater distance (5 km and more). On the other hand, observations of combat operations reveal that not always even a direct hit on the target by an ATGM leads to the destruction of tanks, but rather a limitation of mobility (stopping the movement of the machine) is achieved. This is due not so much to the low armor penetration of the missile, but rather to a number of improvements to the machines themselves, such as: minimizing thermal emissions through camouflage materials, installing additional grilles, nets and other materials to increase their protection.

However, one should not ignore the fact that a large number of relatively old battle tank systems are still used in various conflicts, facing off against the most modern anti-armor systems.

Another feature that everyone must take into account is the terrain. Flat terrain with many open spaces allows the full use of the mobility and long-range capabilities of ATGMs. While rugged terrain with many invisible spaces, especially during an offensive, makes them not very effective, and in these cases the combat distances are even limited to about 1000 meters or less.

Is the importance of tanks decreasing ?

In the ever-evolving nature of warfare, analysts sometimes perceive the tank as having diminished importance. But is that really the case? While drones – strike UAVs or barrage munitions, ATGMs and other anti-tank weapons will continue to support combat operations, the combination of different means remains particularly important to achieve decisive results. The desired end states are usually achieved through the combined use of different types of weapons to impose their will on the enemy and achieve military victory within the framework of the set objectives.

The decision to use tanks must be based on two considerations. First, the balance between maneuverability and protection must be considered. Tanks are mobile elements for deep penetration, but currently require comprehensive protection. Second, the possibility of advancing tanks as leading elements of combat operations must be considered. The trade-off between losses and security must be assessed. However, this

cannot be expected with the use of relatively light armored personnel carriers such as armored personnel carriers or even HMMWVs.

At the moment, especially considering the experience of the battlefields in Ukraine, there is no significant movement in combat operations, mainly due to the time-consuming and resource-intensive process of mastering terrain sections. The attacking side must have sufficient infantry forces, which is essential. In addition, the use of tanks (in conjunction with other elements) remains tactically advantageous where the terrain allows and is not replaced only by combat or pure drone swarms . The protection and survivability of tank crews and progress in active tank protection measures are the decisive factors in this regard.

Conclusion

In summary, it can be noted that the tactical principles regarding the use of ATGMs are generally valid, but adjustment is needed in certain areas. The mobile offensive use of ATGMs represents a significant change in combat tactics, especially in terms of space and time. Furthermore, the combat range of advanced anti-tank systems is often severely limited by terrain, which highlights the continuing importance of terrain assessment. In general, the tactical principles of anti-tank missiles are still valid today, especially in defensive scenarios where they can quickly establish significant firepower. Even in larger areas, armored vehicles can be repelled due to the mobility and long range that ATGMs provide.

For more modern ATGM systems (third generation and above), new deployment opportunities arise, although the defensive nature of these weapon systems is indisputable. Their mobility and operator protection are already provided to a sufficiently high degree, which significantly increases the advantages of using anti-tank missiles.

References

1. Petrov V., „History of the development of anti-tank guided missiles “, International Scientific Conference “Defense Technologies” DefTech 2025, Shumen, 2025, стр. 63-74, ISSN 2815-4282;
2. Radovanović M., Petrovski A., Smileski S., Jokić Ž., “Analysis of the development of five generation of Anti-armor missile systems”, Scientific Technical Review, 2023, Vol.73, No.1, pp. 26-37, doi: 10.5937/str2301026R;
3. https://tdhj.org/blog/post/atgms-ukraine-war/
4. https://www.army-technology.com/features/featurethe-worlds-deadliest-anti-tank-missiles-4159253/

EVOLUTION OF TECHNOLOGIES USED BY INTERCEPTOR DRONES

Ivaylo Zh. Bozov

Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, bozovfakultet@abv.bg,

***Abstract**: In 21st century, the use of unmanned aerial vehicles (UAVs), also called drones, has increased dramatically. Technological advances trigger the production of many different models in shape and purpose. All this has led to the search effective ways for counteraction to UAVs. In the last two years, the use of interceptor drones has proven to be particularly suitable for fight with UAVs.*

***Keywords**: UAVs, interceptor drones, AI*

Introduction

Interception drone technologies underwent a profound breakthrough, evolving from experimental prototypes tested in limited conditions into a mass-produced, industrialized system for asymmetric defense, especially on the battlefields of Ukraine. Massive attacks involving Shahed-136, Shahed-238 (Geran-2/3) and other munitions forced the Ukrainian defense industry and volunteers to quickly move towards large-scale, low-cost but highly effective solutions. While unmanned aerial vehicles (UAVs) used for interceptors were rare at the beginning of 2025, by the end of the year and early 2026, interceptor production reached 950–1,500 units per day (Ministry of Defense of Ukraine and UNITED24).

Drones are specialized unmanned aerial vehicles (UAVs) designed to detect, track, and physically or electronically neutralize enemy drones in the air. They have become a key and cost-effective component of modern air defense (AD), replacing expensive anti-aircraft missiles in combat with cheaper reconnaissance and kamikaze drones .

These drones are integrated with radar, acoustic sensors, and artificial intelligence, achieving 60–80% effectiveness in real combat conditions. This allows for the protection of energy infrastructure, cities, and frontline positions, thus saving expensive Patriot , NASAMS or IRIS-T missiles that cost hundreds of thousands of dollars per launch.

This evolution demonstrates how war is transforming into a technological conflict, where economic efficiency and the speed of innovation overcome numerical superiority. In the beginning it starts with simple modifications of the standard first person view (FPV) drones to intercept enemy reconnaissance UAVs, but by the first half of 2025, the focus in Ukraine is shifting to countering Shahed 's massive strikes . But this evolution is not just technical - it is changing the perception of AD when it comes to unmanned aerial vehicles, including a shift from expensive missiles to cheap UAV models, allowing the defense to withstand daily massive attacks with minimal resource expenditure.

All of this is not just countermeasures - it is a new paradigm of air warfare, where drones hunt drones , and economic efficiency becomes a decisive factor for victory.

1. Technical solutions in using interceptor drones

Increasing the effectiveness of using drones to intercept and destroy other UAVs is associated with the use of a number of technical solutions. Some of them are:

1.1 Radar integration

The integration of interceptors with radar systems is becoming a major component of modern air defense systems, especially in countering mass nighttime attacks by Shahed /Geran-type munitions and other low-altitude threats. Radars provide long-range early detection, transmitting precise coordinates in real time to command and control (C2) systems. This allows for automated or semi-automated launch of FPV interceptors and other countermeasures. Without this integration, the effectiveness of interceptor drones is significantly reduced, as it is extremely difficult for operators to locate targets at long ranges in darkness or fog.

A key addition in 2026 is Spain's Lanza Radar LTR-25 by Indra Sistemas . This mobile, 3D L-band radar is designed for early detection of aerial threats, including UAVs, cruise missiles and aircraft. With a range of over 450–460 km, it is suitable for monitoring large areas. The radar is compatible with NATO systems, allowing for seamless data transmission to the DELTA situational awareness system and coordination with air defense systems.

The French Ground The Master 200 (GM200) is a medium-range radar capable of detecting low-flying drones , missiles, and rocket/artillery fire. It establishes and maintains stable target tracks quickly. The GM200 is often paired with the ControlMaster 200 (CM200) - a package that includes radio communications, a control center, and portable target assignment terminals - creating comprehensive local air defense zones where the radar identifies the threat and the interceptors neutralize it.

1.2 Next generation interceptors

The French X- Wing system (Alta Ares) represents the pinnacle of this integration. The X- Wing combines radar data with AI-controlled terminal guidance (30 km range), increasing accuracy by 35% over manual control. It is EW resistant, utilizing autonomous attack control in the final phase.

Another option for drone interceptors are the DroneHunter mobile systems . VARTA, which are also synchronized with radars. VARTA is a module with specialized anti-drone munitions mounted on FPV drones . It integrates with on-board radar or acoustic sensors for automated targeting.

A prime example of an interceptor is Bumblebee , a quadcopter developed by the Swift Beat project . According to The New York Times (December 2025 – January 2026) Bumblebee achieves over 70% accuracy in autonomous control after lock-on. It uses AI to recognize infantry, fortifications, vehicles, and other UAVs, specifically targeting Shahed intercepts . In the final phase, the drone ignores jamming and completes the strike autonomously.

Another, no less famous drone interceptor is Wild 's Sting . Hornets . It is a 17-inch quadcopter that reaches speeds of 315 km/h (195 mph) and altitudes of 11 km, and is equipped with artificial intelligence modules from The Fourth Law and Odd Systems, allowing autonomous targeting of the device after manual lock. Using artificial

intelligence , Sting tracks the thermal signal and maintains the target in its field of view, even if the operator loses data connection.

1.3 Implementation of artificial intelligence

AI-powered UAV detection transforms drone interception into a truly autonomous process. Once a “lock” is achieved, the drone pursues and attacks the target independently, completely ignoring enemy electronic countermeasures efforts. This represents a key breakthrough, as traditional radio-controlled drones Drone interceptors often lose their signal due to massive jamming by electronic warfare systems. Today's artificial intelligence algorithms analyze thermal signals (infrared radiation from the Shahed 's engines), flight paths, speed and maneuvers, adapting in real time to any changing actions. The interceptor can now predict course changes, adjust its own flight path and perform maneuvers without constant operator intervention.

1.4 Control via optical fibers

UAV interceptors, communicating with the operator via optical fibers, combine perfectly with artificial intelligence: the conductor provides a stable HD video feed and command link, immune to radio interference, while the autonomous module finalizes the attack. The operator confirms the target only in the initial phase, and the drone does the rest.

2. Advantages of interceptor drones

Intercepting UAVs using interceptor drones has several key advantages. These systems are becoming the most effective and cost-effective tools for modern air defense in the context of asymmetric warfare against mass attacks by so-called stray munitions or kamikaze drones .

2.1. Economically efficient

The most significant advantage is the radical optimization of resources. A drone interceptor (Sting , Bullet , Bumblebee , etc.) costs between $1,000 and $5,000 (including warhead, thermal imager and AI module). In contrast, the Shahed-136/238 costs approximately $80,000 – $150,000 per unit. This creates a cost ratio of 1:50 to 1:150, and in some cases even more.

2.2. Mass production

The last two years have seen an industrial scale in the production of interceptors. According to the Ministry of Defense and UNITED24, daily production in Ukraine alone has reached 950–1,500 interceptors by 2025. This has been achieved through a decentralized model involving dozens of volunteer and commercial entities, localized production of components (frames, engines, electronics), and fast production cycles. This scalability allows for rapid saturation of the front line and rear areas, creating a “Wall against drones ” to protect energy infrastructure and cities.

2.3. Resistance to electronic warfare means

Traditional UAVs are vulnerable to electronic warfare. However, optical interceptors completely ignore jamming as the signal travels over a physical cable (up to 20–50 km), providing stable HD video and command links. In addition, AI guidance modules (Bumblebee , Sting , TFL Last Mile) provide terminal autonomy: once a “lock” is achieved, the drone completes the attack, even if the data connection is lost.

2.4. Synchronization of different tools in one system

The interceptors operate within a synchronized system together with radars (Lanza LTR-25, GM200), acoustic sensors (Sky Fortress , Zvook) and mobile strike groups. The sequence of steps - early detection (15–30 km) - data processing - interceptor launch - physical neutralization, significantly reduces the use of high-end systems such as Patriot, NASAMS and IRIS-T, reserving them mainly for ballistic or cruise missile threats.

2.5. Controlling a swarm of UAVs using artificial intelligence

Modern algorithms (Drone Wall , Swift Beat , The Fourth Law) allow a single operator to control dozens or even hundreds of drones simultaneously. Artificial intelligence performs target allocation, flight coordination, and collision avoidance. This is crucial during intense night attacks, when traditional air defense systems can be overwhelmed.

3. Challenges and limitations in using interceptor drones

Drone interception technologies face several critical challenges and limitations. These factors prevent them from fully replacing traditional air defense systems and require continuous improvement.

3.1. Limited flight range

Most FPV interceptors (Sting , Bullet , Bumblebee) have an effective range of 10–25 km (rarely up to 30–40 km in fiber optic versions). Therefore, the interceptor can only operate within the near radar or acoustic sensor detection zone, not over large perimeter strips. Protecting large areas requires multiple early detection and launch points, which complicates logistics and requires a dense sensor network.

3.2. Meteorological dependence

Strong winds (over 10–12 m/s), rain, fog, snow or thunderstorms significantly degrade the effectiveness of an interceptor UAV. Quadcopters lose stability, optics fog up, thermal images lose clarity in heavy rain, and optical cables can become tangled in strong gusts. Observations from their use in autumn-winter attacks in Ukraine show that the effectiveness of interceptors has dropped by 30–50% in adverse weather, forcing the use of expensive air defense systems.

3.3. Requirement for early detection.

Without accurate early warning, the interceptor cannot launch and overtake the target in time. For example, Shahed flies at a speed of 150–200 km/h, leaving only 5–10 minutes of reaction time. If a sensor detects a target only 5–10 km away, the drone will not have the opportunity to intercept the target. Therefore, it is necessary for the UAV to be detected at a distance of at least 15–30 km. This disadvantage is partly overcome by the deployment of multiple acoustic sensors (Sky Fortress , Zvook) and advanced radars (Lanza LTR-25, GM200) to provide depth of detection.

3.4. Vulnerability to jamming and optical limitations.

Standard radio-controlled interceptors are easily jammed by electronic warfare. Optical models, on the other hand, ignore jamming entirely, but introduce new disadvantages: the added weight reduces maneuverability, the range is physically limited by the cable, and the line can break during sharp maneuvers or get tangled in obstacles.

By early 2026, optical models will account for only 20-30% of production, leaving radio models dominant but vulnerable.

3.5. Continuous development of UAVs.

The continuous development of technologies also directly affects the production of UAVs. The addition of radio interference devices, the equipping of aircraft with jet engines (Geran – 4 and 5), the use of decoys and changing the flight altitude are just some of the constant innovations in the production of drones . This requires manufacturers to work in a constant cycle of upgrading, which leads to an increase in research and development costs.

Conclusion

The use of interceptor drones to combat other aircraft is an innovation that has developed particularly rapidly in the last two years. Despite their shortcomings, these means are successfully used to combat kamikaze drones and other UAVs moving at relatively low speeds, thus becoming an integral part of the overall air defense system.

References

1. Джунов. Т., „Ролята на дроновете във войната в украйна и поуките за съвременната военна стратегия", International Scientific Conference ―Defense Technologies DefTech 2025, Шумен, стр. 117-121, ISSN 2815-4282;
2. Димитров. Д., „Електронни методи за противодействие на безпилотни летателни системи", International Scientific Conference ―Defense Technologies DefTech 2025, Шумен, стр. 608-615, ISSN 2815-4282;
3. Bendett, S., Nersisyan, L. „The drone war over Ukraine, The Air War in Ukraine: The First Year of Conflict", Cass Military Studies, 2025;
4. Molloy, O., „Drones in Modern Warfare: Lessons Learnt from the War in Ukraine", Australian Army Occasional Paper No. 29, Commonwealth of Australia, 2024. DOI: https://doi.org/10.61451/267513;
5. Беджева М., „Методика за оценка качеството на работа на оборудването на БЛА за фотограметрични цели", Годишник на ШУ „Еп. К. Преславски", том X E, Факултет по технически науки, Университетско издателство „Еп. К. Преславски", 2020, стр. 104-113, ISSN 1311-834X
6. https://tdhj.org/blog/post/atgms-ukraine-war/
7. https://www.army-technology.com/features/featurethe-worlds-deadliest-anti-tank-missiles-4159253/

OPPORTUNITIES FOR THE USE OF ATGM IN OPERATIONS

Ivaylo Zh. Bozov

Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, bozovfakultet@abv.bg,

Abstract: *The development and continuous improvement of ATGM capabilities has led to an increase in their use in various ways and means. In most of them, especially in the new generations, there is an increasing integration of complex systems with increased autonomy and widespread use of artificial intelligence. Therefore, it is necessary to review the existing capabilities of these weapons for fight with armored vehicles.*

Keywords: *tactics, anti-tank guided missile systems, ATGM generations*

СЪВРЕМЕННИ ВЪЗМОЖНОСТИ НА ПТУРК ПРИ ИЗПОЛЗВАНЕТО ИМ В ОПЕРАЦИИТЕ

Ивайло Ж. Бозов

Факултет „Артилерия, ПВО и КИС",
Национален военен университет, Шумен, България, bozovfakultet@abv.bg,

Резюме: *Развитието и непрекъснатото повишаване на възможностите на ПТУРК, доведе до повишаване на тяхното използване по различни начини и способи. При голяма част от тях, особено при новите поколения, се наблюдава нарастващо интегриране на сложни системи с повишаване на автономността и широко използване на изкуствен интелект. Ето защо е необходимо на се направи преглед на съществуващите възможности на тези оръжия за борба с бронирани средства.*

Ключови думи*: тактика, противотанкови управляеми ракетни комплекси, поколения ПТУРК.*

Увод

От въвеждането им през 50-те и 60-те години на миналия век противотанковите управляеми ракети (ПТУР) са еволюирали от чисто противотанкови активи в универсални оръжия, способни да ангажират широк спектър от цели, включително бронирани бойни машини, укрепления и др. Днес ПТУР са изградени като комплекси, които са в експлоатация в множество страни по света, като непрекъснато се разработват и произвеждат по-нови поколения от тях.

Важно е да се подчертае, че първоначалните очаквания, които предложиха различни видове безпилотни летателни апарати (БЛА) да заменят или поемат функциите на ПТУРК на бойното поле, изглеждат преувеличени. Опитът от продължаващите конфликти в Украйна и в Близкия изток показва, че тези видове оръжия успешно съществуват съвместно и се допълват, въпреки донякъде припокриващите се способности.

1. Съществуващи възможности на ПТУРК

Системите, които в момента се използват в различни страни по света, се различават значително по възраст и поколение. Докато някои страни все още използват системи от първо поколение, като например съветската епоха 9M14 Maliutka или нейните модернизирани производни, други вече са приели така наречените системи от пето поколение, като Akeron на MBDA и Spike LR2 и Spike NLOS на Rafael. Въпреки това, гръбнакът на оръжията ПТУР в повечето страни се състои от преносими и монтирани на превозни средства системи от второто и третото поколение.

Разграниченията на поколенията не винаги са конкретни и ясно разграничими. Възможностите могат да се различават значително в системите от едно и също поколение при по-ранни и по-нови версии на ракети в рамките на едно и също семейство. Например, руската Kornet ATGM се счита от някои за система от трето поколение, въпреки че включва полуавтоматично командване към системата за насочване на видимост (SACLOS), по-типична за ПТУРК от второ поколение. От друга страна, ракетата 9M133M-2 на Kornet има обсег от 8 км и мощна тандемна бойна глава, способна да преодолее 1300 mm хомогенна броня. Освен това, станцията за изстрелване е снабдена с термичен визьор за насочването през нощта. Такива характеристики са по-често свързани със системи от трето поколение.

Примери за системи от второ поколение са 9K115 Metis, 9K111 Fagot, 9K111-1 Konkurs, 9K133 Kornet семейство, семейство Skif (Stugna-P), семейството BGM-71 TOW, семейство MILAN и други. Въпреки че някои от тези системи са въведени през 70-те и 80-те години на миналия век, те остават на въоръжение и непрекъснато са модернизирани, за да удължат експлоатационния си живот и да подобрят бойните си способности. Един от последните случаи на такова подобрение е руската система 9K111-1M Konkurs-M, която има възможност за дистанционно управление. Тази функция е предназначена да увеличи преживяемостта както на системата, така и на нейния екипаж, а единната система за дистанционно управление позволява на оператор на ПТУРК да управлява дистанционно три установки Konkurs-M при добра видимост.

Трябва да се отбележи, че ПТУРК от второ поколение са произведени и масово въведени предимно втората половина на XX-ти век. Днес тези системи остават най-многобройни (с голям запас) и са рентабилни за производство, като същевременно притежават достатъчна бойна ефективност. За сравнение, трето поколение включва редица усъвършенствани способности, което, от една страна, подобрява бойното им ефективност, но от друга увеличава сложността, както и разходите за поддръжка и производство. Представители на това поколение включват системи като FGM-148 Javelin, AT-1K Raybolt, Hongjian-12 (HJ-12) "Red arrow" и други. Повечето системи от трето поколение от среден клас са способни да атакуват цели в обсег от няколкостотин метра до над 5 км.

Системите, класифицирани като трето поколение, обикновено влизат в експлоатация между 1990 и 2010 г. Те са в състояние да съвместят няколко общи функции, като например заключване преди изстрел (Lock-On Before Launch - LOBL), както и да позволят на оператора да избира между директни и полегати

(атака отгоре) траектории. Тези ракети обикновено са оборудвани с търсач на инфрачервени изображения (IR) за насочване в ограничена видимост.

LOBL, който също обикновено се нарича режим „стреляй и забрави", е може би най-важното развитие, въведено в системите от трето поколение. В сравнение с ръчното командване от първо поколение (MCLOS) или системите SACLOS от второ поколение, където операторът трябва да държи целта в полезрението си до удара, режим „стреляй и забрави" позволява на екипажа бързо да промени позицията си след изстрелването, увеличавайки преживяемостта и тактическата гъвкавост на екипажите на бойното поле.

Крайната отличителна черта на противотанкови ракети от трето поколение е способността им за атака отгоре. Възниквайки като решение за противодействие на напредъка в защитата на основните бойни танкове, тази възможност се е превърнала в стандартен елемент в трето поколение и по-нови ПТУР. Този тип атака позволява на ракетата да се насочи към по-слабата броня на купола на силно бронирана цел като танк, като по този начин заобикаля по-голямата част от пасивната му защита.

Докато възможностите за атака отгоре, както и режим „стреляй и забрави" се разглеждат като важни, е трудно да се оцени цялостното им представяне срещу съвременни бронирани машини, както и цялостното им въздействие при провеждането на операции.

В таблица 1 са представени някои от характеристиките на модели от трето поколение.

Таблица 1. Сравнение на характеристиките на някои модели ПТУРК трето поколение

Система	**FGM-148 Javelin**	**Spike-MR**	**HJ-12 (Red Arrow)**	**Akeron MP**
Държава	САЩ	Израел	Китай	Франция
Макс. обсег	4000 м	5500 м	4000 м	5000 м
Основен режим	Стреляй и забрави	Стреляй и забрави	Стреляй и забрави	Стреляй и забрави / Корекция
Профил на полет	Отгоре / Директен	Отгоре / Директен /	Отгоре / Директен	Отгоре / Директен / LOAL
Бронепробиваемост	800 мм	>900 мм	1100 мм	>1000 мм

Междувременно не са малко страните, разработили и приели ПТУРК от четвърто и пето поколение - в зависимост от използваната класификация - като Akeron MP (има основните характеристики на трето поколение) и системите Spike LR/LR2, Spike ER/ER2 и Spike NLOS. Тези ATGM като цяло започнаха да влизат в експлоатация след 2010 г. и разполагат с по-усъвършенствани режими, като например възможност за заключване след стартиране (Lock-On After Launch - LOAL), наричана още „огън и котекция". Режимът LOAL позволява на оператора да наблюдава бойното поле в реално време чрез инфрачервен и/или дневен тракер

на ракетата и да актуализира параметрите на целта или ракетния полет, ако е необходимо. Този режим позволява да се осъществят пускове „отвъд-линия на видимост“ (NLOS).

Илюстративен пример за такава система е OMTAS на турската компания Roketsan, която включва както режими LOBL, така и LOAL. Установката и ракетата OMTAS са в постоянна връзка, което позволява на оператора да заключи цел, след като ракетата е в полет, както и да превключва цели по време на полет.

По-специално, някои класификации определят системите от четвърто поколение като подобни на тези от трето поколение, като основното разграничение е връзката за данни между пусковия блок и ракетата, което позволява на оператора да промени параметрите на полета, да промени целта или да прекрати мисията, ако е необходимо.

Най-модерните ПТУР до момента принадлежат към петото поколение. Тези системи разполагат със сложни възможности, което позволява тяхното внедряване в съвременната война. Обикновено са много гъвкави, предлагайки мултиплатформена интеграция и многофункционални тандемно-топлинни бойни глави с фрагментационни модули, способни да преодолеят експлозивната реактивна броня и да пробият хомогенна броня с дебелина над 1,000 мм.

ПТУР от пето поколение обикновено разполагат с разширена гама от оперативни (стрелкови) режими, включително режими LOBL, LOAL и „стрелба по координати“. Последният режим позволява стрелба по предварително определени координати, като е най-подходящ за неподвижни цели или изстрелване по приблизителни икоординати и след засичане на конкретна цел, промяна на мястото на удара. Някои системи, като например Akeron и Spike, позволяват задаване на цели от трети източник на информация. Тази способност означава, че данните за насочване могат да бъдат получени от пилотирани или безпилотни летателни или наземни разузнавателни средства.

В таблица 2 са показани някои от характеристиките на ПТУРК от четвърто и пето поколение.

Таблица 2. Сравнение на характеристиките на някои модели ПТУРК четвърто и пето поколение

Система	Type 01 LMAT (Япония)	Spike LR2 (Израел)	OMTAS (Турция)	Akeron MP (Франция)
Поколение	4-то поколение	5-то поколение	4-то поколение	5-то поколение
Максимален обсег	4000 м	5500 м	4000 м	5000 м
Глава за самонасочване	Инфрачервена (IR)	Двурежимна: IR + HD дневна камера	Инфрачервена (IR)	Двурежимна: IR + Цветна ТВ камера
Канал за данни	Няма	Оптично влакно + Радиоканал (RF)	Радиоканал (RF)	Оптично влакно
Режим зад линията на видимост (NLOS)	Не	Да (чрез ИИ, GPS или външно насочване)	Да	Да (интеграция с дронове и C4I)
Пренасочване в полет (LOAL)	Не	Да	Да	Да
Основен тип бойна част	Тандемна кумулативна (HEAT)	Тандемна HEAT / Многоцелева	Тандемна кумулативна	Тандемна многоцелева (програмируема)
Бронепробиваемост (след ERA)	700-800 мм	900 – 1000 мм	1000 мм	1000 мм

Едни от последните подобрения при Spike NLOS са: - режим на залп, при който до четири ракети могат да бъдат едновременно изстреляни и контролирани, докато са във въздуха от една установка.; вторият е способност за пренасочване на управлението, при която контролът върху ракетата може да бъде прехвърлен от една платформа на друга. Това дава възможност една платформа за изстрелване бързо да се премести или да се скрие след пуска, докато втора платформа поема управлението, за да гарантира, че целта е успешно поразена.

2. Тенденции в развитието на ПТУРК

В настоящият момент могат да бъдат идентифицирани няколко тенденции в бъдещото развитие на ПТУРК. Първата е увеличаване обхвата на действие поради две причини: изместване на тези комплекси по-назад в бойния ред, с цел по-голяма безопасност и поразяване на цели на по-голяма дълбочина в противниково разположение. Втората причина е особено ценна за системите използващи режими „отвъд линията на наблюдение“ и „стрелба по координати“. Докато по-голямата част от ПТУР, които в момента са в експлоатация, имат максимален обхват около 5 км, изискванията за бъдещите системи сочат увеличаване на разстоянието за поразяване на цели. Бойните действия в Украйна показват че, противотанковите ракети - както преносими, така и монтирани на превозни средства - с максимален обхват от 4-5 км, разположени близо до линията на съприкосновение с противника, стават лесна мишена за различни разузнавателни средства и поразявани от артилерия или други налични огневи средства много преди да са в състояние да влязат в контакт с противниковите бронирани машини. Разстоянието на ефективен

огън до 5 км, съчетано с режима „стреляй и забрави", някога разбирано като достатъчни мерки за зашита на ПТУРК, сега изглежда неефективно.

Втората тенденция се дължи на развитието и използването на защитата на брониранитe бойни машини. В отговор на разпространението на противотанкови средства, включително усъвършенствани ракети и боеприпаси, въоръжените сили по целия свят ускориха темпото на прилагане на усъвършенствани защитни решения както за бронирани, така и за лекобронирани превозни средства. Следователно способността да се унищожат бронирани превозни средства, оборудвани с усъвършенствани многослойни защитни пакети, сега става задължителна.

Друга тенденция е нарастващата гъвкавост на ПТУРК. Докато през 80-те и 90-те години на миналия век, този клас въоръжение се разглежда като основно оръжие за поразяване на противникови танкове, днес спектърът от бойни задачи, изпълнявани от тези ракети, е значително по-широк. Необходимостта от адаптиране за различни бойни сценарии доведе до непрекъснато подобряване и имплементиране на нови функции, които увеличиха тяхната гъвкавост. Илюстративен пример е въвеждането на така наречената функция „меко изстрелване", която позволява на ПТУР да се използват в затворени пространства по време на градска война, както и използването на бездимни горива, допринасяйки за по-добро прикритие на демаскиращите фактори. Друга посока е разработването на многофункционални ракети (с избираеми или модулни конфигурации) или боеприпаси, предлагани с термобарична или високоексплозивна фрагментация, или тандемно-топлинни бойни глави, позволяващи изпълнението на задачи срещу широк спектър от цели.

И накрая, съществуват текущи развития в способностите, които предстои да бъдат въведени в следващото поколение ПТУРК или чрез надстройки на съществуващите системи. Например, MBDA представи наземния Warden AI – система, задвижвана от изкуствен интелект, предназначена да подобри придобиването на цели и процеса на вземане на решения за семейството оръжия на Akeron MP. Други производители, включително Rafael Advanced Defense Systems, Lockheed Martin и други, също работят върху разработването и внедряването на AI и технологии за машинно обучение в ракети.

Заключение

Днес ПТУРК остават основно прецизно насочено оръжие на тактическо ниво, използвано срещу различни цели като бронирани и лекобронирани превозни средства, плавателни съдове, самолети и вертолети, полеви укрепления, сгради и пехота - независимо дали са укрити или открито разположени. Благодарение на евтините технологии и огромните запаси от епохата на Студената война, ПТУР от второ поколение вероятно ще останат в експлоатация и производство в някои страни, допълвайки по-напредналите противотанкови ракети и баражиращите боеприпаси.

В резултат на това въоръжението с ПТУРК на много страни ще се състои от комбинация от технически по-прости и по-евтини, така и усъвършенствани ракети

с подобрени възможности. Макар и да има някои недостатъци, тази конфигурация предлага няколко предимства. Например ракетите от второ поколение са по-достъпни, по-евтини и има възможност за пълноценно обучение на личния състав, включително и с бойни стрелби.

Най-новите поколения ще продължат да се развиват, но ще бъдат произведени и въведени в експлоатация в ограничен брой. Най-значимите фактори, допринасящи за това ограничение, са техните сложни дизайни, по-високи производствени разходи и по-дълги производствени цикли.

Литература

1. Атанасов А., „Надграждат ли дроновете с оптично влакно противотанковите ракетни комплекси четвърто поколение“, International Scientific Conference ―Defense Technologies DefTech 2025, Шумен, стр. 421-429, ISSN 2815-4282;
2. Пенчев Р., „Поддръжка на бронетанковата и автомобилната техника в мирно време“, глава 6, учебник, 2009, София;
3. https://euro-sd.com/2025/03/articles/42885/modern-atgm-capabilities/

LAYERED AIR-DEFENCE SYSTEM: SYNTHESIS, OPERATIONAL ANALYSIS AND MATHEMATICAL MODELING

Stoyan N. Chanev, Matei K. Kirov, Stanimir H. Parvanov

Department of Air Defense, Artillery, Air Defense and CIS Faculty at the Vasil Levski National Military University, Shumen, Bulgaria,
st.chanev@gmail.com, mkkirov@nvu.bg, shparvanov@aadcf.nvu.bg

Abstract: *This paper develops a transparent, scenario-based mathematical model for a layered air-defence architecture combining close-in counter-UAS effects, short-range, medium-range and long-range engagement layers. The resulting model combines conditional interception probability, queueing loss, discrete resource allocation, engagement-time constraints and a parametric electronic-warfare sensitivity analysis. All numerical coefficients are illustrative and are not performance data for named operational weapon systems.*

Keywords: *layered air defence, integrated air and missile defence, saturation, Erlang-B, queueing theory, engagement capacity, directed energy, electronic warfare, mathematical modeling*

Introduction

NATO's 2025 Integrated Air and Missile Defence (IAMD) Policy states that active air and missile defence should combine systems and technologies operating at different ranges and altitudes to create layered defence against threats ranging from small unmanned aircraft to cruise, ballistic and hypersonic missiles [1]. NATO also emphasizes integration among sensors, command-and-control structures and weapons systems, together with resilience, redundancy and the ability to adapt to salvo attacks and degraded electromagnetic conditions [1, 2].

Recent operational analysis of mass one-way-attack drones has likewise highlighted saturation and cost-exchange problems: large numbers of inexpensive threats can impose a disproportionate burden on limited interceptor inventories and engagement channels, which strengthens the case for layered and cost-diverse defensive architectures [3]. Directed-energy systems can complement kinetic interceptors in some counter-UAS roles, but their performance remains constrained by range, atmospheric conditions, cooling and power requirements [5]. These observations motivate a model that separates technical single-engagement effectiveness from finite engagement capacity.

The purpose of this paper is therefore not to predict the performance of a particular fielded system, but to provide a reproducible analytical framework for sensitivity analysis, simulation exercises and force-structure studies. The numerical parameters below are deliberately illustrative. The model is intended to show how layer effectiveness, saturation, reaction time and resource allocation interact, while making the assumptions explicit and mathematically checkable.

1 Layered Architecture and Modeling Assumptions

1.1 Functional layering

A useful abstraction is a sequence of defensive opportunities connected through a common surveillance and command-and-control architecture. The ranges in Table 1 are generic scenario bands rather than verified envelopes of named weapon systems. Similarly, the channel counts, service rates and technical interception probabilities are modelling coefficients chosen to demonstrate the method. This distinction is essential because real IAMD performance depends on threat type, geometry, sensor coverage, interceptor inventory, rules of engagement, environmental conditions and system-specific tactics [1, 2].

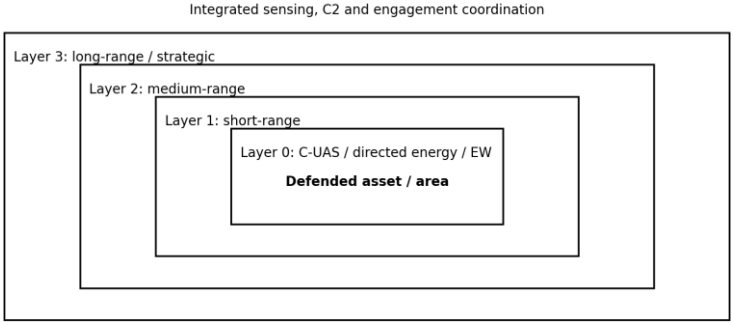


Figure 1: Conceptual four-layer defensive architecture connected by integrated sensing and command and control.

Table 1: Illustrative parameters used in the four-layer model.

Layer	Functional role	Scenario range (km)	C_i	μ_i (s^{-1})	P_i
Layer 0	Directed-energy / EW C-UAS	0–2	8	2.0	0.92
Layer 1	Short range (SHORAD)	2–15	12	1.2	0.85
Layer 2	Medium range	15–70	6	0.8	0.88
Layer 3	Long range / strategic	70–500+	4	0.5	0.95

The technical probability P_i is defined conditionally: it is the probability of neutralization when a threat is actually assigned to an available engagement channel in layer i. Capacity loss is modelled separately. This avoids mixing two different failure mechanisms—technical engagement failure and the inability to initiate an engagement because all channels are busy.

2 Mathematical Model of Sequential Interception

2.1 Unsaturated conditional model

If capacity limitations are temporarily ignored and layer outcomes are treated as conditionally independent, the probability that at least one of L sequential layers neutralizes a threat is the complement of the probability that all layers fail [4].

$$P_{neut} = 1 - \prod_{i=0}^{L-1}(1 - P_i) \quad (1)$$

where:

– P_{neut} – overall probability that the threat is neutralized by at least one layer
– L – number of sequential defensive layers
– P_i – conditional technical neutralization probability of layer i when an engagement is attempted
– i – layer index, i = 0, 1, …, L − 1

Equation (1) is a useful reference model, but it is optimistic whenever layer effectiveness is correlated or when finite engagement channels create blocking. Real layered systems also share sensors, networks, rules of engagement and threat geometry, so statistical independence should be treated as an analytical approximation rather than a physical law.

2.2 Saturation model with finite engagement channels

Each layer is represented as an M/M/C/C loss system. Threat arrivals are approximated by a Poisson process, engagement times are exponentially distributed, there are C_i parallel engagement channels, and a threat that arrives when all channels are occupied cannot wait in a queue. Under these assumptions, the offered traffic in layer i is [4]:

$$\rho_i = \frac{\lambda_i}{\mu_i} \quad (2)$$

where:

– ρ_i – offered traffic to layer i, in erlangs
– λ_i – arrival intensity of threats reaching layer i, in threats per second
– μ_i – mean service rate of one engagement channel in layer i, in s^{-1}; the mean channel occupation time is $1/\mu_i$

$$B_i = \frac{\frac{\rho_i^{C_i}}{C_i!}}{\sum_{k=0}^{C_i}\frac{\rho_i^{k}}{k!}} \quad (3)$$

where:

– B_i – Erlang-B blocking probability in layer i
– C_i – number of simultaneously available engagement channels in layer i
– ρ_i – offered traffic defined in Equation (2)
– k – summation index

A blocked threat is not the only type of threat that survives a layer: a threat can also be accepted by a free channel but survive the attempted engagement. The effective neutralization probability per arriving threat must therefore include both channel availability and technical success:

$$P_{i,eff} = P_i(1 - B_i) \quad (4)$$

where:

– P_i,eff – effective probability that an arriving threat is neutralized in layer i

– P_i – technical probability of neutralization given an attempted engagement
– B_i – probability that all C_i engagement channels are occupied

Consequently, the correct mean-flow recursion is:

$$\lambda_{i+1} = \lambda_i[1 - P_i(1 - B_i)] \quad (5)$$

where:
– λ_{i+1} – mean rate of threats surviving layer i and reaching layer i + 1
– λ_i – mean threat arrival rate at layer i
– P_i – technical neutralization probability of layer i
– B_i – Erlang-B blocking probability of layer i

For a cascade of L layers, a convenient system-level effectiveness measure is the fraction of the input threat flow removed by the architecture:

$$P_{sys} = 1 - \frac{\lambda_L}{\lambda_0} \quad (6)$$

where:
– P_{sys} – system neutralization fraction for the specified arrival process and model assumptions
– λ_0 – threat arrival intensity at the first layer
– λ^L – breakthrough rate after the final layer L – 1

2.3 Corrected numerical example

The original draft used $\lambda_0 = 20$ threats/s, $\mu_0 = 2$ s^{-1} and $C_0 = 8$, hence $\rho_0 = 10$ erlangs. Erlang-B gives $B_0 = 0.3383$, not approximately 0.22. In addition, the original recursion $\lambda_1 = \lambda_0 B_0$ counted only blocked arrivals and omitted accepted engagements that failed technically. Applying Equations (2)–(5) produces the values in Table 2.

Table 2: Recursive saturation calculation for $\lambda_0 = 20$ threats/s.

Layer	λ_i in (s^{-1})	ρ_i	B_i	P_i,eff	λ_{i+1} out (s^{-1})
Layer 0	20.000	10.000	0.3383	0.6087	7.8251
Layer 1	7.825	6.521	0.0185	0.8343	1.2966
Layer 2	1.297	1.621	0.0050	0.8756	0.1613
Layer 3	0.161	0.323	0.0003	0.9497	0.0081

Under this illustrative parameter set, the final mean breakthrough rate is approximately 0.0081 threats/s and the corresponding modeled neutralization fraction is 0.9996. These values should not be interpreted as verified combat effectiveness: they are a consequence of the deliberately optimistic scenario coefficients in Table 1 and of the M/M/C/C assumptions.

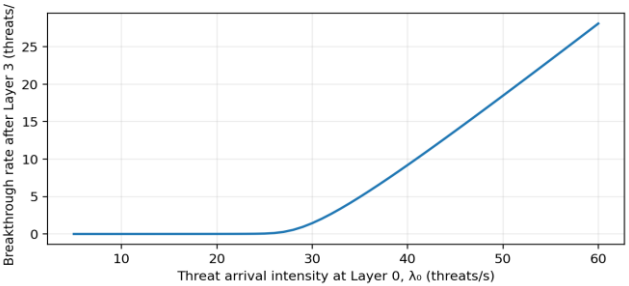


Figure 2: Modeled breakthrough rate as the input arrival intensity increases. The nonlinear rise reflects channel saturation.

Table 3: Sensitivity of the four-layer scenario to increasing arrival intensity.

λ_0 (threats/s)	Breakthrough rate (threats/s)	P_{sys}
10	0.0013	0.9999
20	0.0081	0.9996
30	1.4457	0.9518
40	9.1991	0.7700
50	18.4555	0.6309

3 Resource Allocation Across Layers

The original draft stated that an approximately 40/30/20/10 percent channel split is generally optimal and attributed the result to the Lagrange method. That conclusion does not follow from the stated model. Because C_i is an integer, B_i is nonlinear in C_i, and the arrival rate to every downstream layer depends recursively on all upstream choices, the allocation problem is discrete and scenario-dependent. A defensible formulation is:

$$C_{opt} = arg\,min\ \lambda_L(C),\ \ \Sigma_{i=0}^{L-1} C_i = C_{total},\ \ C_i \in \mathbb{Z}_+ \qquad (7)$$

where:

– C_{opt} – channel-allocation vector that minimizes the modeled breakthrough rate under the stated constraints
– λ^L – breakthrough rate after the final layer, computed recursively from Equation (5)
– C_i – integer number of engagement channels assigned to layer i
– C_{total} – total number of engagement channels available to distribute among all layers
– $\mathbb{Z}_+$ – set of positive integers

For a fixed threat scenario, the solution can be obtained by exhaustive integer enumeration, dynamic programming or other discrete optimization methods. If cost, interceptor inventory, defended-asset value or survivability are relevant, they should appear explicitly as additional constraints or terms in the objective function. Therefore, no universal percentage split is claimed in this paper.

4 Engagement-Time Constraint

For high-speed threats, the time available for detection, tracking, decision, weapon assignment and interception can be extremely short. NATO and JAPCC publications emphasize that hypersonic threats compress the engagement timeline and increase the importance of integrated sensing and resilient command and control [1, 7]. A simple kinematic upper bound is:

$$T_{budget} = \frac{R_e}{v_e} \tag{8}$$

where:
– T_{budget} – approximate time budget before the threat reaches the reference point
– R_e – closing distance from the threat to the reference point at the start of the considered engagement window
– v_e – assumed closing speed of the threat relative to the reference point

The end-to-end engagement time should include all relevant processing and physical delays:

$$T_{eng} = T_1 + T_2 + T_3 + T_4 + T_5 \tag{9}$$

where:
– T_{eng} – total time required to complete the engagement sequence
– T_1 – detection and initial classification time
– T_2 – track-establishment and track-quality time
– T_3 – command, decision and weapon-assignment time
– T_4 – launcher/effector preparation and launch delay
– T_5 – interceptor flight time or directed-energy dwell time to the required effect

$$T_{eng} < T_{budget} \tag{10}$$

where:
– T_{eng} – total engagement time defined in Equation (9)
– T_{budget} – available kinematic time budget defined in Equation (8)

For the illustrative values R_e = 15 km and v_e = 1700 m/s, Equation (8) gives approximately 8.82 s. The original statement that the system "must be below 6 s" is therefore a design margin, not a value derived from the kinematic relation itself. Likewise, a generic claim that AI-enabled systems achieve a 2–4 s reaction time is not retained without system-specific test data. AI-supported decision tools may help reduce operator workload and accelerate data fusion, but the end-to-end timing must be measured for the actual architecture [7].

5 Parametric Electronic-Warfare Sensitivity

The original draft represented jamming by multiplying the nominal sensor range R_0 by the factor $(1 - \gamma)$ and then stated that interception probability decreases nonlinearly. A single linear range-reduction law is not a general radar-jamming model because the effect depends on jammer power, geometry, waveform, processing gain, sensor type and electromagnetic-protection measures. For an unclassified sensitivity study, it is clearer to define γ_i as a normalized loss applied directly to the technical engagement probability:

$$P_i(\gamma_i) = P_{i,0}(1 - \gamma_i) \tag{11}$$

where:
– $P_i(\gamma_i)$ – technical neutralization probability used in layer i under the sensitivity case

– $P_{i,0}$ – baseline technical probability in the absence of the modeled degradation
– γ_i – dimensionless degradation coefficient, $0 \leq \gamma_i \leq 1$

Equation (11) is explicitly a parametric sensitivity model, not a physical prediction of radar or electronic-warfare performance. It can be replaced by a more detailed sensor or link-budget model when the required data are available. The corresponding system-level sensitivity is still evaluated through the same queueing recursion:

$$P_{sys}(\gamma) = 1 - \frac{\lambda_L(\gamma)}{\lambda_0} \tag{12}$$

where:
– $P_{sys}(\gamma)$ – system neutralization fraction under the selected degradation case
– $\lambda^L(\gamma)$ – breakthrough rate after the final layer with degraded technical probabilities
– λ_0 – input threat-arrival intensity

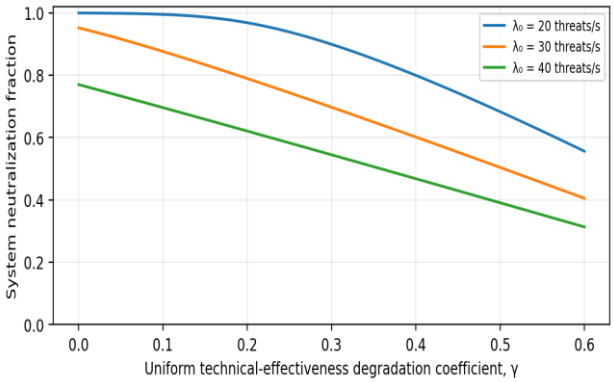


Figure 3: System-level sensitivity to a uniform reduction in technical engagement probability for three arrival intensities.

6 Operational Interpretation and Design Implications

The corrected model supports several conclusions without relying on system-specific classified data. First, layering provides repeated defensive opportunities and redundancy, consistent with NATO's current IAMD policy [1, 2]. Second, saturation is not captured by single-shot probability alone: finite engagement channels can become the dominant limitation as the offered load approaches or exceeds the available service capacity. This is directly reflected in the Erlang-B term [4] and is operationally relevant to mass-drone and salvo scenarios [3].

Third, low-cost or deep-magazine effectors can be valuable complements to expensive kinetic interceptors when they are technically suitable for the threat. Directed-energy systems are attractive because of potential low cost per shot and sustained firing while power is available, but they also face range, atmospheric, cooling and power constraints [5]. Therefore, a layered architecture should be analyzed as a portfolio of complementary effects rather than as a sequence in which every layer is universally superior to the next.

Fourth, command-and-control resilience, sensor integration and rapid information sharing are as important as the nominal range of individual effectors. NATO's IAMD policy explicitly identifies network-centric information sharing, redundancy, distributed C2 nodes, interoperability and rapid decision-making as important elements of the defensive architecture [1]. The model can be extended by making detection probability, track quality, communications availability and decision latency stochastic variables rather than constants.

Finally, the earlier draft's statements that three to five layers are universally optimal, that a sixth layer adds no more than two percent effectiveness, or that integration costs increase by 30–40 percent are not retained because the cited literature could not be verified and the claims do not follow from the presented equations. The economically optimal number of layers depends on threat composition, defended-asset value, interceptor and sensor costs, reliability, geography and logistics, and should be determined by an explicit cost-effectiveness model.

7 Model Limitations and Verification Path

The analytical model is intentionally compact. Its principal limitations are the Poisson-arrival and exponential-service assumptions, the use of mean-flow recursion rather than event-by-event correlation, constant conditional technical probabilities, absence of interceptor-magazine depletion, and simplified geometry. Queueing and simulation literature recommends validating such assumptions against observed or higher-fidelity simulated distributions when quantitative decisions depend on the results [4, 6].

A natural next step is a discrete-event or Monte Carlo implementation in which each threat has a type, trajectory, sensor-detection history, engagement eligibility, service time and conditional kill probability. Model outputs should include breakthrough probability, breakthrough rate, channel utilization, interceptor consumption, confidence intervals and sensitivity to input distributions. Such a simulation can then be compared with the analytical Erlang-B approximation to identify where the compact model is sufficiently accurate and where a richer representation is required [6].

Conclusion

A mathematically consistent model of layered air defence must distinguish between technical engagement effectiveness and the finite capacity to initiate engagements. The revised framework combines a conditional multi-layer probability model with Erlang-B blocking and a recursive threat-flow relation that correctly carries both blocked threats and unsuccessful engagements to downstream layers. The corrected numerical example shows that, for $C_0 = 8$ and $\rho_0 = 10$, the blocking probability is approximately 0.338 rather than 0.22, and it demonstrates how saturation can cause a sharp nonlinear rise in breakthrough rate as arrival intensity increases.

The paper also reformulates resource allocation as a discrete optimization problem, replaces unsupported fixed reaction-time claims with a transparent engagement-time budget, and treats electronic-warfare effects as an explicit sensitivity parameter rather than as a universal physical law. The framework is therefore suitable for unclassified

comparative studies, teaching, simulation verification and preliminary capability analysis, provided that scenario coefficients are not mistaken for validated performance data of operational systems.

This paper contains no classified information.

References

1. NATO. (2025, February 13). NATO Integrated Air and Missile Defence Policy. North Atlantic Treaty Organization.
2. NATO. (2025, February 13). NATO Integrated Air and Missile Defence. North Atlantic Treaty Organization.
3. Jensen, B., & Atalan, Y. (2025, May 13). Drone Saturation: Russia's Shahed Campaign. Center for Strategic and International Studies (CSIS).
4. Gross, D., Shortle, J. F., Thompson, J. M., & Harris, C. M. (2008). Fundamentals of Queueing Theory (4th ed.). John Wiley & Sons. https://doi.org/10.1002/9781118625651
5. U.S. Government Accountability Office. (2023). Science & Tech Spotlight: Directed Energy Weapons (GAO-23-106717).
6. Law, A. M. (2015). Simulation Modeling and Analysis (5th ed.). McGraw-Hill Education.
7. Van Wuytswinkel, A., & Anderson, K. (2025). An Operator's View on the Hypersonic Threat: Challenges and Imperatives for NATO. Joint Air Power Competence Centre, Journal Edition 40.

RECONNAISSANCE UNMANNED AERIAL SYSTEMS IN ARTILLERY: MODERNIZING TARGET ACQUISITION AND FIRE CONTROL FOR THE BULGARIAN LAND FORCES

Ivan K. Vladov, Daniel R. Rusev, Viktor D. Marinchev

Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria,
Ivankvladov@abv.bg, danielrussev@gmail.com, Viktormarinchev117@gmail.com

Abstract: *This paper examines modern requirements in indirect fire control and highlights the tactical necessity of integrating Unmanned Aircraft Systems (UAS) into Bulgarian Land Forces artillery units. It focuses on real-time target acquisition, electronic warfare (EW) resilience, and command-and-control (C2) software integration. Drawing on tactical lessons from the war in Ukraine, the study evaluates the operational effectiveness of pairing legacy Soviet-era platforms (2S1 Gvozdika, D-20, BM-21 Grad) with UAS to shorten the sensor-to-shooter loop.*

Keywords: *Artillery, UAS, Fire Control, Sensor-to-Shooter Loop, Tactical C2 Software, Effectiveness*

Introduction

There are many kinds of technical modernization vectors in the field of military engineering: automated fire control systems, digital tactical mapping networks, precision-guided munitions, counter-battery radar integration, and real-time aerial sensor networks. Indirect artillery fire remains the primary cause of battlefield casualties, accounting up for 80% of combat losses in contemporary armed conflicts. However, traditional target acquisition relying on ground-based Forward Observers (FOs), manual map plotting, and optical range finding has proven inadequate under modern battlefield conditions.

Seismic shifts in NATO's artillery doctrine emphasize that kinetic effectiveness is directly proportional to the speed and precision of target acquisition process. Legacy sight-and-adjust methods suffer from an extended sensor-to-shooter loop (up to 15 minutes), during which armored or mobile targets displace. Furthermore, achieving target destruction with unguided high-explosive (HE) rounds under legacy doctrine requires up to 60 shells per target area, heavily straining ammunition stockpiles and exposing firing batteries to enemy counter-battery fire.

Non-traditional methods of target acquisition using Unmanned Aerial Systems (UAS) enable an artillery battery to obtain real-time grid coordinates and instant battle damage assessment (BDA). By decoupling target acquisition from static ground observers and feeding automated ballistic software directly, the phenomenon of prolonged, inaccurate battery fire is eliminated. Thus, specialized UAS integration fights the root causes of artillery inefficiency, enabling first-round fire for effect and drastically compressing the kill chain.

1. Operational Baseline of Bulgarian Artillery Inventory

To evaluate the enhancement provided by UAS integration, the current baseline of the Bulgarian Land Forces artillery inventory must be established. The inventory relies predominantly on legacy Soviet-era platforms.

Table №1. Baseline capabilities and legacy fire control metrics of Bulgarian artillery platforms.

Platform	Caliber	Max Range (Standard)	Legacy Target Acquisition Method	Sight-and-adjust methods
2S1 Gvozdika	122mm	15.3 km	Visual FO / Optical Rangefinder (1V13)	6-8 minutes
D-20	152mm	17.4 km	Manual Optical Observation	8-10 minutes
BM-21 Grad	122mm	20.4 km	Map Overlay / Area Grid Coordinates	6-8 minutes

2. Investigation of Sensor-to-Shooter Loop Compression via Ukraine War Lessons:

Quantitative analysis of operational data from the conflict in Ukraine demonstrates that pairing aerial reconnaissance platforms with specialized tactical software (*Kropyva*, *Delta*) completely transforms indirect fire dynamics.

1. Loop Compression: The sensor-to-shooter loop duration is compressed from 20 minutes down to 90–180 seconds.
2. Ammunition Conservation: Real-time correction of unguided HE rounds reduces total shell expenditure for target neutralization by up to 60%.
3. Automated Ballistic Offload: Drone operators transmit exact target grid coordinates (x, y, z) directly to tablet-based C2 software (Kropyva), which automatically calculates elevation, deflection, meteorological variables, and barrel wear for each gun within seconds.

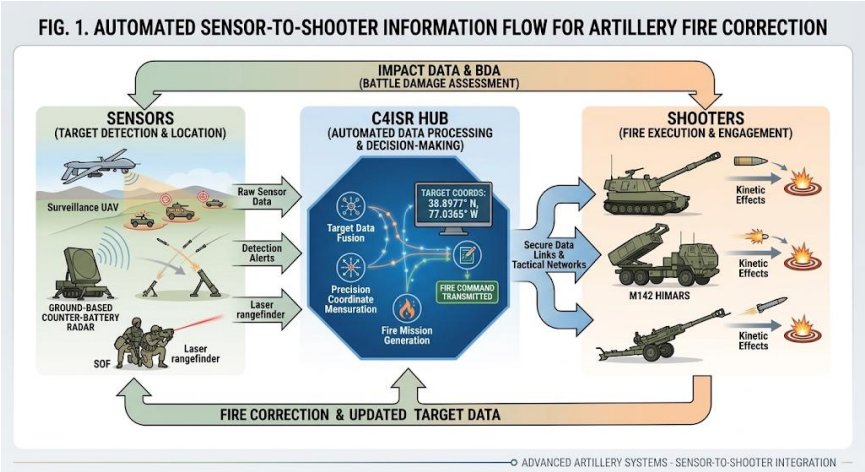


Figure 1: Automated sensor-to-shooter information flow for artillery fire correction

3. Comprehensive Tiered UAS Portfolio for Artillery Operations

Tier 1: Battery-Level Tactical Spotting (Rotary Wing).

Tier 1 systems provide immediate, organic reconnaissance and fire adjustment capabilities directly to forward artillery batteries and mortar platoons. These multirotor platforms require minimal setup time, can take off and land vertically in confined spaces, and offer hover capabilities for continuous target tracking.

Primary Platforms: DJI Matrice 350 RTK & Matrice 30T

- Flight Performance & Endurance:
  - Flight Time: Up to 55 minutes (Matrice 350 RTK) / 41 minutes (Matrice 30T) per battery cycle.
  - Operational Radius: 0 to 10 km from the Forward Line of Own Troops (FLOT), with line-of-sight video transmission extending up to 15 km via encrypted O3 Enterprise transmission links.
  - Environmental Protection: IP55 rating, allowing operations in heavy rain, dust, and extreme temperature ranges (-20°C to 50°C) with wind resistance up to 12 m/s.
- Payload & Sensor Integration:
  - Zenmuse H20T / H30T Payload: Integrates a wide-angle camera, a high-zoom camera (up to 200x optical/hybrid zoom), and an uncooled radiometric thermal sensor (640×512 resolution) for night operations.
  - Laser Rangefinder (LRF): Measures



Pic. 1 – Short Range FPV Style Drone

exact distance to targets from 1,200 m up to 3,000 m away, calculating target GPS coordinates in real time.

- High-Precision Positioning: Dual-antenna Real-Time Kinematic (RTK) system provides sub-meter positioning accuracy, critical for generating precise grid target coordinates for fire direction centers.

- Artillery Tactical Application:
  - Launched by battery-level forward observers to detect enemy positions, confirm target parameters, and observe shell impacts during initial registration fires.
  - Low unit cost (€2500 to 5000 per setup) makes these systems affordable and easily replaceable consumable assets at the platoon/battery level.

Tier 2: Brigade & Division Long-Range Reconnaissance (Fixed Wing).

Tier 2 systems consist of long-endurance, fixed-wing unmanned aircraft designed to operate deep behind enemy lines. They serve brigade and division-level artillery commanders by locating high-value targets, performing counter-battery reconnaissance, and executing Battle Damage Assessment (BDA).

1. Leleka-100 (DeVIRO, Ukraine)

- Key Specifications & Capabilities:
  - Flight Endurance: 2.0 to 2.5 hours.
  - Operational Radius: 45 km to 50 km (total flight path up to 100+ km).
  - Cruising Speed & Altitude: 60–70 km/h cruising speed (max 120 km/h) at operational altitudes up to 1,500 m.
  - EW Hardening: Built specifically for high-intensity warfare environments. Features anti-jamming GNSS modules, Frequency Hopping Spread Spectrum (FHSS) telemetry, and autonomous emergency navigation modes (returns to base via onboard inertial navigation if control signals are severed).

- Artillery Tactical Application:
  - Detects self-propelled howitzers, MLRS launchers, ammunition dumps, and command posts located deep in the enemy rear.
  - Transmits high-definition gyro-stabilized video and infrared imagery back to Brigade Tactical Operations Centers (TOC).



Pic. 2 - Leleka-100

2. WB Electronics FlyEye (Poland - NATO STANAG Compliant)

- Key Specifications & Capabilities:
  - Flight Endurance: Over 2.5 hours.
  - Operational Radius: Up to 50 km line-of-sight.
  - Launch & Recovery: Hand-launched

(no catapult required); landing is performed via a specialized belly-drop system where the payload capsule detaches and descends via parachute to protect sensitive optical payloads.

- NATO Interoperability: Fully compliant with NATO STANAG standards and natively integrates with automated artillery fire management networks (such as Polish TOPAZ system), passing target data directly to automated fire control units.
- Artillery Tactical Application:
- Performs silent gliding reconnaissance over high-risk sectors to pinpoint target positions without exposing its location through engine noise.

Tier 3: Indigenous Bulgarian Manufacturing & Assembly

Tier 3 focuses on establishing domestic assembly, repair, and modular production capabilities within Bulgaria to reduce foreign dependency, ensure supply security, and customize hardware for local geographic and threat conditions.

- Industrial Manufacturing Base:
  - Airframe Production: Composite material processing (carbon fiber molding and fiberglass structures) conducted at Bulgarian defense and aerospace industrial centers located in Plovdiv and Sofia.
  - Avionics & Flight Hardware: Local assembly utilizing open-source flight management architectures (PX4 / ArduPilot) paired with customized carrier boards.
  - Electronic Protection: Integration of Controlled Radiation Pattern Antennas (CRPA) to defeat directional jamming signals and commercial FHSS data links.
- Economic & Strategic Impact:
  - Reduces system procurement costs by approximately 50% compared to off-the-shelf foreign defense acquisitions.
  - Provides complete autonomy over repairs, software updates, maintenance, and rapid modification of frequency bands based on evolving electronic warfare conditions.



Pic. 3 - WB Electronics FlyEye drone

4. Mathematical Model for Coordinate Acquisition and EW Resilience

To ensure reliability in dense EW environments (where GNSS signals like GPS or GLONASS are jammed or spoofed), the technical architecture incorporates three primary countermeasures:

1. CRPA Antennas: Rejects jamming signals originating from terrestrial sources while maintaining satellite locks overhead.

2. Optical Flow & Visual Odometry: Allows flight controllers to maintain position estimation without GNSS telemetry based on camera ground-tracking algorithms.

3. Encrypted Telemetry: AES-128/256 digital encryption on control links prevents signal interception and command hijacking.

Mathematical Model for Coordinate Acquisition and EW Resilience

To achieve effective first-round fire, the drone payload must calculate the target's exact Geographic Coordinates (P_{target}) in MGRS or WGS-84. The drone calculates target position using its onboard GNSS/INS position (P_{drone}), aircraft slant range (R) from the Laser Range Finder (LRF), gimbal azimuth angle (θ), and elevation angle (ϕ):

$$P_{\text{target}} = P_{\text{drone}} + R \cdot \begin{pmatrix} \cos(\phi)\sin(\theta) \\ \cos(\phi)\cos(\theta) \\ \sin(\phi) \end{pmatrix}$$

5. Methods and Tactics for UAS Reconnaissance

The organizational role, tasks, crew composition, and aircraft selection of an Unmanned Aerial System (UAS) depend directly on its operational placement. For supporting artillery formations, UAS units are typically integrated into:

- General Support Artillery (regiments, battalions);
- Direct Support Artillery (self-propelled artillery battalions, mortar batteries).
- Types of Aerial Reconnaissance & Surveillance UAS carry out several core aerial missions:
- Point/Target Reconnaissance: Detailed observation of specific individual assets.
- Route Reconnaissance: Monitoring supply lines, advance routes, and axes of movement.
- Area Reconnaissance: Gathering intelligence over broad areas to identify enemy positions, deployment patterns, and terrain features.
- Aerial Surveillance: Systematic and continuous collection of real-time situational data across assigned sectors.

Tactical Reconnaissance Methods depending on mission requirements, the primary reconnaissance tactics include:

- Single Unmanned Aerial Vehicle (UAV) directional scanning along linear targets;
- Multiple passes over an area using parallel or intersecting flight paths;
- Flight path heading changes upon target approach to avoid predictability;
- Synchronized simultaneous reconnaissance using two UAVs on parallel routes;
- Control handoff of the UAV between two Ground Control Stations (GCS).

Factors Influencing Tactical Selection. The UAS or crew commander determines the specific reconnaissance method based on:

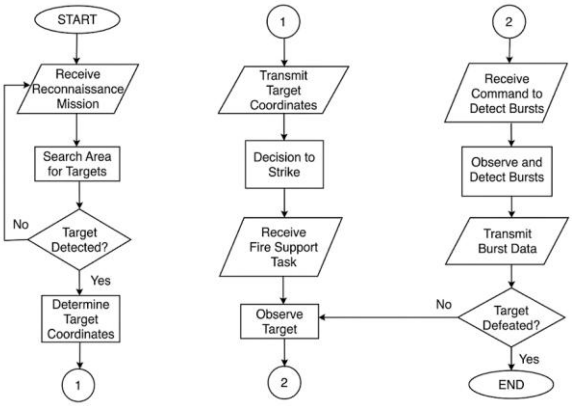
- Mission objectives and launch/landing location relative to the Forward Line of Own Troops (FLOT);

- UAV range, endurance, optical capabilities, and target density/camouflage;
- Enemy Air Defense (AD) and Electronic Warfare (EW) threat environments;
- Time of day, visibility, and atmospheric/weather conditions.

Flight Execution and Control. When supporting artillery fire, primary flight profiles consist of route flights, target search in designated sectors, and multi-area overflights for battle damage re-reconnaissance. Flight plans are generated via control software and executed primarily in automated flight modes with real-time operator intervention capabilities. High-definition video is streamed live to the GCS while encrypted flight and terrain data are saved to onboard storage.

Execution Procedure for UAS Reconnaissance Missions. The principal function of UAS in artillery operations is real-time target coordinate determination and continuous fire adjustment across all modern artillery firing modes. This workflow follows a structured nine-step operational cycle:

- Initiation: Receives the mission, assigns flight routes and UAV allocation, executes launch, and transits to the assigned sector;
- Search: The UAV flies the pre-planned route while the operator monitors live feeds. If a target is suspected, the operator commands loitering/hovering over known coordinates for closer inspection;
- Detection: The operator applies optical/digital zoom or enhances imagery resolution to recognize distinct target signatures. Control is switched to manual mode or designated loiter parameters (altitude, turn radius, heading).
- Identification: Determines target classification, specific elements, operational activity status, and degree of concealment/fortification.
- Location: Measures exact target coordinates, elevation, frontage, and depth using specialized software. Relays target layout, dispersion, and protection status to the Tactical Operations Center (TOC) / Command Post (CP) for target analysis.
- Engagement: The TOC evaluates weapon allocation, computes firing data, and issues fire commands to artillery batteries. The UAS crew is informed of round counts, interval timing, and Time of Flight (TOF). The UAV positions itself at a safe standoff loiter outside the firing plane.
- Correction: The operator detects shell impacts and impact center offsets relative to the target. The UAS commander verifies calculated deviations and transmits corrections directly to the firing unit.
- Assessment (BDA): Evaluates Battle Damage Assessment during and after fire execution. Calculates target destruction levels, equipment damage, fortification breaches, and neutralization percentages.
- Transition: Upon completing the fire mission, the UAV transitions back to broad area search or terminates the reconnaissance task.



Conclusion

For the Bulgarian Land Forces, building a modern, credible defense capability in high-risk environments doesn't require replacing the entire inventory overnight. Integrating a multi-tiered UAS network into existing artillery units provides a pragmatic, highly cost-effective path forward. Drones drastically shrink the sensor-to-shooter loop, turning legacy field guns into precision instruments. By substituting blind area bombardments with exact real-time targeting, troops can neutralize targets using a fraction of the munitions traditionally required.

This shift to precision yields massive financial and logistical benefits. Conserving scarce ammunition and reducing barrel wear drastically cuts long-term maintenance costs and lightens supply chain burdens, stretching defense budgets further without sacrificing firepower. Crucially, immediate target feedback enables rapid shoot-and-scoot operations, protecting firing crews and preserving expensive assets from counter-battery strikes. Ultimately, drone integration offers the military a force multiplier that bridges the gap between legacy systems and modern warfare at a price tag the budget can actually sustain.

References

1. Army Technology (2024). *Commercial-Off-The-Shelf (COTS) Drones in High-Intensity Artillery Operations*. Defense Procurement Reports, 14(3), 45-52.
2. Bozov I, ORDER OF PERFORMANCE TASKS BY UNMANNED AIRCRAFT SYSTEMS TO ARTILLERY FORMATIONS, International Scientific Conference ― Defense Technologies 2024, Shumen: pp 168-171, ISSN 2815-4282
3. Center for Strategic and International Studies (CSIS) (2024). *The First World Cyber-Air-Land War: Lessons from Ukraine*. Washington: CSIS Press.
4. Defense Express Technologies (2023). *Leleka-100 and Shark UAV Integration in Mass Artillery Adjustments*. Technical Analysis Report, Kyiv.

5. European Defence Agency (EDA) (2024). *Counter-EW Strategies for Tactical Unmanned Aerial Systems in European Land Forces*. Brussels: EDA Technical Publication.
6. Institute for the Study of War (ISW) (2024). *Tactical Innovations in Russian and Ukrainian Counter-Battery Warfare*. ISW Research Paper Series, No. 18.
7. International Institute for Strategic Studies (IISS) (2025). *The Military Balance 2025: Bulgarian Land Forces Equipment and Modernization Priorities*. London: Routledge.
8. Journal of Battlefield Technology (2023). *Laser Rangefinding and Target Location Error Reduction in Tactical Reconnaissance UAVs*. 26(2), 112-124.
9. NATO Joint Air Power Competence Centre (JAPCC) (2023). *Integration of Small UAS in Tactical Land Operations (STANAG 4586 Compliance)*. Kalkar: JAPCC.
10. Royal United Services Institute (RUSI) (2023). *Meatgrinder: Russian Tactics in the Second Year of Its War in Ukraine*. London: RUSI Defence Studies.
11. Ukrainian Ministry of Defence (2023). *Operational Field Reports on GIS Kropyva Deployment in Artillery Regiments*. MoD Military Press, Kyiv.

ERASMUS+ KA02 PROJECT DIMAS FINAL ISSUES AND RESULTS ANALYSIS

Linko G. Nikolov[1], Dilyan I. Dimitrov[2], Krasimir O. Slavyanov[3]

[1]Scientific Research and Innovations Institute, Shumen, National Military University, Bulgaria
[2]Radar and Communication systems Department, AADCIS Faculty, Shumen, Bulgaria
[3] AADCIS Faculty, Shumen, National Military University, Bulgaria
linkonikolov@gmail.com , dilyan1973@gmail.com , k.o.slavyanov@gmail.com

***Abstract**: The European Union Erasmus+ program offered the opportunity to work over strategic partnerships among European military academic institutions. By KeyAction02 projects, collaboration over different topics is available. Such is the finalizing DIMAS project, which aimed to improve the teaching and learning process of Defence and Security higher education Mathematics courses. The conclusive results of DIMAS project are presented in this review paper.*

***Keywords**: Erasmus+, Mathematics, Higher education, Defence and Security*

Introduction

The way of teaching and learning Mathematics in a contemporary digital environment, required by on-line learning, seems to be inadequate among young audiences. There are difficulties in presenting formulas, equations, theorems etc. With the DIMAS project the partners want to increase the interest in studying Mathematics, as well as provide more understandable Maths problems and easy to imagine Maths applications via the power of contemporary Math teaching digital tools.

The project is planned by methodological steps, first of which includes survey among students and teachers and after that - analysed responses. Common areas of Mathematics in Defence and Security are allocated and specific Mathematics-based problem scenarios are elaborated. It is planned to review a contemporary Maths teaching software. Test of the proposed innovative way of Mathematics teaching will be performed in the form of 4 learning, teaching and training activities (LTTAs) as part of project activities. One of the important sharing activity is the web domain www.dimas-project.eu creation.

1. Project management analyses.

Project management was the 1st work package of the DIMAS project. It was mainly divided into 8 sections:

1) Project monitoring – level of completion;
2) Work breackdown structure control – "who" did "what" and "when";
3) Fine budget control – workdays control by detailed activities description (eg. finished workdays for A3.1, A3.2, A4.3, …);
4) Risk management, risk handling - absence of missing project activities. Activities with travel and support, as well as with digital platform were ensured;
5) Accessible activities – the multiplier event was planned, and organized;
6) Digital tools – agreed which will be, practically used (e.g Matlab, Simulin, Maple.);
7) Green practices – unofficial online meetings regularly.

The project monitoring included constant communication over a specific internet chat application in a group (fig. 1), email and cloud storage for documents as intellectual outputs. Official Transnational Project Meeting (TPM4) was held in July 2025 in Athens, Greece (fig. 2). Also, unofficial online meetings were held, supporting the official Transnational Project Meetings, which were planned only 3 for the whole project period. By which transport and support funding savings is achieved. More than 10 persons took part during TPM4 with discussion over project tasks, budget details and accounting, DIMAS implementation plan and developed Math concepts for Defence and Security.

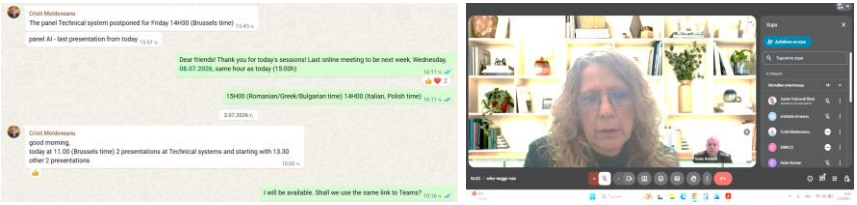


Fig. 1: Constant communication and unofficial online meetings



Fig. 2: DIMAS 4th Transnational Project Meeting, Athens, July 2025

The budget control included strict following the work days and work hours of the personnel allocated to the specific activities – not less than predefined from the project funding. Project contribution is made by including more work than the predefined in the project, as a co-financing mechanism.

Risk assessment concluded in more than one person to create project content and outcomes. For the financial coordination and control form Bulgarian side, two persons were available for funding transactions, and project leader and project coordinator available for double-chack control.

Project results achievement, sharing, planning and control was done by a combination between EMILYO IG Meetings, the DTF2025, DTF2026 and other conferences.

2. Math – related directions, branches and scenarios in Defence and Security education.

Work package 2 was named "Mathematics-based scenarios in defence and security and education". Total of 5 activities were planned and all of it were completed. An important point is to declare the most relevant Maths model directions of Defence and Security education. Such a list is presented in table 1. Some military specialties comprise more than 1 direction.

Table 1. Most descriptive directions of Defence and Security education

No	Directions in Defence and Security education	Example specialties
1	Technical systems for defence and security	Artillery
		Air Defence
		Missile Defence
		Military communication and information systems
2	Electronic warfare and cybersecurity	Signal reconnaissance and warfare
		Cyberoperations
		Electronic warfare
3	Logistics for defence and security	Military logistics
		Armament and ammunitions
4	Military leadership	Mechanized Land force troops
		Intelligence
5	AI for Defence and Security	Land forces
		Cyberoperations
		Military communication and information systems

After reviewing the DIAMS A2.1 Survey analysis, the A2.2 Definitions and the Security and Defence education subjects' content, most relevant mathematical branches and study cases were defined. The participating institutions had agreed over such a proposal, indicating 5 military directions. The proposed directions are included in the curriculum for diverse armed forces specialities. It needs to be stated that infantry tactics, intelligence operations tactics, shooting and other relevant for the military service knowledge is in its core away from Mathematics. But when it comes to science, all natural processes, connected with the tactical results and efficiency must be calculated.

After reviewing the different kinds of military specialties across the survey-respondent institutions, and thus defining relevant directions, the taught subjects were discussed and analysed. The most famous and most unknown Math topics were pointed out during formal and informal meetings activities. Although Math branches in Higher education are large number, with Table 2 efforts were concluded to present the most used in Defence and Security education.

Some of the presented branches in Table 2 are very complex, but in any case, seem relevant inside important subjects.

Table 2. Most used Mathematical branches

No.	**Mathematical branch**	**Relevancy** (where it can be found, formulas, explanations of processes etc.)
1	Basic mathematics	Higher Mathematics, Algorithm, Linear Algebra, Analytical Geometry, Trigonometry $s(t) = U_m.\sin(2.\pi.f.t)$, $s(t) = U_m.\cos(2.\pi.f.t)$
2	Algebra	Field theory, Abstract algebra, Boolean, Linear Algebra – vector representation of data, Distance computations in multidimensional space
3	Calculus and analysis	Modelling in telecommunications, Theory of electric equipment, Fourier-vector, Complex analysis, Functional analysis, Differential equations, Analytic Geometry – spatial relationships and geolocation clustering, Calculus – gradient concepts underlying data transformations and normalization $s(f) = \int_{-\infty}^{+\infty} s(t)e^{-i2\pi ft}\,dt$ $X = \frac{M_1X_1 + M_2X_2 + M_3X_3 + \cdots + M_nX_n}{M_1 + M_2 + M_3 + \cdots + M_n}$
4	Discrete mathematics	Discrete structures
5	Statistics Theory Probability theory	Statistics, Statistics & Probability – data distribution analysis, mean and variance calculations $\min \boldsymbol{K} = \sum_{i=1}\sum_{j=2} \boldsymbol{c_{ij}} \cdot \boldsymbol{x_{ij}}$
6	Decision theory	Numerical Methods – algorithmic parameter tuning and computational optimization, Problem solving
7	Graph theory	WAN area networks, number of routers,
8	Operational research (Game theory)	Data driven learning: collection of the results of the simulation and the participative discussion

The proposed directions in Table 1 and branches in table 2 can be included in several military specialties. A proposed education plan can be used during future Erasmus+ KA01 mobilities for cadets and for civilian students, having applied Math included (table 3).

Table 3. Curriculum for Military CIS and Electronic Warfare

No	**Subject**	**Math concept**	**Study cases**	**Class hours**
1	Signal processing	- Set operations and calculations	- Signal modulation	8 (4 hours for intensive LTTAs)
2	Modelling in telecommunications	- Random values and Gaussian distribution	- Signal-to-noise ratio calculation	8 (4 hours for intensive LTTAs)
		- Trigonometry and vector space representation	- Signal modulation	8 (4 hours for intensive LTTAs)

3	Decision Theory	- Linear Algebra - Mathematical Programming	- Transportation Problem, - Assignment Problem for Military Units	8 (4 hours for intensive LTTAs)
4	Logistics	- Boolean Algebra - Mathematical Programming	- The Shortest Route Problem	8 (4 hours for intensive LTTAs)
5	Artificial intelligence	- Set theory - Boolean mathematics	- Application of fuzzy logic in cybersecurity decision-making and analysis	8 (4 hours for intensive LTTAs)
6	Operational Research	- Algorithms - Graph Theory	- Minimum Spanning Tree	8 (4 hours for intensive LTTAs)
Total subjects number:		6	Total class hours:	48

The proposed curriculums in the DIMAS project can be further elaborated as subjects for an Erasmus+ mobility semester according to the desired specialties.

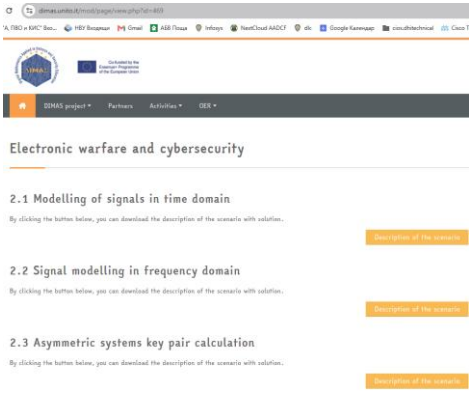


Fig. 3: Open "access on-demand" educational resources

It is believed that Math teaching and learning process will be mastered in a better manner with the developed open educational resources, which are be available as "access-on-demand" in the specialized dedicated web-based platform dimas.unito.it .

As an output of WP2, the following documents were created:

1) Best practices for Maths teaching and learning in security and defence education, An analysis after survey, 21 pages;
2) Math concepts for security and defence education, an education plan (Curriculum) with labelled study cases, 10 pages;
3) Typical mathematical branches and study cases, an analysis report, 7 pages;

4) Applied mathematical based scenarios in security and defense education, a Handbook, 27 pages.

The presented areas in the field of military education seem quantitative enough to conform many study cases. In DIMAS project the partner institutions have collected data and agreed 27 specific cases, called Scenarios

3. Didactic interactive materials based on mathematical software.

The objectives of DIMAS Work Package 3 were:

1) (O3.1) Identification of digital tools, digital environments and software that will be used for mathematical interdisciplinary activities, and
2) (O3.2) Creation of interactive materials specifically designed for the training of military officers that use digital tools to deal with mathematics and that contemplate interdisciplinary scenarios.

In details, (O3.1) aimed at promoting a comprehensive overview of the technological resources available for mathematical and interdisciplinary learning activities. Such resources, paired with proper methodologies, enhanced mathematical teaching and learning, collaborating among interdisciplinary teams. Tools were be explored through a survey for best practices (Activity A3.1) among European higher education institutions considering computational potentialities, effectiveness for teaching and learning, user-friendliness, number of different functionalities and other factors. The tools supported data analysis, visualization, modelling and simulation. The survey was created as a Google form and responded with 35 teachers.

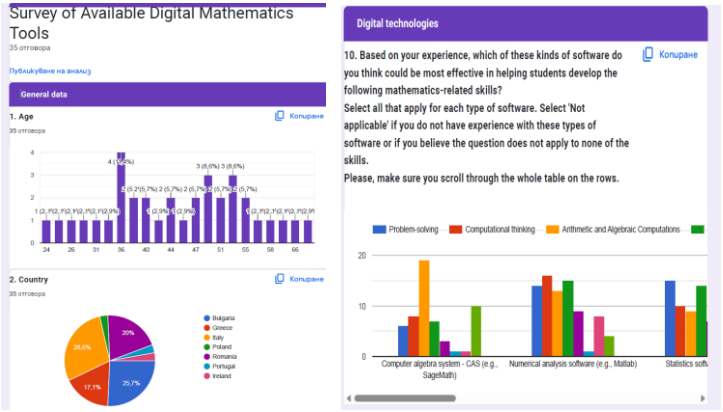


Fig. 4: Survey of available software tools

Objective (O3.2) aimed at providing teachers and students with the necessary elements for Math scenarios through interactive learning experiences to understand complex mathematical concepts, linked with the specific needs of security and defence education. Moreover, the materials allowed officers to develop their technical proficiency

in the use of digital tools, which is essential in today's technology-driven military landscape.

Outputs from the WP3 are:

1) Digital mathematics tools, An analysis after survey, 10 pages;
2) Open educational resources - in a dedicated platfiorm, for 5 specialties.

Example of a resource is https://dimas.unito.it/pluginfile.php/2319/mod_page/content/3/2.2.Signal%20Modelling%20in%20Frequency%20Domain.pdf

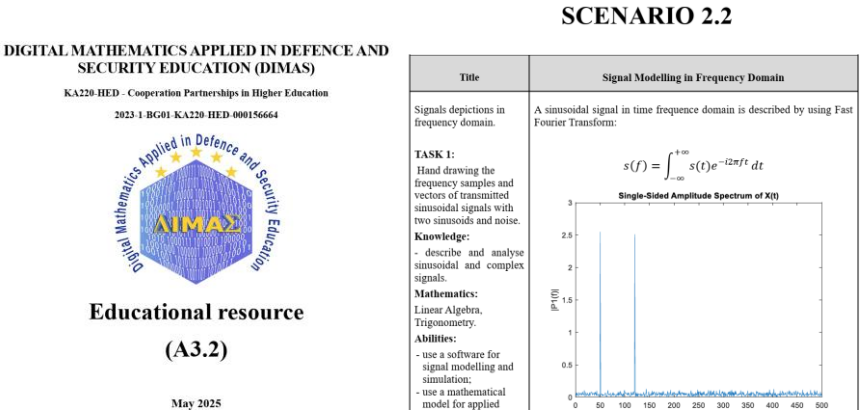


Fig. 5: OER for signal modelling in frequency domain

Some of the proposed scenarios are tested during Learning, Teaching and Training activities (LTTAs).

4. Learning, teaching and training activities as pilot courses for mathematics-based scenarios in defence and security education.

By this DIMAS Work Package 4, an extracted review of the Interactive didactic materials content was involved in 2 short term (5-days) joint staff training schools - LTTA1 and LTTA3. During these activities, teachers trained and test the availability and applicability to teach Maths via digital tools. A new approach to formulas, equations and theory presentation are trained among teachers i.e. 2D/3D visualisations, real-time calculations and live simulations.

With the 2 short term (5-days) course-specific schools - LTTA2 and LTTA4 the results are increased interest for learners in Math theory and positive attitude for problems solving. During LTTA2 and LTTA4 a certain amount of the WP3 prepared product was exploited - some practical tasks and some resolutions were performed. It is believed that it improved the Maths skills at a certain level.

The proposed activities in this WP4 were learning, teaching and training short-term pilot schools. During the staff training events, teachers were trained to operate and to teach with a specified Maths software. During the short-term pilot courses for students

they accessed, tested and implemented a newly created digital approach to learn applied Maths science in Defence and Security education fields.



Fig 6: LTTA2, logistics problem solving, Poland, 2025



Fig. 7: LTTA3, Application of digital tools for Math courses, Romania, 2026

By the proposed practising experience with short-term learning, teaching and training activities, most of the objectives for this WP4, and even for the whole project, are reached - test and evaluate the innovative Maths teaching experience. Actually, the essence of the DIMAS project proposal are these pilot schools in order to check how come a digital tools can help the new realities in Maths studies.



Fig. 8: LTTA4, signals modelling, Italy, 2026

Teachers and students experienced a newly created approach for Maths teaching. This approach is elaborated for a comfortable and understandable way of learning Math.

This project predicted 2 teachers from each partner to participate in LTTAs, but the number is higher. In this manner, more than 15 teachers from partner Institutions participated in the LTTAs. The profile of teachers is competences in Maths, or in Defence and Security education field. More than 30 students form all partner institutions were involved and benefited from the DIMAS project experience.

5. DIMAS project dissemination.

The development a shared web-based platform seems most valuable for higher education institutions in the field of military education. The sharing of the achieved results contributes to the adaptation of the created innovative methodology for the easier understanding and practical application of different mathematical approaches for working with different defense systems. DIMAS project results are regularly disseminated during Implementation Group (IG) meetings of the created network for sharing results through the "European Initiative for the exchange of young officers inspired by Erasmus" - EMILYO, an

initiative undertaken by the European Union Member States aimed at developing the exchanges between armed forces of future military officers as well as their teachers and instructors during their initial education and training - https://www.emilyo.eu/exchange_experience. The results of the project receive secure distribution not only on the website of the organization, but also at the regular meetings of the Implementation Group, the European Union Military Academies Commandants'

Seminar, the International Military Academy Forum (iMAF) and others. Another conference is obviously the Defence Technology Forum - Shumen.

A Matematics for applied military problems was organized and conducted among european students. They received tasks to calculate complex problems and defended by an online presentation in front of scientific comitte.

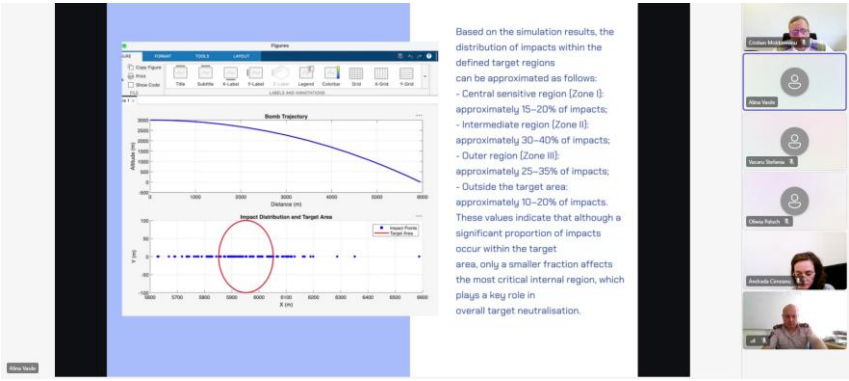


Fig. 9: Olympiad presentation, Alina Vasile, Romania, 2026



Fig. 10: DIMAS Multiplier event, Hotel Shumen, Bulgaria, 2026

For the dissemination and exploitation of open educational resources based on digital mathematics, 1 multiplier events was held in Shumen, Bulgaria, in which more than 80 participants understood the achieved results from the DIMAS project.

Conclusion

Increased interest in Mathematics science was observed in students' activities using modelling, simulation and coding software. The handbook for specific Maths-based scenarios and interactive didactic materials were used at the short-term schools (LTTAs). These short-term pilot schools tested the knowledge and skills of teachers and learners, connected with Maths science. All results from this project are presented in several

reviewing scientific papers and uploaded in the dedicated website: www.dimas-project.eu and the open educational resources web platform: https://dimas.unito.it/ .

Acknowledgments

This paper is created in favour of “Erasmus+” KA02 project 2023-1-BG01-KA220-HED-000156664 “Digital Mathematics Applied in Defence and Security Education - DIMAS”.

FUNCTIONING AND MILITARY EMPLOYMENT OF UNMANNED AERIAL SYSTEMS: STATISTICAL ANALYSIS OF DESIGN CONCEPTS, MISSION ROLES AND EMPLOYMENT TRENDS

Deyan N. Dimitrov

Department of Air Defense, Artillery, Air Defense and CIS Faculty at the Vasil Levski National Military University, Shumen, Bulgaria, deyandimitrov@aadcf.nvu.bg

Abstract: *This paper extends a functional analysis of military unmanned aerial systems with a descriptive statistical assessment of how drone concepts are implemented, what missions they support and how frequently selected concepts appear in recent public procurement and employment data. The study separates airframe configuration, control method, mission role and employment intensity because these dimensions overlap. Global proliferation data are combined with recent official Ukrainian procurement statistics, NATO and allied policy documents, and open-source analysis of one-way-attack drone campaigns. The results show broad worldwide proliferation, strong numerical dominance of FPV systems in recent high-intensity-war procurement snapshots, rapid growth of FPV and one-way-attack concepts, and growing importance of interceptor and fiber-optic-control variants. The statistical evidence is interpreted as descriptive rather than universal, because the underlying datasets differ in scope, date and denominator.*

Keywords: *unmanned aerial systems, UAV, military drones, FPV, ISR, one-way attack, reconnaissance, autonomy, statistical analysis, procurement, NATO*

Introduction

Unmanned aerial systems have evolved from specialized intelligence, surveillance and reconnaissance assets into a broad family of military capabilities that includes tactical observation, communications relay, electronic support, logistics, armed support, one-way attack, air-defence interception and increasingly autonomous functions. NATO and European defence institutions therefore treat UAS as part of a wider digital and networked force rather than as isolated aircraft [1–5]. The growing diversity of roles is accompanied by an equally important quantitative change: inexpensive small systems can now be procured and consumed in numbers that are orders of magnitude greater than traditional aviation platforms.

A statistical description of military drones is not straightforward because the word "drone" combines several different dimensions. An FPV system describes a piloting and employment concept; fiber-optic control describes a data-link implementation; "fixed-wing" describes an airframe; reconnaissance describes a mission; and one-way attack describes an expendable operational concept. These labels can overlap on the same platform. The purpose of this paper is therefore to analyse design and use through separate statistical dimensions and to avoid treating overlapping categories as if they were mutually exclusive.

The empirical basis combines long-term global proliferation data from the Center for the Study of the Drone with recent official procurement and delivery statistics from

Ukraine, allied support data, NATO policy documents and open analytical assessments of the Russia–Ukraine war [6–18]. The results are descriptive: they reveal scale, growth and concept prevalence within the cited datasets, but they do not represent a complete global inventory or a statistically random sample of all military UAS.

1 Functional Architecture and Design Concepts

1.1 Airframe implementation

Military UAS can be implemented as conventional fixed-wing aircraft, multirotors, helicopter-type rotorcraft, hybrid vertical-take-off-and-landing fixed-wing systems, expendable one-way aircraft, and very small nano or micro platforms. Fixed-wing systems generally favour endurance and area coverage; multirotors favour vertical take-off, hovering and precise low-altitude manoeuvre; hybrid VTOL designs combine runway independence with more efficient forward flight. Expendable concepts trade recoverability for simplicity, mass production and mission-specific use [1, 2].

Recent procurement data also demonstrate that "implementation" is increasingly modular. The same basic airframe can exist with radio-frequency or fiber-optic control, different cameras or sensors, different autonomy software and different mission payloads. This modularity explains why a single category may contain many variants and why counting only named platform families understates actual design diversity.

1.2 Control, navigation and autonomy

The UAS architecture includes the aircraft, flight-control computer, navigation subsystem, payload, communications link, ground-control or mission-management node, and the wider command-and-control network. Control ranges from direct tele-operation through waypoint-based semi-autonomy to higher levels of onboard perception, planning and cooperative behaviour. EDA's Action Plan on Autonomous Systems explicitly identifies enhancement of individual unmanned systems, cooperative autonomous systems and manned–unmanned teaming as development priorities [2]. NATO's revised AI strategy and Alliance Digital Strategy add requirements for responsible AI, interoperability, resilient digital infrastructure and data-centric operations [3, 4].

2 Military Mission Roles

The most persistent mission family is ISR. Small multirotors and fixed-wing systems provide local observation, while larger aircraft offer longer endurance and broader sensor coverage. A second family comprises armed or strike-support roles, including reusable armed UAS, FPV systems and one-way-attack aircraft. Other mission families include communications relay, electronic support, logistics, resupply, deception and counter-UAS interception. Public sources increasingly show that the same platform class may be repurposed across several roles, which supports a multi-label rather than single-label statistical representation [1, 14, 15].

Table 1: Functional interpretation of major military UAS concepts.

Concept	Typical structural feature	Primary military purpose	Statistical treatment
Multirotor / FPV	VTOL, high manoeuvrability, short-range tactical employment	ISR, close support, local strike, adjustment	High-volume concept; FPV may overlap with fiber-optic control
Fixed-wing reusable	Efficient forward flight and longer endurance	ISR, surveillance, relay, selected strike roles	Countable by model family and procurement category
Hybrid VTOL fixed-wing	Vertical launch/recovery plus wing-borne cruise	ISR, relay, logistics	Emerging design concept; limited public quantitative breakdown
One-way attack / loitering	Expendable air vehicle, mission-specific payload	Longer-range or persistent strike concept	Employment often measured as launch rate rather than inventory
Interceptor UAS	High responsiveness and air-target engagement role	Counter-UAS / point and area defence support	Often reported as daily delivery or production rate
Cargo / logistics UAS	Payload volume prioritized over sensors	Resupply, evacuation support, delivery	Lower-volume specialized mission category

3 Statistical Methodology

3.1 Data hierarchy and comparability

Three types of quantitative evidence are used. First, global proliferation indicators describe how widely military drone programmes and platform types have spread. Second, procurement and delivery statistics measure industrial and force-generation scale. Third, launch or delivery rates indicate operational intensity for selected concepts. These quantities have different denominators and must not be combined into a single global percentage. In particular, the recent Ukrainian data are highly informative about high-intensity warfare but are not assumed to represent the force structure of every NATO member or every conflict.

The distinction between mutually exclusive categories and overlapping attributes is essential. A reconnaissance drone can be fixed-wing; an FPV drone can use fiber-optic control; and an interceptor can also be a multirotor. Therefore, mission shares and technical-attribute incidences are calculated separately.

3.2 Statistical indicators

For a mutually exclusive concept category i, its descriptive share in a dataset of N systems is:

$$p_i = \frac{n_i}{N} \tag{1}$$

where: p_i – share of concept i; n_i – number of observations assigned to concept i; N – total observations in the dataset.

For a technical attribute j that can overlap other categories, an incidence rate is used:

$$q_j = \frac{m_j}{N} \tag{2}$$

where: q_j – incidence of attribute j; m_j – observations carrying attribute j; N – total observations. Because attributes may overlap, the sum of q_j across attributes may exceed 1.

Changes in scale are summarized by a growth factor and a relative percentage change:

$$G = \frac{X_2}{X_1} \tag{3}$$

where: G – growth factor; X_1 – earlier value; X_2 – later value.

$$\Delta = \frac{X_2 - X_1}{X_1} \times 100\% \tag{4}$$

where: Δ – relative change, percent; X_1 – earlier value; X_2 – later value.

A simple catalogue-diversity indicator is used only for descriptive comparison of public marketplaces:

$$D = \frac{M}{S} \tag{5}$$

where: D – average number of listed models per participating manufacturer; M – listed models; S – participating manufacturers. It is not a quality or productivity metric.

4 Statistical Analysis of Military Drone Concepts

4.1 Global proliferation

The Drone Databook reported in September 2019 that at least 95 countries maintained active military drone programmes, with at least 21,000 military drones and more than 170 different types in service worldwide [6]. The March 2020 update raised the estimate to at least 102 countries with active military drone programmes [7]. This corresponds to an increase of about 7.4% in the number of countries recorded within roughly half a year. The numbers are now historically dated, but they demonstrate that military UAS had already moved from a specialist capability to standard equipment before the recent mass proliferation of FPV and one-way-attack systems.

4.2 High-volume concept prevalence in recent Ukrainian deliveries

A particularly useful recent dataset is the Ukrainian Ministry of Defence report covering more than 2.2 million drones delivered over a six-month period. It states that the total included nearly 1.8 million FPV drones, 352,000 fiber-optic-controlled drones, around 23,000 deep-strike drones and more than 53,000 reconnaissance drones; at the same time, interceptor drones were being supplied at a current rate of 1,500 per day [8]. Using Equation (1), FPV drones account for approximately 81.8% of the reported total. Reconnaissance and deep-strike categories correspond to about 2.4% and 1.0%, respectively. Using Equation (2), fiber-optic control has an incidence of 16.0%.

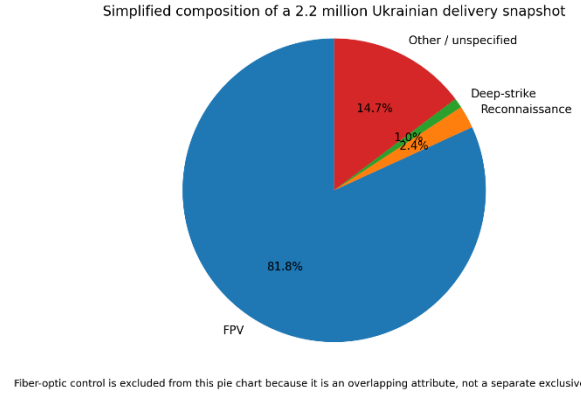


Figure 2: Simplified exclusive composition of the six-month Ukrainian delivery snapshot, excluding the overlapping fiber-optic-control attribute [8].

Figure 2 deliberately uses a pie chart only for the simplified exclusive split FPV–reconnaissance–deep-strike–other. The overlapping fiber-optic-control attribute is excluded from the pie chart because it is largely embedded inside the FPV category. Figure 3 then presents the overlapping incidences separately in order to avoid a misleading sum of percentages.

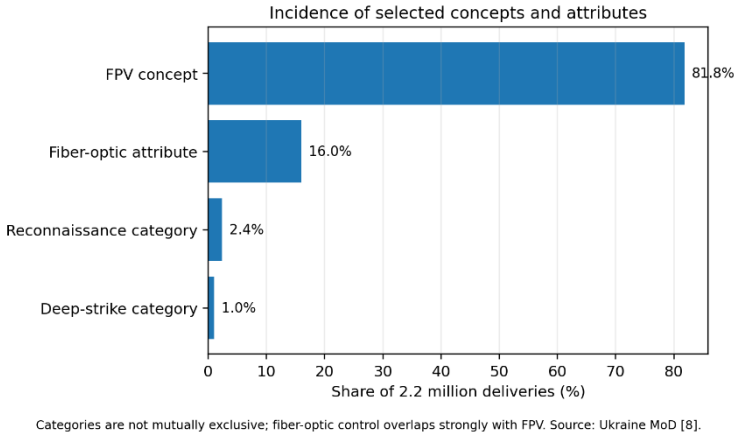


Figure 3: Incidence of selected concepts and overlapping attributes in the same Ukrainian dataset [8].

4.3 FPV scaling as a dominant mass concept

FPV systems are the clearest example of a concept moving from niche experimentation to industrial scale. Ukraine stated that 3 million FPV drones would be delivered in 2025, almost 2.5 times the previous year [9]. The implied 2024 baseline is approximately 1.2 million FPV drones, giving a growth factor of about 2.5 and a relative increase of roughly 150% according to Equations (3) and (4). In March 2025, the Ministry of Defence also stated that procurement plans had reached 4.5 million FPV drones for that year, while total drone procurement in 2024 exceeded 1.5 million systems of all types [16]. These figures demonstrate the central role of expendable, short-range, low-cost platforms in high-intensity force generation.

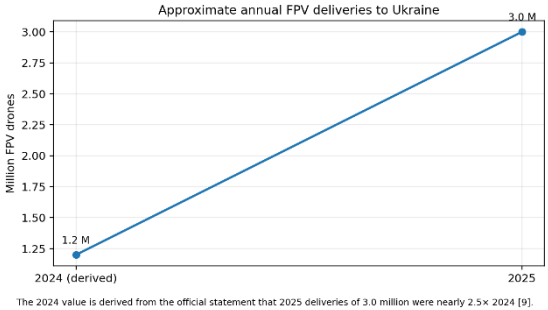


Figure 4: Approximate scaling of annual FPV deliveries, using the official 2025 total and reported 2.5× year-on-year ratio [9].

4.4 Model diversity and structural implementation

High-volume procurement is accompanied by rapid design diversification. By November 2025, the DOT-Chain Defence marketplace offered more than 180 FPV drone models from 40 manufacturers; nearly one third of the first 100,000 FPV drones delivered through the platform used fiber-optic control [10]. In a separate fixed-wing marketplace update, 12 models from eight Ukrainian companies were available, with most described as reconnaissance systems [11]. These values do not measure industrial efficiency because the marketplace dates and inclusion criteria differ, but they illustrate how FPV concepts are characterized by especially rapid variant proliferation.

Multirotor procurement also continued to accelerate: Ukraine reported a 17% increase in February 2026 deliveries relative to January and at least a doubling of contracted multirotor volumes compared with the same period of the previous year [12]. The procurement source identifies reconnaissance as a major daily task for these systems, confirming that multirotor airframes are not synonymous with strike employment alone.

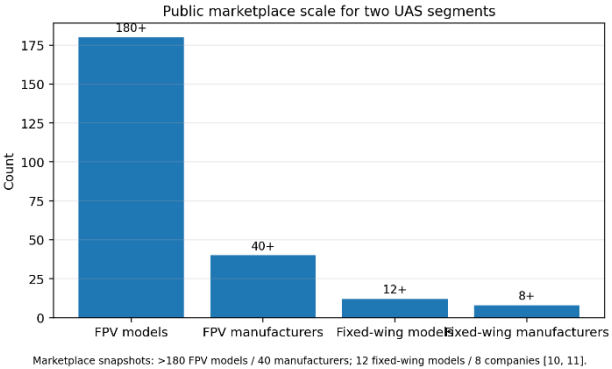


Figure 5: Reported public marketplace scale for FPV and fixed-wing segments [10, 11].

4.5 One-way-attack and interceptor concepts

The one-way-attack concept represents a different statistical pattern: operational intensity is often measured in launches rather than reusable inventory. CSIS reported that Russian Shahed-type launches increased from approximately 200 per week in September 2024 to more than 1,000 per week by March 2025 [13]. Taking 1,000 as a lower-bound value gives a growth factor of at least 5 and a relative increase of at least 400%. RUSI similarly described the current war as characterized by millions of FPV systems on the battlefield and thousands of one-way-attack drones used in long-range strike campaigns [14].

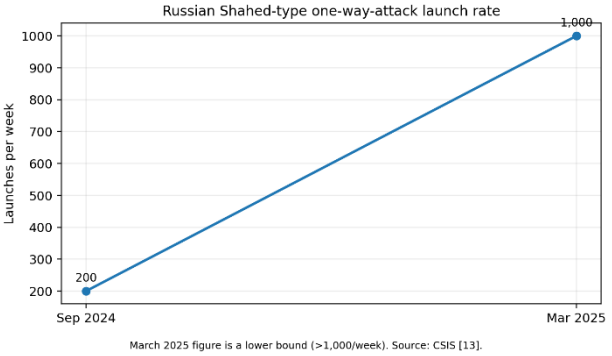


Figure 6: Increase in the weekly Russian Shahed-type one-way-attack launch rate reported by CSIS [13].

At the opposite end of the engagement cycle, interceptor drones are emerging as a distinct air-defence concept. Ukrainian procurement reporting in early 2026 cited a current supply rate of 1,500 interceptor drones per day [8], while a separate procurement

update recorded an average December 2025 delivery rate of about 950 anti-Shahed interceptor drones per day [17]. These are rates rather than annual totals, but they indicate a shift toward using unmanned systems not only as threats and strike assets, but also as lower-cost components of layered counter-UAS defence.

5 Interpretation of the Statistical Results

The first conclusion is that no single statistic captures "how often drones are used." Inventory counts favour reusable systems, procurement counts favour expendable systems, and launch rates favour actively consumed attack concepts. A complete analytical picture therefore requires at least four dimensions: number of platforms, number of variants, mission category and utilization or delivery rate.

Second, the current high-intensity-war data show a pronounced numerical dominance of FPV systems. Their 81.8% share in the cited six-month Ukrainian delivery snapshot reflects a combination of low unit cost, rapid manufacturing, direct tactical demand and high attrition. This does not imply that FPV systems are strategically more important than every other UAS type. Reconnaissance, fixed-wing surveillance, communications and long-range systems may be far fewer in number while generating disproportionate information or operational value.

Third, the relationship between airframe and mission is many-to-many. Multirotors perform reconnaissance, adjustment, logistics and strike tasks; fixed-wing systems can provide ISR, relay or deep-mission functions; fiber-optic control is a communications solution rather than a mission; and autonomous functions can be added to several airframe classes. For this reason, future military UAS databases should use multi-label coding and should present pie charts only for explicitly non-overlapping subsets.

Fourth, current procurement and market data reveal a short innovation cycle. The presence of more than 180 FPV models from 40 manufacturers on one procurement platform, together with rapid shifts toward fiber-optic control and interceptor concepts, suggests that configuration diversity is itself an operational characteristic. Standardization remains necessary for interoperability, but excessive standardization can slow adaptation. The challenge is therefore to standardize interfaces, data and safety requirements while allowing rapid evolution of airframes, payloads and control methods [2–4].

6 Autonomy, Networking and Future Military Employment

Future UAS development is likely to move from platform-centric to network-centric capability. NATO's Alliance Digital Strategy emphasizes interoperable, secure-by-design infrastructure, data-centric operations and human–machine collaboration [4]. EDA's autonomous-systems plan similarly emphasizes cooperative autonomy and manned–unmanned teaming [2]. For military drones, these directions imply more onboard perception, resilient navigation, distributed mission management, sensor fusion and coordination among multiple platforms.

Statistically, this transition will make traditional platform counts even less informative. A swarm or collaborative mission may involve many inexpensive nodes acting as one functional system, while a large reusable UAS may support several units

simultaneously through persistent sensing or communications relay. Future evaluation should therefore include mission effects per sortie, information latency, availability, loss rate, operator workload, network resilience and cost per mission effect, not only the number of aircraft procured.

7 Limitations and Verification Requirements

The statistical analysis has several limitations. The global Bard College data provide broad proliferation coverage but predate the 2022–2026 acceleration in FPV and one-way-attack concepts. The Ukrainian figures are recent and unusually detailed, but they describe one country fighting a high-intensity war and therefore should not be generalized directly to peacetime force structures. Several reported categories overlap, and some sources describe planned procurement while others report actual deliveries or launch rates. Official wartime claims may also reflect institutional definitions and reporting incentives.

Accordingly, the paper does not use confidence intervals or significance tests, because the observations are not a probability sample. The appropriate method is descriptive statistics with explicit denominators, source dates and category definitions. A more rigorous international study would require a standardized database with platform-level records, mission coding, airframe configuration, control method, procurement quantity, loss or attrition status and annual sortie or launch counts.

Conclusion

Military UAS are best understood as a family of overlapping technological and operational concepts rather than a single aircraft category. The structural implementation ranges from reusable fixed-wing and multirotor platforms to hybrid VTOL, expendable one-way systems and emerging interceptor drones. Their purposes span ISR, communications, electronic support, logistics, close tactical support, longer-range strike and counter-UAS defence.

The statistical evidence shows two simultaneous trends. Globally, military drone capability has become widespread: by 2020 more than 100 countries were already recorded as operating military drone programmes. In contemporary high-intensity warfare, the numerical centre of gravity has shifted toward mass, expendable or rapidly replaceable systems. In the cited Ukrainian six-month delivery snapshot, FPV drones represented about 81.8% of all reported drone deliveries, while fiber-optic control had a 16.0% incidence as an overlapping technical attribute. FPV deliveries increased by roughly 2.5 times from 2024 to 2025, and Russian Shahed-type launch rates increased by at least five times between September 2024 and March 2025.

These figures should not be interpreted as a universal formula for future forces. Lower-volume reconnaissance, communications, long-endurance, logistics and interceptor systems perform functions that cannot be replaced simply by increasing FPV quantities. The more robust conclusion is that future military UAS architectures will combine mass with specialization: large numbers of inexpensive tactical systems, smaller numbers of persistent and high-value nodes, resilient communications, data-centric command and control, and progressively higher levels of autonomy. Statistical evaluation

must therefore remain multidimensional and transparent about the difference between airframe design, mission, control technology and actual employment frequency.

References

1. Joint Air Power Competence Centre (JAPCC). (2010). Strategic Concept of Employment for Unmanned Aircraft Systems in NATO.
2. European Defence Agency. (2024). EDA Action Plan on Autonomous Systems (APAS).
3. NATO. (2024, July 10). NATO releases revised AI strategy.
4. NATO. (2026, January 13). Alliance Digital Strategy.
5. U.S. Department of Defense. (2024, December 5). DoD Announces Strategy for Countering Unmanned Systems.
6. Gettinger, D. (2019). The Drone Databook. Center for the Study of the Drone at Bard College.
7. Center for the Study of the Drone at Bard College. (2020, March). Drone Databook Update.
8. Ministry of Defence of Ukraine. (2026). Systemic changes to strengthen Ukraine's military: report on weapons procurement and drone deliveries.
9. Ministry of Defence of Ukraine. (2025, December 24). Armed Forces of Ukraine to receive 3 million FPV drones by year-end.
10. Ministry of Defence of Ukraine. (2025, November 24). First 100,000 FPV drones delivered through DOT-Chain Defence.
11. Ministry of Defence of Ukraine. (2025, September 25). DOT-Chain Defence: fixed-wing drones now available for order by the military.
12. Ministry of Defence of Ukraine. (2026, March 11). The Ministry of Defence contracted a record number of multirotor drones for the front.
13. Jensen, B., & Atalan, Y. (2025, May 13). Drone Saturation: Russia's Shahed Campaign. Center for Strategic and International Studies.
14. Bronk, J. (2025, August 4). NATO Should Not Replace Traditional Firepower with "Drones". Royal United Services Institute.
15. Watling, J., & Reynolds, N. (2025). Emergent Approaches to Combined Arms Manoeuvre in Ukraine. Royal United Services Institute.
16. Ministry of Defence of Ukraine. (2025, March 10). In 2025, the Ministry of Defence plans to procure 4.5 million FPV drones.
17. Defence Procurement Agency of Ukraine. (2026, January 7). Interceptor drones for the military: 2025 results.
18. UK Ministry of Defence. (2025, June 4). Tenfold increase in UK drone deliveries for Ukraine.

INNOVATIVE ALGORITHMS FOR RADAR INFORMATION PROCESSING: SPARSE RECOVERY, TRANSFORMERS, DEEP UNFOLDING AND COGNITIVE RADAR

Stanimir H. Parvanov, Ivan Y. Radev, Dilyan I. Dimirov

Department of Air Defense, Artillery, Air Defense and CIS Faculty at the Vasil Levski National Military University, Shumen, Bulgaria,
shparvanov@aadcf.nvu.bg, iyradev@nvu.bg, dilyan.dimitrov@aadcf.nvu.bg

Abstract: *Modern radar systems operate in an increasingly heterogeneous electromagnetic environment characterized by dense clutter, low-observable and maneuvering targets, interference, limited coherent processing time, and rapidly growing data volumes. Conventional radar processing based on matched filtering, Doppler processing, constant-false-alarm-rate detection, and model-based tracking remains indispensable because it is physically interpretable and computationally efficient. Nevertheless, recent research shows that several bottlenecks can be reduced by combining classical signal processing with sparse reconstruction, Bayesian learning, deep neural networks, transformers, graph-based data association, deep unfolding, and reinforcement learning.*

Keywords: *radar signal processing, sparse recovery, STAP, sparse Bayesian learning, deep learning, transformer, micro-Doppler, deep unfolding, cognitive radar, reinforcement learning*

Introduction

Digital radar processing has traditionally been built around a sequence of well-understood operations: calibration, pulse compression, coherent integration, Doppler processing, adaptive suppression of interference and clutter, threshold detection, measurement extraction, tracking, and classification. This architecture remains technically sound because each processing stage is connected to a physical model and can be verified with known limiting cases [1]. However, the operational environment of modern radar is more demanding than the assumptions used in many classical derivations. The clutter may be nonstationary, the training data available for adaptive filtering may be nonhomogeneous, targets may maneuver abruptly, multiple objects may cross within the same resolution cell, and low-observable targets may generate only weak or intermittent signatures. At the same time, modern active electronically scanned arrays and multi-channel receivers create large multidimensional data cubes that cannot always be processed by computationally expensive optimal algorithms in real time.

The development of artificial intelligence has therefore produced two parallel trends. The first is data-driven radar processing, in which convolutional neural networks (CNN), recurrent neural networks, Vision Transformers (ViT), general transformer architectures and graph neural networks learn mappings directly from radar measurements or derived representations such as range-Doppler maps, high-resolution range profiles, micro-Doppler spectrograms, and SAR images. Reviews of deep learning for radar show applications in waveform design, radar signal recognition, automatic target recognition, jamming/clutter identification and suppression, and array processing [3, 4]. The second trend is model-driven learning, in which the mathematical structure of radar estimation is

preserved while selected parameters or update steps are learned from data. Sparse Bayesian learning, deep unfolding, physics-informed priors, and reinforcement learning for cognitive radar belong to this category [5, 6, 10, 12, 13].

The objective of this paper is to systematize the most relevant innovative algorithms for radar-information processing and to formulate a practical hybrid architecture suitable for research, simulation and subsequent experimental validation. The emphasis is on algorithms that address five recurring problems: (1) clutter suppression with insufficient homogeneous training data; (2) detection and reconstruction in sparse scenes; (3) automatic recognition from short or noisy radar observations; (4) multi-target association and tracking of maneuvering objects; and (5) adaptive allocation of waveform and radar resources. The numerical performance values cited in the paper are taken only from the corresponding published sources and are not generalized beyond their experimental conditions.

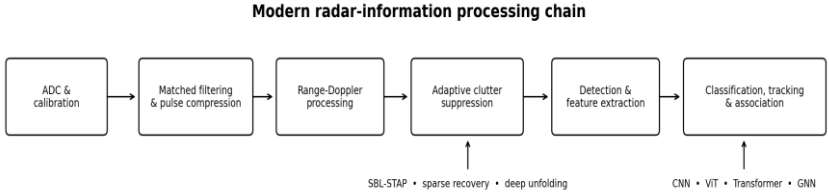


Figure 1: Classical and innovative stages in a modern radar-information processing chain.

1 Radar-Information Model and Classical Baseline

1.1 Complex baseband echo model

A useful starting point is the complex baseband model of the received radar signal. For a set of K point-like scattering components, the received waveform can be represented as

$$r(t) = \sum_{k=1}^{K} \alpha_k \, s(t - \tau_k) e^{j2\pi f_{D,k} t} + c(t) + n(t) \quad (1)$$

where:

$r(t)$ – complex received signal;
K – number of modeled scattering components;
α_k – complex amplitude of component k;
$s(t)$ – transmitted baseband waveform;
τ_k – delay associated with target range;
$f_{D,k}$ – Doppler frequency of component k;
$c(t)$ – clutter and structured interference;
$n(t)$ – receiver noise.

Equation (1) highlights why modern radar processing is inherently multidimensional. The useful information is distributed over delay, Doppler, angle, polarization, time, and sometimes over several spatially separated sensors. Classical processing extracts these dimensions sequentially. The main advantage of this architecture is interpretability; its weakness is that each stage usually assumes a simplified statistical model of the environment.

1.2 Matched filtering and coherent processing

For a known transmitted waveform, the matched filter maximizes the output signal-to-noise ratio for a deterministic signal in additive white Gaussian noise [1]. Its delay-domain output can be written as

$$y(\tau) = \int r(t)s^*(t-\tau)\,dt \tag{2}$$

where:

$y(\tau)$ – matched-filter output;

$r(t)$ – received signal;

$s(t-\tau)^*$ – complex-conjugated delayed replica of the transmitted waveform;

τ – trial delay.

After pulse compression, a discrete Fourier transform across successive pulses produces Doppler information and the familiar range-Doppler representation. CFAR detection, Kalman-family tracking, and conventional beamforming remain strong baselines because they are efficient and their error mechanisms are well understood. Innovative algorithms should therefore be evaluated against these baselines rather than treated as automatic replacements.

2 Innovative Algorithm Families

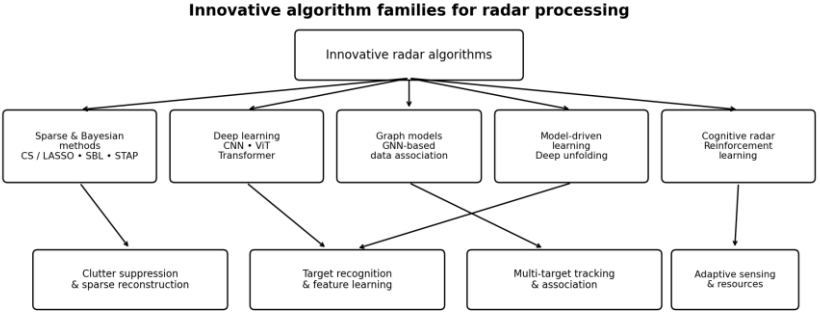


Figure 2: Taxonomy of algorithm families currently influencing radar-information processing.

2.1 Sparse recovery and compressive sensing

Many radar scenes are sparse in an appropriate domain. A surveillance volume may contain only a small number of targets compared with the number of range-angle-Doppler cells, while SAR scenes can often be represented with a limited set of dominant scatterers. Sparse-recovery methods exploit this structure by reconstructing a high-dimensional scene from fewer or corrupted measurements. A common formulation is the LASSO-type estimator

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}} \left[\frac{1}{2} \| \mathbf{y} - \mathbf{A}\mathbf{x} \|_2^2 + \lambda \| \mathbf{x} \|_1 \right] \tag{3}$$

where:

– estimated sparse scene vector;

y – measurement vector;

A – sensing or dictionary matrix;
λ – regularization coefficient;
$||\cdot||_2$ – Euclidean norm;
$||\cdot||_1$ – sparsity-promoting ℓ_1 norm.

A 2024 review by Quan et al. summarizes sparse recovery in spatial processing, pulse compression, coherent processing, radar imaging and target detection [5]. The main advantage is the ability to exploit scene sparsity and potentially reduce the number of required samples. The main limitations are sensitivity to dictionary mismatch, regularization selection, off-grid targets, and computational cost when iterative optimization is applied to very large data cubes.

Sparse Bayesian learning (SBL) addresses part of this problem by assigning probabilistic priors to coefficients and iteratively estimating their relevance. In heterogeneous environments this can be especially useful for covariance estimation. Cao, Wang and Wang proposed a reduced-dimension beam-space post-Doppler STAP method in which SBL estimates the clutter-plus-noise covariance matrix from only a single training sample, followed by angular-Doppler channel selection and reduced-dimension filtering [6]. The result is important because conventional optimal STAP requires many statistically homogeneous training samples, which are often unavailable near clutter edges, terrain transitions or strong discrete interferers.

2.2 Space-time adaptive processing with data-efficient covariance estimation

STAP jointly exploits spatial and pulse-to-pulse degrees of freedom to suppress clutter and interference. For a steering vector **s** and clutter-plus-noise covariance matrix **R**, the classical minimum-variance distortionless response weight is

$$\mathbf{w}_{\text{opt}} = \frac{\mathbf{R}^{-1}\mathbf{s}}{\mathbf{s}^{H}\mathbf{R}^{-1}\mathbf{s}} \tag{4}$$

where:

w_{opt} – optimal adaptive weight vector;
R – clutter-plus-noise covariance matrix;
s – target steering vector;
$(\cdot)^{H}$ – Hermitian transpose.

The theoretical expression is compact, but reliable covariance estimation is the practical bottleneck. Contemporary approaches use reduced-rank methods, knowledge-aided covariance models, shrinkage estimators, low-rank plus sparse decompositions and SBL. The 2024 SBL-STAP result [6] demonstrates the broader trend: innovative radar algorithms increasingly focus not only on better asymptotic performance, but on maintaining useful performance when the assumptions required by the optimum processor are violated.

2.3 Deep learning for target detection and recognition

Deep-learning radar processing is most mature in classification tasks in which the input has a regular structure. CNNs are effective on SAR images and range-Doppler maps, while one-dimensional networks can operate directly on HRRP or Doppler sequences. Vision Transformers and attention-based architectures are attractive because

they model long-range dependencies rather than relying only on local convolution kernels. The literature review by Jiang et al. shows that deep-learning radar target recognition has been investigated for motion, micro-motion, HRRP, SAR and ISAR representations [4]. Geng et al. similarly emphasize applications in ATR, waveform recognition and clutter/jamming processing, while also warning that limited training data and adversarial examples can severely limit real-world performance [3].

Ma, Egiazarian and Chen proposed a two-channel Vision Transformer for low-resolution radar target classification based on single-frame micro-Doppler information. Their method fuses short-time Fourier transform and bispectrum-derived features so that a decision can be produced from one radar frame rather than from a long observation sequence [7]. A subsequent 2025 study by Ma and Chen presented a one-dimensional cascaded denoising-and-classification framework in which a DnCNN-style denoiser and an AlexNet-based classifier are jointly optimized for weak or noisy micro-Doppler spectra [11]. These studies illustrate two current directions: attention-based feature learning and joint optimization of preprocessing with classification.

2.4 Transformers for tracking and multi-target association

The transformer attention mechanism maps queries, keys and values through

$$\text{Attention}(\mathbf{Q},\mathbf{K},\mathbf{V}) = \text{softmax}\left(\frac{\mathbf{Q}\mathbf{K}^T}{\sqrt{d_k}}\right)\mathbf{V} \tag{5}$$

where:

Q – query matrix;

K – key matrix;

V – value matrix;

d_k – key-vector dimension;

softmax(·) – normalized exponential weighting.

For radar tracking, attention can encode relations between observations separated in time and can reduce the dependence on a fixed motion model. Zhang et al. proposed the TrMTT transformer model for strongly maneuvering targets. The model learns correlations among states and uses encoder-decoder attention to infer the transition of rapidly changing target motion [8]. This is particularly relevant where constant-velocity, constant-acceleration or interacting-multiple-model filters have difficulty adapting quickly enough to abrupt maneuvers.

Transformer models are also being applied directly to radar multi-object tracking. Dell et al. proposed RadarMOTR, which combines conventional radar object detection with transformer-based association on range-Doppler data [9]. In their reported experiment, the model achieved 78.9% HOTA and an association accuracy improvement of 10.4 percentage points relative to a linear Kalman-filter baseline on the evaluated range-Doppler dataset [9]. This result should not be treated as a universal performance gain, but it demonstrates that learned association can exploit contextual relations that are not represented by nearest-neighbor or simple gating logic.

Graph neural networks extend this idea by representing detections or tracks as nodes and candidate associations as edges. Such models are attractive in dense multi-target scenes because the decision for one track can be conditioned on the geometry and

temporal behavior of neighboring tracks. In military surveillance, however, data scarcity and domain shift remain major obstacles: a graph model trained on one sensor, scan strategy, target mix or geography may not transfer reliably to another without calibration.

2.5 Deep unfolding and model-driven neural processing

A major limitation of purely data-driven networks is that they can learn spurious correlations and may require large representative datasets. Deep unfolding provides a compromise: an iterative optimization algorithm is mapped into a fixed number of network stages, and selected parameters are learned while the physical structure of the original estimator is preserved. This creates interpretable layers and often reduces the number of iterations required at inference time.

Zhao et al. proposed a memory-augmented deep-unfolding network for sparse SAR imaging in maritime environments [10]. The network combines algorithmic unfolding with short- and long-term memory mechanisms between stages to preserve information during iterative reconstruction. The importance of this approach is broader than SAR imaging. Similar architectures can be constructed for sparse detection, interference suppression, deconvolution and parameter estimation. For radar engineering, model-driven networks are especially attractive because they permit explicit insertion of known propagation, array, waveform and noise structure rather than forcing a network to learn these relations from data.

3 Cognitive Radar and Reinforcement Learning

The concept of cognitive radar introduced by Haykin is based on intelligent signal processing, a feedback path from receiver to transmitter, and preservation of information through a perception-action cycle [2]. Modern reinforcement-learning methods provide an algorithmic mechanism for implementing this closed loop. Rather than optimizing one dwell independently, the radar can treat waveform selection, dwell allocation, bandwidth, power or revisit interval as sequential decisions whose current action affects future tracking uncertainty.

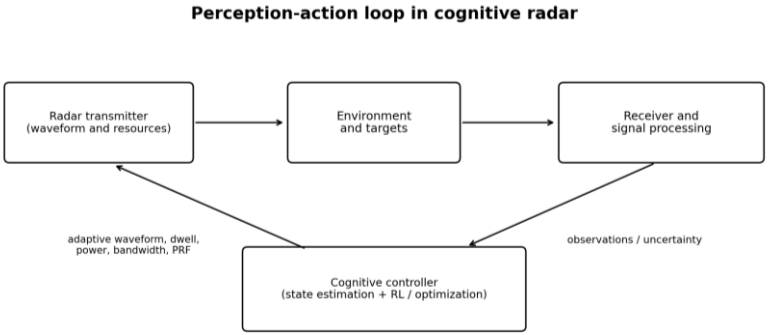


Figure 3: Perception-action loop used in cognitive radar and reinforcement-learning resource management.

For a policy π with state s_t, action a_t and reward r_t, a generic discounted objective is

$$\pi^* = \arg\max_{\pi} \mathbb{E}_{\pi}\left[\sum_{t=0}^{\infty} \gamma^t r_t\right] \tag{6}$$

where:

π – radar control policy;

s_t – estimated state of the environment at time t;

a_t – selected radar action, such as waveform or dwell allocation;

r_t – reward representing tracking quality, resource use, detection performance or a combination of objectives;

γ – discount factor, $0 \leq \gamma < 1$.

Zhu et al. formulated cognitive-radar waveform selection for maneuvering-target tracking as a learning problem and proposed reinforcement-learning methods that update the transmitted waveform as the estimated target state changes [12]. Qin et al. subsequently modeled waveform resource management as a partially observable Markov decision process and used an LSTM-based twin-delayed deep deterministic policy-gradient algorithm. Their simulations showed improved tracking behavior and reduced processing time for waveform-parameter selection within the studied scenario [13].

The operational significance is that radar processing is no longer a one-way chain from receiver to display. Information extracted by detection and tracking can modify the future sensing action. This is particularly useful when radar resources are limited, multiple targets compete for dwell time, or the electromagnetic environment changes faster than a fixed scan schedule can adapt. The major risk is that reinforcement-learning policies can behave unpredictably outside the training distribution. Therefore, practical cognitive radar should use constrained action spaces, safety rules, deterministic fallback modes, and continuous monitoring of model confidence.

4 Proposed Hybrid Processing Architecture

The analysis above suggests that the most robust next-generation architecture is a hybrid model-driven chain rather than a fully end-to-end neural receiver. Figure 4 illustrates such an architecture. The first stages retain calibration, matched filtering and Doppler processing because these operations are directly related to the transmitted waveform and are highly efficient. Adaptive clutter suppression is then performed with SBL-STAP or another data-efficient covariance estimator. Sparse-recovery or deep-unfolding modules can operate on the resulting range-angle-Doppler cube to enhance weak structured components. Classification and track association are delegated to attention-based networks, while a separate model-quality monitor evaluates CFAR statistics, uncertainty and out-of-distribution indicators. Finally, a cognitive resource manager closes the loop to the transmitter.

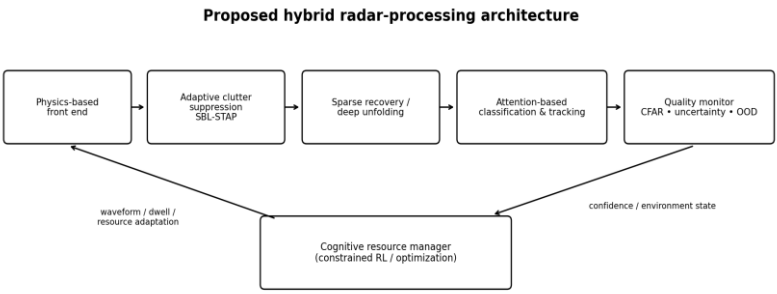


Figure 4: Proposed hybrid architecture combining physics-based processing, learned inference and cognitive feedback.

A convenient way to combine heterogeneous confidence measures is to retain them separately rather than compressing all evidence into one opaque neural score. For example, a fused decision statistic can be written as

$$S_{\text{fused}} = w_1 S_{\text{CFAR}} + w_2 S_{\text{sparse}} + w_3 S_{\text{DL}}, \qquad \sum_{i=1}^{3} w_i = 1 \tag{7}$$

where:

S_{fused} – fused decision statistic;

S_{CFAR} – normalized classical detection evidence;

S_{sparse} – normalized evidence from sparse reconstruction or Bayesian estimation;

S_{DL} – normalized neural-network confidence;

w_i – scenario-dependent non-negative weights.

Equation (7) is not proposed as a universal optimal detector. Its purpose is architectural: separate evidence channels make it possible to inspect disagreements. If the neural classifier is confident but CFAR and sparse reconstruction are inconsistent with the detection, the system can flag the observation for additional dwell time or human review rather than automatically promoting the track.

4.1 Processing logic

The proposed chain can be summarized in five stages. First, the front end produces calibrated I/Q data and performs waveform-matched operations. Second, an adaptive interference processor estimates clutter statistics with conventional or sparse-Bayesian techniques. Third, detection is performed with a combination of physically interpretable thresholds and structured reconstruction. Fourth, classification and tracking are performed with CNN/ViT/Transformer modules that exploit spatial-temporal context. Fifth, a cognitive controller allocates future sensing resources based on uncertainty rather than only on the current track existence probability.

This arrangement has three advantages. Interpretability: the signal can be inspected at several physically meaningful intermediate representations. Graceful degradation: if a learned module is unavailable or outside its validated domain, the radar can revert to classical processing. Data efficiency: learning is concentrated where the analytical model

is weakest, rather than spending training data on deterministic operations such as matched filtering.

5 Comparative Assessment of Algorithmic Approaches

Table 1 compares representative algorithm families. The assessment is qualitative because the cited studies use different datasets, sensors and performance metrics. Direct numerical ranking across papers would therefore be misleading.

Table 1: Qualitative comparison of radar-processing algorithm families.

Algorithm family	Primary task	Main advantage	Main limitation
Matched filtering / FFT / CFAR	Detection and measurement	Strong physical basis; low latency	Sensitive to model mismatch and nonhomogeneous backgrounds
STAP	Clutter and interference suppression	Joint spatial-temporal adaptation	Requires representative covariance statistics
Sparse recovery / SBL	Detection, imaging, covariance estimation	Exploits sparsity; data-efficient estimation	Dictionary mismatch and iterative computational cost
CNN / ViT	Classification and recognition	Learns discriminative target signatures	Requires representative labeled data
Transformer / GNN	Maneuvering-target tracking and association	Models long-range temporal and relational context	Data/compute intensive; uncertain extrapolation
Deep unfolding	Imaging and inverse problems	Model structure plus learnable parameters	Depends on validity of the unfolded model
Cognitive radar / RL	Waveform and resource management	Closed-loop adaptation	Policy safety, validation and generalization

Recent literature provides concrete examples of these trends. Cao et al. show that SBL can be used to construct reduced-dimension STAP from a single training sample in a strongly heterogeneous simulated clutter case [6]. Ma et al. demonstrate single-frame ViT classification using measured micro-Doppler data [7]. Zhang et al. use a transformer architecture for highly maneuvering target tracking [8]. RadarMOTR reports 78.9% HOTA and a 10.4 percentage-point gain in association accuracy over its linear Kalman baseline on the reported dataset [9]. Zhao et al. combine sparse SAR reconstruction with memory-augmented deep unfolding [10], while Ma and Chen demonstrate a 2025 cascaded denoising-and-classification framework designed for weak single-frame micro-Doppler signatures [11]. In cognitive radar, reinforcement-learning methods are being used to select waveforms and trade tracking performance against resource consumption [12, 13].

These examples show that the word *innovative* does not correspond to one algorithm. Innovation is occurring simultaneously in adaptive statistics, sparse inference, representation learning, sequence modeling, optimization and closed-loop control.

6 Verification, Robustness and Implementation Challenges

6.1 Dataset scarcity and domain shift

Radar data differ fundamentally from internet-scale visual datasets. High-quality labeled radar measurements are expensive, sensor-specific and frequently restricted. A classifier trained on one waveform, frequency band, antenna configuration or site can learn features that are not invariant to a new system. Deep-learning radar surveys identify limited representative training data as one of the principal obstacles to deployment [3, 4]. This problem is amplified in military applications, where the most important target classes may be rare and realistic electronic-warfare conditions may be difficult to reproduce.

6.2 Uncertainty and out-of-distribution detection

A neural-network softmax value is not automatically a calibrated probability. In a safety-critical radar system, the processing chain should estimate both aleatoric uncertainty caused by measurement noise and epistemic uncertainty caused by insufficient training coverage. Out-of-distribution detection is particularly important for new target types, unusual interference, sensor faults and novel tactics. A practical architecture should therefore retain conventional quality indicators such as SNR/SCNR, track innovation residuals, covariance consistency, CFAR background estimates and measurement geometry alongside neural confidence.

6.3 Adversarial and electronic-warfare robustness

Radar neural networks can be affected not only by ordinary domain shift but also by intentionally structured interference. Geng et al. explicitly identify adversarial examples as a major concern for deep-learning radar processing [3]. Robust training, randomized preprocessing, physically constrained feature extraction and multi-model verification can reduce risk, but no purely software-based defense can guarantee robustness to an adaptive adversary. For that reason, innovative AI modules should complement rather than eliminate classical signal-consistency checks.

6.4 Real-time implementation

Transformers and iterative sparse solvers can demand substantial memory bandwidth and compute. This matters because radar processing often has strict latency requirements and must operate continuously. Reduced-dimension STAP [6], one-dimensional micro-Doppler networks [11], pruning, quantization, tensor accelerators, FPGA/SoC deployment and heterogeneous CPU-GPU processing are relevant engineering directions. The design objective should not be maximum classification accuracy in isolation, but a Pareto trade-off among accuracy, latency, energy, memory and robustness.

6.5 Verification path

A defensible verification program should proceed in four levels. **Level 1:** analytical verification using limiting cases and synthetic signals whose true parameters are known. **Level 2:** Monte Carlo simulation with statistically controlled clutter, noise, interference and maneuver models. **Level 3:** recorded-data replay with independent

train/validation/test partitions and cross-site evaluation. **Level 4:** hardware-in-the-loop and field tests with real-time latency measurement. For learned algorithms, the test set should include deliberately shifted conditions rather than only random samples from the same recording session.

7 Recommended Research Experiment

A practical research study suitable for subsequent implementation in MATLAB or Python can compare four processing chains on the same radar data cube:

1. Baseline: matched filter → Doppler FFT → CA-CFAR → Kalman/IMM tracking;
2. Sparse adaptive chain: matched filter → SBL-STAP → sparse detector → Kalman/IMM;
3. Learned chain: matched filter → range-Doppler tensor → CNN/ViT detector/classifier transformer track association;
4. Hybrid cognitive chain: SBL-STAP + classical detector + transformer association + reinforcement-learning resource manager.

The principal evaluation indicators should be probability of detection, false-alarm rate, track continuity, position/velocity RMSE, association accuracy, processing latency, memory consumption and sensitivity to clutter nonhomogeneity. For classification, balanced accuracy and confusion matrices should be reported rather than only overall accuracy. For the cognitive controller, performance should be presented jointly with resource use—for example, tracking RMSE versus dwell time or transmitted energy.

The experiment should not assume that the neural architecture will outperform the classical chain in every condition. The scientifically important result is the boundary of applicability: the SNR region, maneuver severity, clutter heterogeneity, target density and data volume at which each algorithm becomes advantageous. This comparison would provide a strong basis for a later dissertation chapter or a follow-on experimental paper.

Conclusion

Radar-information processing is moving from a sequence of fixed statistical algorithms toward a hybrid architecture that combines physical signal models with learned representations and adaptive decision-making. Sparse recovery and sparse Bayesian learning are particularly valuable when the scene is sparse or when homogeneous training samples are insufficient. Transformer and ViT architectures can extract long-range temporal or feature relationships for classification and tracking, while graph-based methods can improve association in dense multi-target scenarios. Deep unfolding offers a technically attractive middle ground between iterative optimization and black-box neural processing. Cognitive radar closes the loop by using the estimated environment to select future waveform and resource actions.

The proposed hybrid architecture therefore retains a physics-based front end, introduces SBL-STAP and sparse/deep-unfolding processing at the interference and reconstruction stages, uses attention-based networks for recognition and tracking, monitors uncertainty and out-of-distribution behavior, and employs constrained reinforcement learning only for bounded resource decisions. Future work should

implement this architecture in a reproducible simulation and recorded-data framework, quantify the computational cost, and determine the conditions under which each innovative algorithm produces a statistically significant operational benefit.

References

1. Richards, M. A. (2014). Fundamentals of Radar Signal Processing (2nd ed.). McGraw-Hill Education.
2. Haykin, S. (2006). Cognitive radar: A way of the future. IEEE Signal Processing Magazine, 23(1), 30–40. https://doi.org/10.1109/MSP.2006.1593335
3. Geng, Z., Yan, H., Zhang, J., & Zhu, D. (2021). Deep-learning for radar: A survey. IEEE Access, 9, 141800–141818. https://doi.org/10.1109/ACCESS.2021.3119561
4. Jiang, W., Wang, Y., Li, Y., Lin, Y., & Shen, W. (2023). Radar target characterization and deep learning in radar automatic target recognition: A review. Remote Sensing, 15(15), 3742. https://doi.org/10.3390/rs15153742
5. Quan, Y., Wu, Y., Duan, L., Xu, G., Xue, M., Liu, Z., & Xing, M. (2024). A review of radar signal processing based on sparse recovery. Journal of Radars, 13(1), 46–67. https://doi.org/10.12000/JR23211
6. Cao, J., Wang, T., & Wang, D. (2024). Beam-space post-Doppler reduced-dimension STAP based on sparse Bayesian learning. Remote Sensing, 16(2), 307. https://doi.org/10.3390/rs16020307
7. Ma, B., Egiazarian, K., & Chen, B. (2023). Low-resolution radar target classification using Vision Transformer based on micro-Doppler signatures. IEEE Sensors Journal, 23(22), 28474–28485. https://doi.org/10.1109/JSEN.2023.3322684
8. Zhang, Y., Li, G., Zhang, X.-P., & He, Y. (2024). A deep learning model based on transformer structure for radar tracking of maneuvering targets. Information Fusion, 103, 102120. https://doi.org/10.1016/j.inffus.2023.102120
9. Dell, M., Bradfisch, W., Schober, S., & Klöck, C. (2024). RadarMOTR: Multi-object tracking with transformers on range-Doppler maps. In 2024 International Radar Conference (RADAR). IEEE. https://doi.org/10.1109/RADAR58436.2024.10994166
10. Zhao, Y., Ou, C., Tian, H., Ling, B. W.-K., Tian, Y., & Zhang, Z. (2024). Sparse SAR imaging algorithm in marine environments based on memory-augmented deep unfolding network. Remote Sensing, 16(7), 1289. https://doi.org/10.3390/rs16071289
11. Ma, B., & Chen, B. (2025). A 1D cascaded denoising and classification framework for micro-Doppler-based radar target recognition. Remote Sensing, 17(9), 1515. https://doi.org/10.3390/rs17091515
12. Zhu, P., Liang, J., Luo, Z., & Shen, X. (2023). Waveform selection method of cognitive radar target tracking based on reinforcement learning. Journal of Radars, 12(2), 412–424. https://doi.org/10.12000/JR22239

13. Qin, J., Zhu, M., Pan, Z., Li, Y., & Li, Y. (2023). Memory-based deep reinforcement learning for cognitive radar target tracking waveform resource management. IET Radar, Sonar & Navigation, 17(12), 1822–1836. https://doi.org/10.1049/rsn2.12469

ANALYSIS AND MATHEMATICAL MODELING OF AIR AND MISSILE DEFENSE SYSTEMSWITH EMPHASIS ON THE RADAR EQUATION

Matei K. Kirov, Vencislav M. Vasilev, Vladislava S. Georgieva

Department of Air Defense, Artillery, Air Defense and CIS Faculty at the Vasil Levski National Military University, Shumen, Bulgaria, mkkirov@nvu.bg, venci_vass@abv.bg, vladgs_93@abv.bg

Abstract: *This paper presents an analytical framework for modeling air and missile defense (AMD) as a chain of sensing, decision, and engagement processes. The radar equation is used as the physical basis for estimating detection range and is coupled with probabilistic detection models, layered-defense reliability, Erlang-B channel saturation, constrained resource allocation, and a reproducible Monte Carlo simulation framework. The resulting framework is transparent, traceable to standard radar and defense-modeling literature, and suitable for sensitivity analysis and subsequent simulation studies.*

Keywords: *radar equation, air defense, missile defense, mathematical modeling, detection probability, Erlang B, resource allocation, Monte Carlo simulation*

Introduction

Modern air and missile defense (AMD) systems combine surveillance and fire-control sensors, command-and-control functions, identification processes, and weapon systems. Radar performance is a necessary but not sufficient condition for overall defensive effectiveness: target detection, track quality, decision time, engagement capacity, interceptor performance, and the interaction among multiple defensive layers all contribute to the final outcome. The monostatic radar equation provides the basic physical relationship between transmitted power, antenna gain, wavelength, target radar cross section (RCS), receiver noise, and signal-to-noise ratio (SNR) at a given range [1–3].

At system level, the same physical model can be embedded in probabilistic and operations-research formulations. Combat modeling literature uses probability, queueing, optimization, and stochastic simulation to quantify weapon effectiveness and resource limitations, while NATO modeling-and-simulation practice emphasizes explicit assumptions, verification, validation, and reproducibility [4–7]. Accordingly, this paper first establishes a consistent radar-detection model, then connects it to engagement-chain, layered-defense, saturation, resource-allocation, and Monte Carlo models. The numerical examples are illustrative and are not intended to represent the performance of any specific operational system.

1 Radar Detection Model

1.1 Classical radar equation and maximum detection range

Radar systems are widely used in various fields to determine the range, velocity, and azimuth of targets [8]. For a monostatic radar using the same antenna for transmission and reception, a convenient single-pulse SNR form of the radar equation is given by Eq. (1). The expression is idealized: propagation, scan, polarization, processing,

implementation, and other losses are represented by the aggregate factor L. The receiver noise is expressed using the standard reference temperature T_0 and noise factor F. If an equivalent system noise temperature T_s is used instead, F should not be applied again, because doing so can double count receiver noise [1, 2].

$$R_{max} = \sqrt[4]{\frac{P_t G^2 \lambda^2 \sigma}{(4\pi)^3 \, k \, T_0 \, B \, F \, L \, \gamma_{min}}} \qquad (1)$$

where*:*

R_{max} – maximum detection range, m;
P_t – peak transmitted power, W;
G – linear antenna gain;
λ – radar wavelength, m;
σ – target radar cross section (RCS), m²;
k – Boltzmann constant, 1.380649×10^{-23} J/K;
T_0 – reference noise temperature, K;
B – receiver noise bandwidth, Hz;
F – receiver noise factor in linear form;
L – aggregate system-loss factor in linear form;
γ_{min} – minimum required linear SNR at the detector input.

Equation (1) shows the characteristic fourth-root dependence of detection range on transmitted power and target RCS. For a monostatic radar, antenna gain appears in both the transmit and receive paths, so the ideal range varies as $G^{1/2}$ rather than $G^{1/4}$ [1–3].

Table 1: Illustrative parameter set used for the radar-range calculation.

Parameter	Symbol	Value
Peak transmitted power	P_t	1 MW
Antenna gain	G	40 dB = 10^4
Wavelength	λ	0.03 m (10 GHz)
Illustrative target RCS	σ	0.1 m²
Reference noise temperature	T_0	290 K
Receiver noise bandwidth	B	1 MHz
Noise factor	F	3 dB ≈ 2
Aggregate loss	L	1 (idealized)
Required SNR	γ_{min}	13.18 dB ≈ 20.81

Using the parameters in Table 1 and the nonfluctuating single-pulse threshold corresponding to $P_D = 0.9$ and $P_{FA} = 10^{-6}$, Eq. (1) gives $R_{max} \approx 72.2$ km for $\sigma = 0.1$ m² and $R_{max} \approx 128.4$ km for $\sigma = 1$ m². A tenfold change in RCS changes range by the factor $10^{1/4} \approx 1.78$, provided all other parameters remain unchanged.

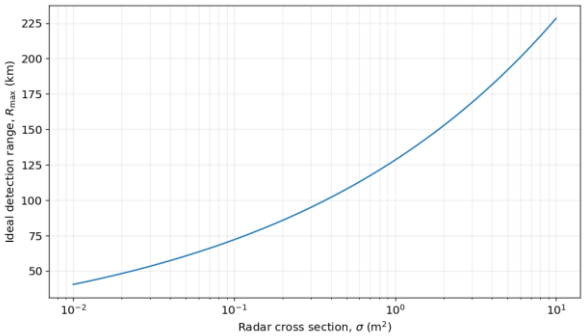


Figure 1: Ideal detection range as a function of target RCS for the illustrative parameter set in Table 1.

1.2 Detection probability and false-alarm probability

Radar detection is statistical. For a single nonfluctuating target observed by a square-law detector, the detection probability can be expressed through the first-order Marcum Q-function as in Eq. (2), where γ is the linear SNR [1, 3]. This expression should not be labeled as a Swerling-I model. For a single pulse from a target whose instantaneous power follows the exponential fluctuation model associated with Swerling I/II statistics, Eq. (3) is a common closed-form relation. Multi-pulse noncoherent integration requires the appropriate target-fluctuation and integration model rather than simply multiplying SNR by the number of pulses inside Eq. (2).

$$P_D = Q_1(\sqrt{2\gamma}, \sqrt{-2\ln P_{FA}}) \tag{2}$$

where*:*

P_D – probability of detection;
Q_1 – first-order Marcum Q-function;
γ – linear signal-to-noise ratio (SNR);
P_{FA} – probability of false alarm.

$$P_D = exp\left[\frac{ln\,(P_{FA})}{1+\gamma}\right] = P_{FA}^{\frac{1}{1+\gamma}} \tag{3}$$

where*:*

P_D – single-pulse probability of detection for the exponential target-power fluctuation model;
P_{FA} – probability of false alarm;
γ – linear SNR;
exp – exponential function;
ln – natural logarithm.

For Eq. (2), $P_{FA} = 10^{-6}$ and $P_D = 0.9$ require $\gamma \approx 20.81$, or 13.18 dB. The SNR at another range R follows directly from the fourth-power propagation dependence in Eq. (4).

$$\gamma(R) = \gamma(R_0) \cdot \left(\frac{R_0}{R}\right)^4 \tag{4}$$

where*:*

$\gamma(R)$ – linear SNR at range R;
$\gamma(R_0)$ – linear SNR at the reference range R_0;
R – target range;
R_0 – reference range.

Table 2: Detection probability versus range for a normalized reference range $R_0 = 100$ km, with $P_D(R_0) = 0.9$ and $P_{FA} = 10^{-6}$ under the nonfluctuating single-pulse model.

R (km)	Relative SNR	P_D
50	16.000 (+12.0 dB)	1.000
80	2.441 (+3.9 dB)	1.000
100	1.000 (+0.0 dB)	0.900
120	0.482 (-3.2 dB)	0.251
150	0.198 (-7.0 dB)	0.012

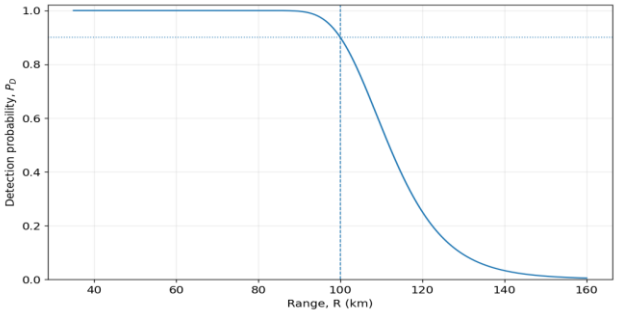


Figure 2: Detection probability versus range for the normalized nonfluctuating-target example.

2 Engagement-Chain Model

2.1 Timing of detection, tracking, identification, decision, and engagement

A system-level model should represent the sequence from detection to engagement as a set of time-dependent processes. The total reaction time may be written as the sum of sensor, tracking, identification, decision, and interceptor-flight components. In practice, these quantities are system- and scenario-specific and may be correlated; consequently, the values in Table 3 are only illustrative inputs for a simulation model rather than representative performance data [4, 5].

Table 3: Illustrative timing inputs for an engagement-chain model (seconds).

Stage	Symbol	Mean	Range
Detection	τ_{det}	0.5	0.2–2.0
Tracking	τ_{track}	1.0	0.5–3.0
Identification / IFF	τ_{id}	0.3	0.1–1.0
Assessment and decision	τ_{dec}	2.0	1.0–5.0
Interceptor flight	τ_{fly}	10.0	5.0–30.0
Total	T_{total}	13.8	6.8–41.0

2.2 Single-shot and salvo engagement probability

Let P_{ss} denote the probability that the interceptor reaches a valid engagement state and $P_{k|ss}$ the conditional probability of a kill given that state. The effective single-shot probability is $P_{hit} = P_{ss} \cdot P_{k|ss}$. If n statistically independent shots with identical P_{hit} are taken against the same target, the probability of at least one successful kill is given by Eq. (5). The independence assumption is important; common guidance, sensing, environmental, or target-behavior effects can make the outcomes correlated [4, 5].

$$P_{kill} = 1 - (1 - P_{hit})^n \tag{5}$$

where**:**

P_{kill} – probability of at least one successful kill;
P_{hit} – effective single-shot kill probability;
n – number of statistically independent shots.

3 System-Level Models

3.1 Layered defense

For L defensive layers, if layer l independently stops a target with probability p_l, the probability that the target penetrates every layer is given by Eq. (6). This compact model is useful for sensitivity analysis, but it can overestimate the benefit of layering when failures are correlated or when layers share sensors, command links, engagement zones, or other common resources. [4, 5, 7]

$$P_{leak} = \prod_{l=1}^{L}(1 - p_l) \tag{6}$$

where**:**

P_{leak} – probability that a target penetrates all defensive layers;
L – number of defensive layers;
p_l – probability that layer l stops the target;
l – layer index.

Table 4: Leak probability for identical, independent layers.

L	p = 0.6	p = 0.8	p = 0.9
1	0.4000	0.2000	0.1000
2	0.1600	0.0400	0.0100
3	0.0640	0.0080	0.0010
4	0.0256	0.0016	0.0001

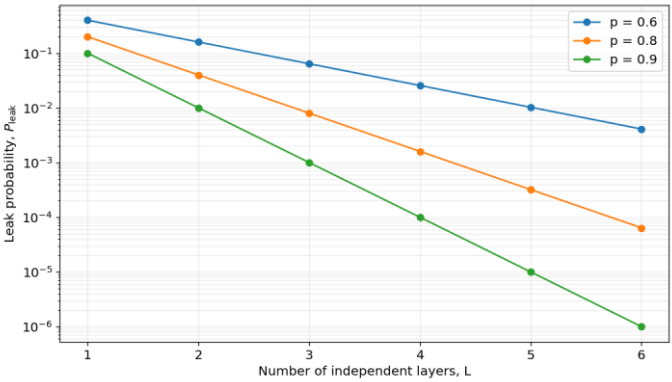


Figure 3: Multiplicative reduction in leak probability for identical independent defensive layers.

3.2 Saturation and blocking: Erlang-B approximation

A simple way to approximate saturation is to model C simultaneous engagement channels as an M/M/C/C loss system. Targets arrive according to a Poisson process, channel holding times are exponentially distributed, and no waiting queue is available. With offered traffic $\rho = \lambda_a/\mu$, where λ_a is the target-arrival rate and μ is the service rate per channel, the blocking probability is given by the Erlang-B formula in Eq. (7). The model is analytically convenient but does not capture geometry, finite engagement windows, re-engagement logic, inventory depletion, or prioritized scheduling. [5–7]

$$P_{block} = \frac{\frac{\rho^C}{C!}}{\sum_{k=0}^{C} \frac{\rho^k}{k!}}, \quad \rho = \frac{\lambda_a}{\mu} \tag{7}$$

where**:**

P_{block} – Erlang-B blocking probability;
ρ – offered traffic, in erlangs;
C – number of simultaneous engagement channels;
λ_a – target-arrival rate, s^{-1};

μ – service rate per channel, s^{-1};
k – summation index.

Table 5: Corrected Erlang-B blocking probabilities for selected channel counts and offered loads.

C	ρ	P_{block}
4	2.0	0.095
4	3.0	0.206
6	3.0	0.052
6	4.0	0.117
8	4.0	0.030
8	6.0	0.122
12	8.0	0.051
12	10.0	0.120

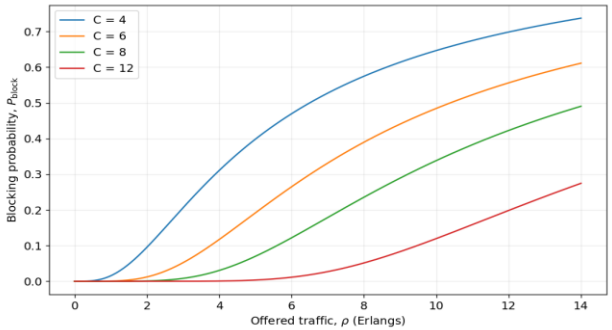


Figure 4: Erlang-B blocking probability as a function of offered traffic for several channel counts.

3.3 Constrained resource allocation

Suppose object i has importance weight w_i and residual vulnerability $Q_i(r_i)$ after assigning a continuous resource amount r_i. A stylized resource-allocation problem maximizes total weighted protection subject to a common resource budget R. For $Q_i(r_i) = \exp(-\alpha_i r_i)$, the continuous Karush–Kuhn–Tucker solution is given by Eq. (8), where ν is selected so that the resource constraint is satisfied for all active allocations. This result is a continuous relaxation; integer interceptor, launcher, and crew assignments require discrete or mixed-integer optimization [5].

$$r_i = max\left\{0, \frac{1}{\alpha_i} ln\left(\frac{\alpha_i w_i}{\nu}\right)\right\} \quad (8)$$

where:

r_i – optimal continuous resource allocated to object i;
α_i – resource-effectiveness coefficient for object i;
w_i – importance weight of object i;
ν – Karush–Kuhn–Tucker multiplier chosen to satisfy the resource constraint;
i – object index.

4 Monte Carlo Simulation Framework

Monte Carlo simulation is appropriate when detection, tracking, engagement, channel availability, and target arrival processes interact in ways that make a closed-form solution impractical. A reproducible experiment should define the random variables and their distributions, the number of independent replications N, the random-number seed or seed policy, the service-time model, channel-assignment and re-engagement rules, interceptor inventory, target mix, and termination criterion. Model verification should be separated from validation, and simple limiting cases should be checked against analytical results such as Eqs. (5)–(7) [6, 7].

For a scalar output X observed across independent replications, an approximate large-sample 95% confidence interval for the mean is given by Eq. (9). For an estimated event probability $\hat{p}$, Eq. (10) provides the familiar normal approximation, although Wilson or exact binomial intervals are preferable when probabilities are close to zero or one or when N is small [6]. Numerical Monte Carlo results should not be reported without these reproducibility parameters, because confidence intervals cannot be checked from summary values alone.

$$CI_{95\%} \approx \bar{x} \pm 1.96 \cdot \frac{s}{\sqrt{N}} \tag{9}$$

where**:**

$CI_{95\%}$ – approximate 95% confidence interval for the mean;
$\bar{x}$ – sample mean of the simulated output;
s – sample standard deviation;
N – number of independent simulation replications;
1.96 – 97.5th percentile of the standard normal distribution.

$$CI_{95\%}(\hat{p}) \approx \hat{p} \pm 1.96 \sqrt{\frac{\hat{p}(1-\hat{p})}{N}} \tag{10}$$

where**:**

$CI_{95\%}(\hat{p})$ – approximate 95% confidence interval for an estimated event probability;
$\hat{p}$ – estimated event probability;
N – number of independent simulation replications;
1.96 – 97.5th percentile of the standard normal distribution.

5 Discussion and Sensitivity Analysis

The corrected equations clarify several sensitivities that are easy to misstate. First, ideal radar range varies as $P_t^{1/4}$ and $\sigma^{1/4}$, but as $G^{1/2}$ for a monostatic radar because antenna

gain acts on both the transmitted and received signal. Second, layered defense can reduce leak probability rapidly only under the independence assumption; common-mode failures can substantially reduce this benefit. Third, Erlang-B blocking is governed jointly by the offered traffic and the number of channels, so there is no universal rule that C must be "significantly larger" than ρ. Capacity should instead be selected against a target blocking probability and the validity of the loss-system assumptions. [1–3, 5, 6]

Finally, no single parameter can be declared universally "most cost-effective" without an explicit cost model, engagement geometry, inventory constraints, and operational objectives. Increasing radar power, antenna gain, engagement channels, or defensive layers affects different parts of the kill chain and may shift the system bottleneck. The value of the presented framework is therefore not a prescriptive design rule, but a consistent set of equations that can be used for sensitivity studies and for verification of more detailed simulation models.

Table 6: Summary of parameter sensitivities in the corrected analytical model.

Parameter	Effect
Transmit power P_t	$R_{max} \propto P_t^{1/4}$ in the ideal radar equation
Antenna gain G	$R_{max} \propto G^{1/2}$ for a monostatic radar
Target RCS σ	$R_{max} \propto \sigma^{1/4}$
Independent layers L	P_{leak} decreases multiplicatively
Engagement channels C	P_{block} decreases according to Erlang B for fixed ρ
Arrival rate λ_a	Raises ρ and therefore P_{block} for fixed μ and C
Single-shot P_{hit}	$P_{kill} = 1 - (1 - P_{hit})^n$; nonlinear for $n > 1$

Conclusion

The radar equation provides a defensible physical foundation for mathematical modeling of air and missile defense, but system-level conclusions require consistent probabilistic, capacity, and engagement assumptions. This paper combined a corrected radar-range formulation with detection statistics, engagement probability, layered-defense reliability, Erlang-B saturation, continuous resource allocation, and a reproducible Monte Carlo methodology. The numerical examples show the fourth-root sensitivity to power and RCS, the square-root sensitivity to monostatic antenna gain, and the strong dependence of blocking and penetration probabilities on system architecture and model assumptions. Future work should add propagation and clutter losses, sensor fusion, correlated layer failures, inventory-constrained engagement scheduling, cyber resilience, and validated adaptive resource-allocation methods.

References

1. Skolnik, M. I. (2001). Introduction to radar systems (3rd ed.). McGraw-Hill;
2. Barton, D. K. (2005). Radar system analysis and modeling. Artech House;

3. Richards, M. A. (2014). Fundamentals of radar signal processing (2nd ed.). McGraw-Hill Education;
4. Washburn, A. R., & Kress, M. (2009). Combat modeling. Springer. https://doi.org/10.1007/978-1-4419-0790-5;
5. Przemieniecki, J. S. (2000). Mathematical methods in defense analyses (3rd ed.). American Institute of Aeronautics and Astronautics. https://doi.org/10.2514/4.862137;
6. Law, A. M. (2015). Simulation modeling and analysis (5th ed.). McGraw-Hill Education;
7. North Atlantic Treaty Organization Science and Technology Organization. (2013). M&S support to transitioning forces and emerged/emerging disruptive M&S technologies (STO-MP-MSG-111). NATO STO;
8. Parvanov, St., Georgiev, G, Kozarev, K. (2022). "Techniques for the Protection of Key Sites Against Unmanned Aerial Vehicles", Ruse, Proceedings of the University of Ruse – 2022, Vol. 61, Session 3.2, pp. 207–216, 2G.302-2-CCT2-10, ISSN 1311-3331.

MATHEMATICAL MODEL FOR ASSESSING THE EFFECTIVENESS OF INTEGRATED AIR AND MISSILE DEFENSE IN MULTI-DOMAIN OPERATIONS

Matei K. Kirov, Stanimir H. Parvanov

Department of Air Defense, Artillery, Air Defense and CIS Faculty at the Vasil Levski National Military University, Shumen, Bulgaria,
mkkirov@nvu.bg, shparvanov@aadcf.nvu.bg

Abstract: *This paper develops a transparent mathematical framework for assessing Integrated Air and Missile Defense (IAMD) in the context of Multi-Domain Operations (MDO). The model combines a layered-defense penetration formulation, a force-coverage coefficient, a kinematic time-to-engagement relation for high-speed threats, a multiplicative engagement-chain probability, a proposed multi-domain convergence index, and a chronometric decomposition of readiness and combat functions. Several inconsistencies in the source draft are corrected. In particular, the layered model is reformulated so that penetration is the product of layer failures rather than the complement of that product; the publicly documented 2021 M-SHORAD plan of 144 systems for four battalions is distinguished from scenario-specific force requirements; and HBTSS is treated correctly as a tracking sensor that can improve track continuity and fire-control-quality data, not as an interceptor with a directly assignable kill probability. The paper also distinguishes doctrinal MDO functions from illustrative timing assumptions. All numerical effectiveness coefficients that are not publicly supported are explicitly identified as scenario inputs. The resulting model is intended for sensitivity analysis, simulation exercises, and capability-planning studies rather than for estimating classified or system-specific combat performance.*

Keywords: *Multi-Domain Operations, Integrated Air and Missile Defense, A2/AD, layered defense, M-SHORAD, HBTSS, mathematical modeling, convergence*

Introduction

NATO describes Multi-Domain Operations as the orchestration of military activities across five operating domains—land, air, maritime, space, and cyberspace—synchronized with non-military activities to create desired effects [1]. In this environment, Integrated Air and Missile Defense is not a single weapon system but a networked function that depends on sensing, command and control, engagement capacity, interceptor availability, mobility, and coordination across echelons. U.S. Army modernization literature likewise emphasizes layered and integrated air and missile defense, M-SHORAD for maneuver-force protection, and IBCS/AIAMD as an integrating command-and-control architecture [2, 6].

The U.S. Army MDO concept does not define an operation as only three fixed chronological phases. It frames the problem through competition and armed conflict, including the functions of penetrate, dis-integrate, exploit, and re-compete; these actions can overlap in time and space [3]. Accordingly, the models below treat penetration, convergence, readiness, and engagement as analytical components rather than as a literal doctrinal timeline. The numerical examples are deliberately unclassified and illustrative;

they must not be interpreted as verified performance estimates for a named operational system.

1 IAMD Architecture and Modeling Assumptions

1.1 Functional layering in an integrated defense

A useful analytical abstraction is to represent IAMD as a sequence of defensive opportunities linked by a common sensing and command-and-control backbone. The Army describes a layered approach that includes maneuver short-range air defense, indirect fire protection, Patriot-class lower-tier defense, and upper-tier ballistic-missile defense, while AIAMD/IBCS is intended to integrate sensors, weapons, and mission command [2, 6]. The delivery of an eighth U.S. THAAD battery in 2025 illustrates continuing investment in upper-tier ballistic-missile defense capacity [7]. Figure 1 is therefore a functional schematic, not a claim about exact engagement ranges or probabilities.

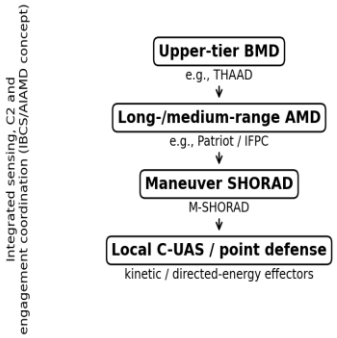


Figure 1: Simplified functional layering of IAMD with an integrated sensing and command-and-control backbone.

Table 1: Functional layers used in the simplified IAMD model.

Layer	Primary analytical role	Treatment in the model
Local point defense / C-UAS	Counter small UAS and local threats	Scenario parameter; no public kill probability assumed
Maneuver SHORAD	Protect maneuver formations	M-SHORAD is publicly documented as a maneuver-protection capability [4]
Short-/medium-range defense	Protect fixed, semi-fixed and maneuver-support assets	Can include IFPC-type functions; model uses generic effectiveness
Long-range / lower-tier AMD	Area air and missile defense	Representative Patriot-class function; no classified performance values used
Upper-tier BMD	Terminal ballistic-missile defense	Representative THAAD-class function [7]

1.2 Assumptions and limits

The analytical model assumes that the effectiveness of each layer can be represented by a normalized conditional stop probability and, where needed, by a scenario-specific degradation term. This abstraction does not reproduce sensor geometry, clutter, electronic warfare, interceptor kinematics, inventory depletion, command latency, or correlated failures. Consequently, all layer probabilities and degradation coefficients are inputs for sensitivity analysis and must be calibrated from validated exercise, test, or simulation data before operational use.

2 Layered A2/AD Penetration Model

Let layer i have a nominal conditional stop probability p_i and an optional scenario degradation factor $\exp(-\lambda_i d_i)$. The effective stop probability of that layer is therefore $p_i \exp(-\lambda_i d_i)$. If layer outcomes are treated as statistically independent, the probability that a threat penetrates all n layers is the product of the layer failure probabilities. This corrects the source draft, in which the complement of that product was labeled as penetration even though it actually represented cumulative stopping probability.

$$P_{pen} = \prod_{i=1}^{n} \left(1 - p_i \, exp(-\lambda_i d_i)\right) \quad (1)$$

where: P_{pen} – probability that the threat penetrates all modeled layers; n – number of modeled defensive layers; p_i – nominal conditional stop probability for layer i; λ_i – scenario degradation coefficient for layer i, in reciprocal distance units when multiplied by distance; d_i – path length or exposure-distance variable associated with layer i; i – layer index.

The complementary cumulative probability that at least one modeled layer stops the threat is given by Eq. (2).

$$P_{stop} = 1 - P_{pen} \quad (2)$$

where: P_{stop} – probability that at least one modeled defensive layer stops the threat; P_{pen} – probability that the threat penetrates all modeled layers.

For sensitivity analysis it is convenient to replace the detailed layer term by a common effective stop probability q. Then $P_{pen} = (1 - q)^n$. Figure 2 shows the strong mathematical benefit of multiple independent layers; however, this benefit is reduced when layers share sensors, communications, decision logic, or other common failure modes.

Table 2: Penetration probability for identical independent effective layers.

n	q = 0.4	q = 0.6	q = 0.8
1	0.6000	0.4000	0.2000
2	0.3600	0.1600	0.0400
3	0.2160	0.0640	0.0080
4	0.1296	0.0256	0.0016
5	0.0778	0.0102	0.0003
6	0.0467	0.0041	0.0001

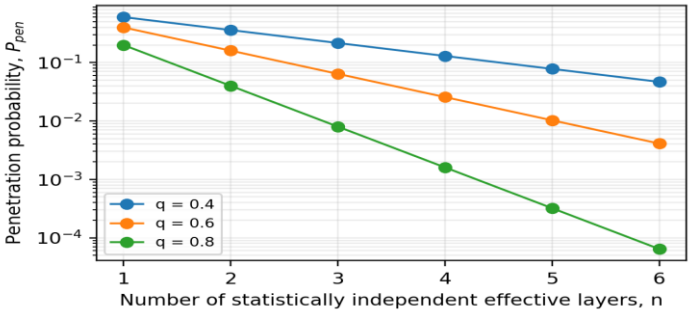


Figure 2: Sensitivity of penetration probability to the number of statistically independent effective layers.

3 M-SHORAD Capacity as a Force-Structure Constraint

The source draft stated that three available M-SHORAD battalions covered only part of a requirement for twelve battalions. That specific 3-of-12 claim is not supported by the cited 2021 U.S. Army fielding information. The Army stated in April 2021 that it planned to field 144 M-SHORAD systems to four battalions, beginning with the first unit in Germany [4]. Therefore, the defensible quantity is the documented four-battalion fielding plan; any larger requirement must be defined explicitly by the analyst as a scenario assumption rather than presented as an Army requirement.

A normalized coverage coefficient can be defined for any scenario by Eq. (3).

$$C_{cover} = min\left[1, \frac{N_{avail}}{N_{req}}\right] \tag{3}$$

where: C_{cover} – normalized force-coverage coefficient in the analytical scenario; N_{avail} – number of available or planned units used by the scenario; N_{req} – number of units required by the scenario definition; min – minimum operator, constraining the coefficient to a maximum value of 1.

Table 3: Coverage coefficient using the publicly documented four-battalion plan as the available baseline.

N_{avail}	N_{req}	C_{cover}	Interpretation
4	4	1.000	Public plan
4	6	0.667	Analyst-defined scenario requirement
4	8	0.500	Analyst-defined scenario requirement
4	10	0.400	Analyst-defined scenario requirement
4	12	0.333	Analyst-defined scenario requirement

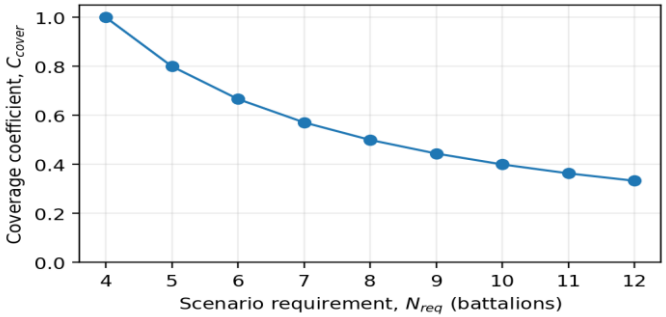


Figure 3: Coverage-coefficient sensitivity when the available/planned baseline is four M-SHORAD battalions [4].

4 High-Speed Threat Timing and Engagement Probability

4.1 Kinematic time remaining after reliable track

For a high-speed threat, the simplest timing quantity is the remaining kinematic time from the point at which a reliable track is available. If R_{track} is the remaining path length and v is treated as constant, the time is given by Eq. (4). This is a first-order relation only; a real engagement model must include geometry, trajectory curvature, acceleration, sensor latency, command-and-control delay, interceptor launch delay, and interceptor flight time.

$$t_{rem} = \frac{R_{track}}{v} \tag{4}$$

where: t_{rem} – kinematic time remaining after a reliable track is established; R_{track} – remaining threat path length at the first reliable track, m; v – assumed threat speed, m/s.

For illustration only, taking v = 1700 m/s (approximately Mach 5 under a simplified reference condition) gives 29.4 s for 50 km and 588 s for 1000 km. These distances are not asserted sensor detection ranges; they are scenario values used to show the inverse relationship between speed and available reaction time.

Table 4: Illustrative remaining time for a constant threat speed of 1700 m/s.

R_{track} (km)	t_{rem} (s)	t_{rem} (min)
50	29.4	0.49
100	58.8	0.98
200	117.6	1.96
500	294.1	4.90
1000	588.2	9.80

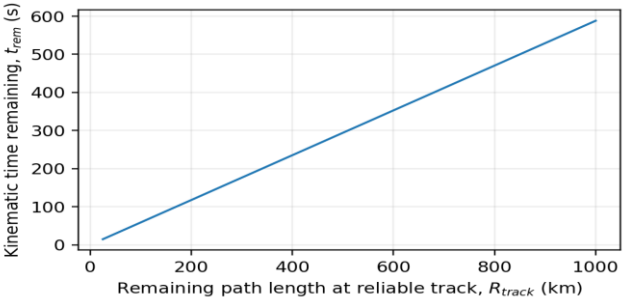


Figure 4: Kinematic time remaining versus reliable-track range for the illustrative constant speed v = 1700 m/s.

4.2 Engagement-chain probability

A transparent way to represent the engagement chain is to separate detection, track maintenance, and successful interceptor engagement. Under a simplifying conditional-independence assumption, the resulting probability is the product in Eq. (5). The source draft used values 0.6, 0.5, and 0.4 and obtained 0.12; the arithmetic is correct, but the values were not supported by the cited public sources. They are therefore retained only as an illustrative numerical example, not as measured performance.

$$P_{eng} = P_D \cdot P_T \cdot P_I \tag{5}$$

where: P_{eng} – overall engagement-chain success probability in the simplified model; P_D – probability of detection with the required quality and timeliness; P_T – conditional probability of maintaining a usable track; P_I – conditional probability of a successful interceptor engagement given a usable track.

Illustrative calculation: $P_{eng} = 0.6 \times 0.5 \times 0.4 = 0.12$. No claim is made that these values describe a specific weapon system.

HBTSS should not be assigned a direct kill probability. The Missile Defense Agency describes HBTSS as a space-based tracking capability intended to provide low-latency, fire-control-quality tracking data and support the advanced-threat kill chain [5]. Thus, HBTSS can influence quantities such as P_D, P_T, track continuity, and available decision time, but the final P_I also depends on the interceptor, geometry, command-and-control path, and engagement conditions.

5 Proposed Multi-Domain Convergence Index

Convergence is a central tenet of the Army MDO concept: capabilities from multiple domains are combined to create complementary effects and windows of superiority [3]. The source draft introduced a quantity called a multi-domain synergy coefficient. That equation is not a NATO or U.S. Army doctrinal metric, but it can be retained as a proposed heuristic index if its interpretation is stated explicitly. Let E_j be a normalized contribution from domain j, bounded between zero and one. The complement-product

index in Eq. (6) then measures how quickly the modeled combined contribution approaches one.

$$S_M = 1 - \prod_{j=1}^{m}(1 - E_j) \quad (6)$$

where: S_M – proposed normalized multi-domain convergence index, not an official doctrinal measure; m – number of domain contributions included in the model; E_j – normalized contribution assigned to domain j, with $0 \leq E_j \leq 1$; j – domain index.

Using the illustrative domain values retained from the source draft gives Eq. (7).

$$S_M = 1 - (0.2 \cdot 0.3 \cdot 0.8 \cdot 0.9 \cdot 0.1) = 0.99568 \quad (7)$$

where: S_M – value of the proposed convergence index for this numerical illustration; 0.2, 0.3, 0.8, 0.9, 0.1 – complements ($1 - E_j$) of the illustrative Air, Land, Cyber, Space, and Maritime contributions.

Table 5: Illustrative normalized domain contributions used only to demonstrate the proposed index.

Domain	**E_i**
Air	0.80
Land	0.70
Cyber	0.20
Space	0.10
Maritime	0.90

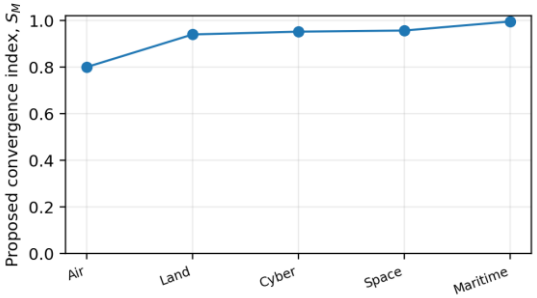


Figure 5: Cumulative value of the proposed convergence index for the illustrative domain inputs in Table 5.

The numerical result above also demonstrates a limitation: the complement-product form can saturate near one even when one or more domain contributions are weak. It should therefore be interpreted as a sensitivity index, not as a validated measure of combat effectiveness or "synergy." A calibrated operational model would require interaction terms, mission-dependent weights, uncertainty, and empirical validation.

6 Readiness and Chronometric Modeling of MDO Functions

6.1 Readiness-time decomposition

A generic readiness-time decomposition can be useful for planning studies. Equation (8) separates deployment, integration, and maneuver preparation. The 72-hour and 5–30-day values in the source draft are not established by the cited AUSA or Army MDO documents as universal readiness standards, so they are not presented here as factual benchmarks.

$$T_{ready} = T_{deploy} + T_{integrate} + T_{maneuver} \tag{8}$$

where: T_{ready} – total scenario readiness time; T_{deploy} – time required to deploy or reposition the force; $T_{integrate}$ – time required for command, communications, sensor, and fire-control integration; $T_{maneuver}$ – time required to complete maneuver preparation or movement into the modeled operational posture.

6.2 Central armed-conflict functions

TRADOC Pamphlet 525-3-1 describes MDO across competition and conflict and identifies the problems of compete, penetrate, dis-integrate, exploit, and re-compete [3]. The source draft focused only on the three central armed-conflict functions—penetrate, dis-integrate, and exploit. That narrower focus is acceptable for a chronometric submodel provided it is not described as the complete MDO sequence. For such a scenario, the modeled combat interval can be written as Eq. (9).

$$T_{combat} = T_p + T_d + T_e \tag{9}$$

where: T_{combat} – modeled duration of the three selected armed-conflict functions; T_p – scenario duration assigned to Penetrate; T_d – scenario duration assigned to Dis-integrate; T_e – scenario duration assigned to Exploit.

If each function is represented by a minimum and maximum scenario duration, the total interval follows Eq. (10). The 1–3, 2–4, and 5–15 day intervals below are retained from the source draft strictly as illustrative simulation inputs; they are not attributed to TRADOC as doctrinal durations.

$$T_{combat} \in \left[T_{p,min} + T_{d,min} + T_{e,min}, T_{p,max} + T_{d,max} + T_{e,max}\right] \tag{10}$$

where: T_{combat} – total duration interval for the selected scenario functions; $T_{p,min}$ – minimum scenario duration for Penetrate; $T_{p,max}$ – maximum scenario duration for Penetrate; $T_{d,min}$ – minimum scenario duration for Dis-integrate; $T_{d,max}$ – maximum scenario duration for Dis-integrate; $T_{e,min}$ – minimum scenario duration for Exploit; $T_{e,max}$ – maximum scenario duration for Exploit.

Table 6: Illustrative timing inputs retained from the source draft; values are scenario assumptions, not doctrinal standards.

Function	Symbol	Minimum (days)	Maximum (days)
Penetrate	T_p	1	3
Dis-integrate	T_d	2	4
Exploit	T_e	5	15

For this illustration, $T_{combat} \in [8, 22]$ days.

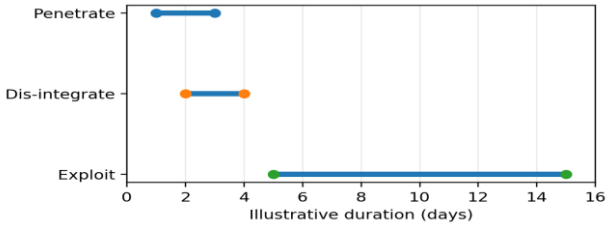


Figure 6: Illustrative duration ranges for the three selected armed-conflict functions; TRADOC notes that such actions can overlap [3].

7 Discussion and Applicability

The corrected framework separates publicly supported facts from analytical assumptions. Public sources support NATO's five operating domains [1], the Army's emphasis on layered and integrated AMD [2], the MDO functions and convergence concept [3], the 2021 M-SHORAD plan of 144 systems for four battalions [4], HBTSS as a fire-control-quality tracking sensor [5], and AIAMD/IBCS as an integrating command-and-control capability [6]. They do not support the source draft's 3-of-12 M-SHORAD requirement, a universal 72-hour readiness standard, a 5–30 day expeditionary-force standard, or a direct HBTSS-related kill probability of 0.8. Those numerical claims have therefore been removed or reclassified as explicit scenario inputs.

For national capability planning, the same modeling discipline is applicable to force-development studies in which assumptions, constraints, readiness, interoperability, and modernization priorities must be stated transparently. Bulgaria's Defence Capabilities Development Programme 2032 provides a national strategic framework for capability development and modernization through 2032 [8]. The equations in this paper can support sensitivity analysis within such planning, but any operational application requires nationally validated data and appropriate security handling.

Conclusion

This paper presented a corrected and more defensible mathematical model for studying IAMD within Multi-Domain Operations. The layered penetration equation was reformulated so that penetration is the product of layer failures; M-SHORAD capacity

was tied to the publicly documented four-battalion fielding plan rather than to an unsupported 3-of-12 claim; the hypersonic section was recast around kinematic time and engagement-chain decomposition; HBTSS was treated as a tracking sensor rather than an interceptor; and the MDO chronometric model was aligned with the broader compete–penetrate–dis-integrate–exploit–re-compete framework. The proposed convergence index and all unvalidated effectiveness coefficients are explicitly labeled as heuristic or scenario inputs. This separation between evidence and assumptions makes the model suitable for transparent sensitivity analysis, simulation exercises, and subsequent validation with authoritative test or exercise data.

References

1. NATO Allied Command Transformation. (2023, October 5). Multi-Domain Operations in NATO – Explained.
2. Dickinson, J. H. (2019, June 21). Protect, Defend, Exploit: Air and Missile Defense Evolves for Multidomain Operations. Association of the United States Army.
3. U.S. Army Training and Doctrine Command. (2018). The U.S. Army in Multi-Domain Operations 2028 (TRADOC Pamphlet 525-3-1). Department of the Army.
4. Army Futures Command. (2021, April 23). M-SHORAD Units Arrive to 5-4 ADA. U.S. Army.
5. U.S. Missile Defense Agency. (2021, January 22). Hypersonic and Ballistic Tracking Space Sensor Phase IIb Awards (21-NEWS-0001).
6. U.S. Army Acquisition Support Center. (2020). Weapon Systems Handbook 2020–2021. Department of the Army.
7. Lockheed Martin. (2025, June 18). Lockheed Martin Delivers Eighth U.S. Terminal High Altitude Area Defense Battery.
8. Ministry of Defence of the Republic of Bulgaria. (2021). Defence Capabilities Development Programme of the Armed Forces of the Republic of Bulgaria 2032. Sofia, Bulgaria.

Proceedings of International Scientific Conference "Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

SYSTEM BOUNDARY AND ANALYTICAL LEVEL IN LOSS ANALYSIS

Nikolay T. Iliev

Vasil Levski National Military University, Veliko Tarnovo, Bulgaria, ntiliev@nvu.bg

Abstract: *The paper examines two conditions for valid conclusions about realized loss: the system boundary and the analytical level. It argues that a loss established for a component or subsystem cannot automatically be transferred to a function, capability or wider system. Explicitly fixing the scope and level of each conclusion limits overgeneralization, causal shortcuts and double counting.*

Keywords: *system boundary, analytical level, loss, system analysis, national security*

СИСТЕМНА ГРАНИЦА И АНАЛИТИЧНО РАВНИЩЕ ПРИ ИЗСЛЕДВАНЕТО НА ЗАГУБИТЕ

Николай Т. Илиев

Национален военен университет „Васил Левски", Велико Търново, България, ntiliev@nvu.bg

Абстракт: *Докладът разглежда две условия за валидност на изводите за реализирана загуба — системната граница и аналитичното равнище. Обосновава се, че загуба, установена за компонент или подсистема, не се пренася автоматично към функция, способност или по-широка система. Изричното фиксиране на обхвата и равнището ограничава свръхобобщаването и двойното отчитане.*

Ключови думи: *системна граница, аналитично равнище, загуба, системен анализ, национална сигурност*

1. Въведение

Твърдението за загуба винаги се прави спрямо определен обект и определен обхват. В сложните системи на националната сигурност един и същ фактически резултат може да има различно значение за отделен компонент, за подсистема и за системата като цяло. Затова установяването на загуба изисква да бъде уточнено не само какво е изменено, но и за коя система е валиден изводът и на какво аналитично равнище е направен.

Практическият проблем възниква, когато резултат, доказан на едно равнище, се пренася към друго без самостоятелна проверка. Унищожаването или недостъпността на компонент може да бъде безспорна компонентна загуба, но функционалното отражение зависи от фактическото изпълнение след нея. Същото важи и при преминаване към оценка на способност или на по-широкото системно състояние. Военните подходи към оценяване на пораженията разграничават физическото състояние на елемента от функционалното състояние и от оценката на по-висока система [1], [2].

Паралелен проблем е системната граница. Ресурс може да бъде загубен за конкретно звено, но да остане наличен в рамките на по-широка организация. Обратно, физически съществуващ ресурс може да бъде недостъпен или неизползваем за конкретната подсистема. Ако системната граница не е фиксирана, едно и също фактическо положение може да бъде описано с противоречиви на пръв поглед твърдения.

Целта на доклада е да се изясни отношението между системната граница и аналитичното равнище при изследването на реализирани загуби и да се обоснове правило за валидността на прехода между различни системни обхвати и равнища.

2. Системната граница като обхват на валидност но извода

Системната граница определя системата или подсистемата, за която се прави твърдението за загуба. Тя очертава обхвата, в който се оценяват принадлежността, достъпността и използваемостта на конкретния референт. Това е особено важно при йерархични, мрежови и организационно разпределени системи, където един и същ ресурс може да участва в повече от една структура.

Елемент, който е отпаднал от една подсистема, не е непременно загубен за по-широката система. Ако например определено средство остава физически налично, но вече не може да бъде използвано от звеното, към което е било отнесено, компонентната загуба за това звено може да е фактически реализирана. Същевременно по-широката организация може да продължава да разполага със средството. Двете твърдения не са логически несъвместими, защото се отнасят към различни системни граници.

Обратното също е възможно. Физическото наличие на ресурс в рамките на организацията не доказва, че той остава достъпен и използваем за конкретната подсистема. Ограничение на достъпа, прекъсната свързаност, промяна в подчинението или друго фактическо условие може да доведе до загуба на използваемост в по-тясната системна граница, без физическо унищожаване на референта.

Системната граница не следва да се избира след установяването на резултата с цел предварително желана квалификация. Тя произтича от предмета на анализа, от действителните отношения на принадлежност и използване и от функцията, спрямо която референтът има значение. Когато едновременно се разглеждат подсистема и по-широка система, изводите за всяка от тях трябва да бъдат формулирани отделно.

3. Аналитичното равнище като характер на установеното изменение

От системната граница трябва да се разграничава аналитичното равнище. Границата отговаря на въпроса „за коя система е валидно твърдението“, докато равнището определя „какъв тип изменение е установено“. За анализа на загубите могат да бъдат разграничени компонентно, функционално, способностно и системно равнище.

Компонентното равнище се отнася до конкретни човешки, материални, технически, информационни, инфраструктурни или организационни елементи и

техни характеристики. Функционалното равнище описва фактическото изпълнение на определена функция или дейност. Способностното равнище е свързано с възможността при определени условия да бъде изпълнена задача или да бъде постигнат необходим резултат, а системното — със състоянието на разглежданата система като организирано цяло.

Тези равнища са свързани, но не са взаимозаменяеми. Компонентите участват в изпълнението на функции, а функциите могат да имат значение за способности и по-широки системни резултати. Самото наличие на такава зависимост обаче не определя автоматично какъв фактически резултат ще настъпи при загубата на конкретен елемент. Подходът на Дейвис към mission-system analysis също подчертава необходимостта да се разглеждат отношенията между мисии, способности и системни елементи, вместо един резултат да се пренася механично между равнищата [3].

Оттук произтича основното правило: загубата, доказана на едно аналитично равнище, представлява доказателство за изменение именно на това равнище. Извод за друго равнище изисква самостоятелно установяване на фактическото състояние там. Физическото поражение на елемент например не е достатъчно за заключение за функционална деградация, ако функцията продължава да се изпълнява чрез друга налична конфигурация [1], [2].

4. Граница и равнище при прехода между свързани изменения

При настъпване на загуба често се наблюдават последващи изменения в други компоненти, функции или системи. Тяхната свързаност не означава, че представляват една и съща аналитична позиция. За всеки последващ резултат трябва да бъде установено към коя системна граница и на кое равнище се отнася.

Това правило е особено важно при инфраструктурните взаимозависимости. Rinaldi, Peerenboom и Kelly показват, че измененията могат да се разпространяват между физически, кибер, географски и логически свързани инфраструктури [4]. Фактът, че нарушение в една инфраструктура има ефект върху друга, е основание да се изследва причинната връзка, но не заличава границата между отделните системи и техните собствени състояния.

Подобна необходимост се вижда и при информационните системи. NIST FIPS 199 разграничава нарушенията на поверителност, цялостност и наличност от потенциалното им въздействие върху операции, активи и лица [5]. Така свойството на конкретен информационен ресурс и последицата за по-широка дейност се отнасят към различни аналитични позиции, дори когато между тях има непосредствена зависимост.

При комуникационни инфраструктури разграничението между физическа инфраструктура, покритие и фактически показатели за свързаност също е наблюдаемо на практика. Disaster Connectivity Map на Международния съюз по далекосъобщения представя отделно инфраструктурните елементи, мобилното покритие и показатели като закъснение (latency) и пропускателна способност (throughput) [6]. Това позволява физическото състояние на мрежата да бъде различавано от фактическото качество на услугата.

5. Ограничаване на свъхобобщаването и двойното отчитане

Едновременното фиксиране на системната граница и аналитичното равнище ограничава две чести грешки. Първата е свръхобобщаването — резултатът за отделен компонент или подсистема да бъде представен като състояние на по-широката система без допълнително доказване. Втората е многократното отчитане — едно и също фактическо изменение да бъде представено последователно като няколко отделни загуби само защото е описано на различни равнища.

Например загубата на комуникационен възел е компонентна загуба. Ако след нея е установено прекъсване на конкретна комуникационна функция, може да бъде налице отделно функционално изменение. За да се говори за последващо намаляване на способност или промяна в системното състояние, е необходимо фактически да бъде установен съответният резултат. Ако такова изменение не е настъпило, смяната на наименованието не създава нова загуба.

Обратната грешка е различими загуби да бъдат слети единствено защото са причинно свързани. Подходите към проследяване на каскадни последствия и взаимозависимости разграничават отделните състояния и пътищата между тях [4], [7]. Причинната връзка обяснява отношението между измененията, но не премахва необходимостта всяко от тях да бъде индивидуализирано според собствената си системна граница и равнище.

Системният подход към критичната инфраструктура също изисква разглеждане на елементите и връзките в рамките на определен системен контекст [8]. Практическата стойност на този подход се увеличава, когато всяко твърдение за загуба съдържа ясно посочване на обхвата, за който е валидно, и на типа изменение, който действително е доказан.

6. Практическо приложение в анализа на националната сигурност

В системите за национална сигурност границите рядко съвпадат с физическите очертания на отделен обект. Един ресурс може организационно да принадлежи на една структура, функционално да обслужва друга и да бъде част от по-широка мрежа от зависимости. Поради това аналитичната граница трябва да се определя спрямо конкретния въпрос, а не само спрямо административната принадлежност.

Същевременно равнището на извода трябва да следва доказаното състояние. Ако наличните данни установяват единствено отпадане на компонент, анализът трябва да остане на компонентно равнище, докато няма достатъчно основания за извод относно функцията. Ако е установено функционално ограничение, това също не предрешава автоматично способностното или системното състояние.

Така системната граница и аналитичното равнище изпълняват две различни, но взаимно допълващи се функции. Първата локализира пространството на валидност на твърдението. Втората определя характера на установеното изменение. Съвместното им използване позволява причинните връзки да бъдат проследявани, без да се разширява обхватът на първоначалната загуба и без да се заличават самостоятелните последващи изменения.

Заключение

Системната граница и аналитичното равнище са различни условия за валидност на извода за реализирана загуба. Системната граница определя за коя система или подсистема се отнася твърдението, а аналитичното равнище показва какъв тип изменение е установено.

Едно и също фактическо положение може да бъде различно квалифицирано спрямо вложени системни граници, без това да представлява противоречие. Същевременно зависимостта между компонент, функция, способност и по-широко системно състояние не прави резултатите на тези равнища взаимозаменяеми. Всеки преход изисква собствено фактическо основание.

Изричното фиксиране на границата и равнището ограничава свръхобобщаването, неправомерното пренасяне на изводи и многократното отчитане на един и същ резултат. По този начин се създава по-проследима основа за изследване на причинно свързани загуби и на тяхното отражение в сложни системи на националната сигурност.

Литература

1. UNITED STATES JOINT FORCES COMMAND. Joint Fires and Targeting Handbook. 19 October 2007, pp. III-110, III-112, III-118–III-119.
2. JOINT TARGETING SCHOOL. Student Guide. Dam Neck, Virginia, effective 1 March 2017, pp. 166–168.
3. DAVIS, Paul K. Analytic Architecture for Capabilities-Based Planning, Mission-System Analysis, and Transformation. Santa Monica, CA: RAND Corporation, MR-1513-OSD, 2002.
4. RINALDI, Steven M.; PEERENBOOM, James P.; KELLY, Terrence K. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine, 2001, Vol. 21, No. 6, pp. 11–25. DOI: 10.1109/37.969131.
5. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems. Gaithersburg, MD: NIST, February 2004. DOI: 10.6028/NIST.FIPS.199.
6. INTERNATIONAL TELECOMMUNICATION UNION. Disaster Connectivity Map (DCM). Online. URL: https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Pages/Disaster-Connectivity-Map.aspx [accessed: 27.10.2025].
7. UNITED NATIONS OFFICE FOR DISASTER RISK REDUCTION. DELTA Resilience: Disaster Losses and Damages Tracking System. Онлайн. URL: https://www.undrr.org/building-risk-knowledge/disaster-losses-and-damages-tracking-system-delta-resilience [посетен на: 07.07.2025 г.].
8. MEDNIKAROV, Boyan; DIMITROV, Nedko; KALINOV, Kalin. Applying the System Approach to the Study of Critical Infrastructure. Information & Security: An International Journal, 2007, Vol. 22, pp. 138–150. DOI: 10.11610/isij.2212.

REALIZED AND SCENARIO-BASED LOSS: DIFFERENCES IN ANALYTICAL AND EVIDENTIARY STATUS

Nikolay T. Iliev

Vasil Levski National Military University, Veliko Tarnovo, Bulgaria, ntiliev@nvu.bg

Abstract: *The paper distinguishes realized loss from scenario-based loss in national security analysis. It argues that the same analytical categories may structure both modes, while their evidentiary status remains different. A scenario describes conditional future developments; a realized loss requires factual establishment. The distinction is preserved when causality, functional effects and response mechanisms are assessed.*

Keywords: *realized loss, scenario analysis, evidence, risk, national security*

РЕАЛИЗИРАНА И СЦЕНАРНО РАЗГЛЕЖДАНА ЗАГУБА: РАЗЛИЧИЯ В АНАЛИТИЧНИЯ И ДОКАЗАТЕЛСТВЕНИЯ СТАТУС

Николай Т. Илиев

Национален военен университет „Васил Левски", Велико Търново, България, ntiliev@nvu.bg

Абстракт: *Докладът разграничава реализираната от сценарно разглежданата загуба в анализа на националната сигурност. Обосновава се, че едни и същи аналитични категории могат да структурират двата режима, но доказателственият им статус остава различен. Сценарият описва условно бъдещо развитие, а реализираната загуба изисква фактическо установяване.*

Ключови думи: *реализирана загуба, сценарен анализ, доказване, риск, национална сигурност*

1. Въведение

Анализът на националната сигурност работи едновременно с фактически настъпили събития и с възможни бъдещи развития. В първия случай задачата е да се установи какво действително се е изменило, кога е настъпило изменението и какви последици могат да бъдат доказани. Във втория се изследват възможни събития, зависимости и резултати при предварително зададени предпоставки. Двата режима използват сходен понятиен апарат, но отговарят на различни доказателствени въпроси.

Рискът по своята природа е свързан с неопределеността и с възможни последствия за целите, поради което риск-анализът не предполага фактическа реализация на разглеждания резултат [1], [2]. Това разграничение е особено важно при употребата на понятието „загуба". Една прогнозирана, очаквана или сценарно моделирана загуба може да бъде количествено конкретна и дори оценена като високовероятна, без поради това да се превърне във фактически настъпила загуба.

Проблемът е не само терминологичен. Ако условен сценарен резултат бъде представен като доказано състояние, се смесват прогнозата и фактът. Ако, обратно, фактически настъпилото изменение се разглежда единствено през предварително изграден сценарий, съществува риск реалната картина да бъде подчинена на допускания, които не са се потвърдили. Това затруднява причинното проследяване, оценката на функционалното отражение и проверката на предприетите мерки.

Целта на доклада е да се изясни границата между реализирана и сценарно разглеждана загуба и да се обосноват различията в техния аналитичен и доказателствен статус. Акцентът е върху това как един и същ набор от аналитични категории може да се използва при фактически и при перспективен анализ, без условните положения да бъдат представяни като доказани факти.

2. Реализираната загуба като фактическа аналитична позиция

Реализираната загуба се отнася до изменение, което вече е настъпило по отношение на определим референт. За да бъде направен такъв извод, трябва да съществува доказателствена основа, позволяваща да се установи както състоянието след събитието, така и релевантното сравнително състояние. Самият факт на реализацията е различен от момента, в който загубата е открита, и от точността, с която е определен нейният размер.

На практика първоначалната информация често е непълна. Бойното оценяване, аварийното реагиране и оценяването след бедствия работят с последователно постъпващи данни, при които увереността в наличието на определено изменение може да бъде по-висока от увереността в пълния му обхват. В подобни случаи е важно да се отдели въпросът „настъпила ли е загуба“ от въпроса „какъв е окончателният ѝ размер“. Подходите към последващото оценяване на пораженията също разграничават първоначалната оценка от последващото уточняване на фактическите резултати [3].

Следователно реализираният характер на загубата не зависи от наличието на изчерпателна количествена оценка. Достатъчно е да бъде доказано релевантно отпадане или намаляване спрямо фактическо сравнително състояние. Количествената точност, пълнотата на данните и увереността в отделни параметри се отнасят до качеството и обхвата на оценката, а не до самия факт, че изменението вече е настъпило.

Това положение има значение и за причинния анализ. Установяването на загубата и доказването на причината са свързани, но различни операции. Причинното обяснение може да остане непълно, докато фактът на определено отпадане или намаляване вече е достатъчно надеждно установен. По същия начин предварително предполагаемата причина не замества доказването на самото изменение.

3. Сценарно разглежданата загуба и условният статус на изводите

Сценарният анализ използва бъдещи или условно зададени състояния. В него могат предварително да бъдат определени предполагаем референт, изходно състояние, възможен размер на загубата, вероятни причинни връзки и очаквани

последици. Тези позиции позволяват да бъдат изследвани уязвимости, варианти за развитие и потребности от реакция, но запазват статута си на зависими от предварителните допускания.

Високата правдоподобност не променя този статус. Дори когато сценарият е изграден върху реални зависимости, исторически данни и надеждни модели, резултатът му остава условен до фактическото настъпване и установяване на съответното изменение. Показателен пример е системата PAGER на Геоложката служба на САЩ, която след земетресение формира ранни моделни оценки за потенциални човешки и икономически загуби преди да е налична пълната фактическа картина от място [4]. Моделната оценка има непосредствена практическа стойност, но нейният доказателствен статус се различава от последващо установените фактически загуби.

Същата логика се отнася до причинната структура. В сценария може да бъде заложена верига, според която отпадането на определен компонент ще доведе до ограничаване на функция или до друго последващо изменение. Тази връзка представлява аналитично допускане, което трябва да бъде проверено, ако събитието действително настъпи. Реалните зависимости могат да се проявят по различен начин поради конкретните условия, наличните ресурси и реакцията на системата.

Условен е и статусът на предварително предвидените механизми за реакция. Наличието на резерв, заместител, алтернативен канал или възстановителна възможност в план не доказва, че при реален случай този механизъм ще бъде наличен и ефективен. По тази причина сценарното твърдение, че определена функция ще бъде запазена или възстановена, се различава от фактически установения резултат след настъпване на събитието.

4. Доказателствена асиметрия между двата режима

Реализираната и сценарно разглежданата загуба могат да използват едни и същи аналитични категории, но към тях се прилагат различни доказателствени изисквания. При реализирания случай референтът, сравнителното състояние и последиците се установяват чрез фактически данни. При сценарния режим същите позиции се задават като предпоставки, параметри или моделни резултати.

Това създава принципна асиметрия. При фактическия анализ неизвестното се намалява чрез събиране и проверка на доказателства за вече настъпилото състояние. При сценарния анализ неопределеността не може да бъде отстранена чрез доказване на бъдещия резултат; тя се управлява чрез допускания, диапазони, вероятности и варианти. По тази причина степента на детайлност на един сценарий не трябва да се приема като доказателство за неговата реализация.

Планирането, основано на способности, също работи с бъдещи задачи, условия и необходими резултати. При Дейвис акцентът е върху устойчивото планиране при неопределеност и множество възможни бъдещи сценарии [5]. В Процеса на НАТО за отбранително планиране се идентифицират изисквани способности, разпределят се цели за способности и се оценява напредъкът по тяхното развитие [6]. Тези

подходи са перспективни по предназначение и не следва да бъдат смесвани с ретроспективното доказване на вече реализирана загуба.

Разликата има практическо значение и при оценяването на недостиг. Несъответствието между налично и необходимо състояние може да бъде съществено за планирането, но не представлява непременно фактически реализирана загуба. Система може да не притежава изисквана бъдеща способност, без преди това да е разполагала с нея и да я е загубила. Следователно дефицитът спрямо критерий и фактическото отпадане спрямо доказуемо предходно състояние трябва да бъдат обозначавани отделно.

5. Преход от сценарно към фактическо установяване

Когато събитие, сходно със сценарно разглежданото, действително настъпи, предварителният сценарий не се превръща автоматично във фактическа констатация. Той може да служи като отправна точка за наблюдение и проверка, но реалният анализ започва от действително установените състояния.

На първо място се проверява дали фактически засегнатият референт съвпада с предварително приетия. След това се установява действителното сравнително състояние, размерът и характерът на настъпилото изменение. Отделно се проверяват причинните връзки и реалното функционално отражение. Ако планът е предвиждал определена реакция, тя също се оценява според фактическото ѝ задействане и постигнатия резултат.

Така несъответствието между очакваното и действително настъпилото не е грешка, която трябва да бъде заличена чрез приспособяване на фактите към сценария. То представлява самостоятелен аналитичен резултат. Разликата може да покаже неправилно допускане, непълно позната зависимост, различно поведение на системата или ефект от предприета реакция. Именно тази проверка придава на сценарния анализ стойност за последващото усъвършенстване на планирането.

Оттук следва и методологично ограничение: предварително моделираната причинна верига, очакваното функционално отражение и прогнозираният резултат от реакцията запазват условния си статус до тяхната фактическа проверка. Това ограничение не намалява практическата стойност на сценариите. Напротив, то позволява сценарното планиране да бъде използвано активно, без неговите резултати да се представят като вече доказани състояния.

6. Значение за анализа на националната сигурност

Разграничението между реализиран и сценарен режим е приложимо в широк кръг анализи на националната сигурност — от оценяване на рискове и критична инфраструктура до планиране на способности и подготовка за кризи. Общият понятиен апарат улеснява съпоставянето между предварително очакваното и реално настъпилото, но само ако се запази различният доказателствен статус на двете групи изводи.

Практическата полза се проявява в три направления. Първо, намалява се вероятността прогнозни величини да бъдат представени като фактически загуби. Второ, след настъпване на събитие се създава ясна основа за проверка на

предварителните допускания и причинни връзки. Трето, резултатите от фактическия анализ могат да се върнат към планирането като доказателствена основа за коригиране на бъдещите сценарии.

Това двупосочно използване не изисква смесване на режимите. Ретроспективният анализ предоставя доказателствен материал за това как системите действително са реагирали при настъпили загуби, а сценарният анализ използва тези знания за структуриране на възможни бъдещи развития. Свързването им е продуктивно именно когато границата между факт и допускане остава видима.

Заключение

Реализираната и сценарно разглежданата загуба представляват различни аналитични позиции. При реализираната загуба изводът се отнася до фактически настъпило и доказателствено установимо изменение. При сценарно разглежданата загуба изводът е условен и зависи от предварително определени предпоставки, допускания и моделни зависимости.

Еднаквият понятиен апарат не заличава тази разлика. Референт, сравнително състояние, причинна връзка, функционално отражение и механизъм за реакция могат да бъдат разглеждани и в двата режима, но в сценарния анализ те имат прогнозен или хипотетичен статус до последваща фактическа проверка.

При настъпване на реално събитие сценарият може да насочи анализа, но не замества самостоятелното установяване на фактическите състояния. Разликата между предварително очакваното и действително настъпилото следва да бъде запазена като аналитичен резултат. По този начин сценарното и ретроспективното изследване могат да бъдат свързани, без да се смесват рискът, планирането и доказването на реализирана загуба.

Литература

1. AVEN, Terje. Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, 2016, Vol. 253, No. 1, pp. 1–13. DOI: 10.1016/j.ejor.2015.12.023.
2. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 31000:2018 Risk management — Guidelines. 2nd ed. Geneva: ISO, 2018.
3. JOINT TARGETING SCHOOL. Student Guide. Dam Neck, Virginia, effective 1 March 2017, pp. 166–168.
4. U.S. GEOLOGICAL SURVEY. PAGER — Prompt Assessment of Global Earthquakes for Response: FAQ. Онлайн. URL: https://earthquake.usgs.gov/data/pager/faq.php [посетен на: 20.01.2026 г.].
5. DAVIS, Paul K. Analytic Architecture for Capabilities-Based Planning, Mission-System Analysis, and Transformation. Santa Monica, CA: RAND Corporation, MR-1513-OSD, 2002.
6. NATO. NATO Defence Planning Process. Updated 16 April 2025. Онлайн. URL: https://www.nato.int/en/what-we-do/introduction-to-nato/nato-defence-planning-process [посетен на: 18.09.2025 г.].

7. SHALAMANOV, Velizar M.; TAGAREV, Todor D. Reengineering the Defense Planning in Bulgaria. Sofia: Institute for Security and International Studies, 1998.

WEAPONS, TECHNOLOGIES, LOGISTICS

MODIFICATION OF THE BURNING RATE OF A LIGHTING PYROTECHNIC COMPOSITION IN LIGHTING AIR BOMBS BY INTRODUCING AN INHIBITOR – STEARIC ACID

Ivelina Ivanova Angelska

NITI SHS Kazanlak, Bulgaria, angelska.i@abv.bg

***Abstract**: The report presents a study of the burning rate of a lighting pyrotechnic composition in lighting air bombs through the introduction of an inhibitor – stearic acid.*

***Keywords:** pyrotechnics, airbombs. lighting pyrotechnic composition.*

Introduction

Pyrotechnic compositions are multicomponent mixtures of various chemical substances designed to produce different light effects through exothermic reactions [5]. Their primary function is the transformation of chemical energy into a specific physical effect – light, sound, or smoke. Unlike explosive materials, the primary mode of energy conversion is combustion rather than detonation. Pyrotechnic compositions are widely used for both civilian and military purposes.

Lighting pyrotechnic compositions play a key role in modern lighting air bombs. They provide reliable, intense, and sustained illumination under various operating conditions. One of the main parameters determining the suitability of such compositions is the burning rate, which directly affects the luminous intensity, its duration, and the thermal stability of the system.

Practical experience shows that unstable combustion leads to deviations from the specified operational characteristics, necessitating the development of more effective methods for controlling and stabilizing the combustion process. This requires the use of substances known as inhibitors, which influence the combustion kinetics without adversely affecting the technical illumination characteristics of the pyrotechnic composition.

There are several methods for reducing the burning rate of pyrotechnic lighting compositions; however, stearic acid has proven to be an effective inhibitor in practical applications. It is an organic saturated fatty acid whose physicochemical properties enable it to interact with the components of pyrotechnic compositions.

The present study aims to analyze the possibilities for modifying the burning rate of a lighting pyrotechnic composition used in lighting air bombs by introducing stearic acid as an inhibitor, while maintaining a balance between combustion stability and the functional characteristics of the lighting system. The operating conditions of lighting air bombs impose additional requirements on the stability of the lighting composition and the combustion process. Lighting air bombs operate at considerable altitude, where the ambient temperature is low, which can significantly affect the physicochemical properties of the lighting pyrotechnic composition. Low temperatures affect heat transfer

and the initial stages of combustion, which may result in changes in the burning rate as well as in the illumination efficiency.

1. Theoretical Part

The study was conducted on a lighting composition used in the SAB-250 lighting air bomb, consisting of the following components:

- Oxidizer – $NaNO_3$ (sodium nitrate), which provides oxygen for the combustion process and influences the burning rate;
- Fuel – powdered rosin-coated magnesium, which determines the combustion process and its rate;
- Binder – rosin;
- Additives – industrial oil and graphite.

For the purpose of the study, five samples weighing 2 kg each were prepared, with different percentages of stearic acid.

- Sample 1 – pure composition, 100%, without stearic acid;
- Sample 2 – stearic acid content: 2.5%;
- Sample 3 – stearic acid content: 1.5%;
- Sample 4 – stearic acid content: 2.8%;
- Sample 5 – stearic acid content: 3%.

The compositions for the samples were conditioned and prepared in the respective percentage proportions in accordance with the manufacturing technology. The prepared samples were pressed using a 100-ton hydraulic press into paper tubes, which had also been conditioned. After pressing, the samples were prepared for testing.

Test Objective

To determine the burning rate and luminous intensity of the pure lighting composition used in the SAB-250 lighting air bomb in comparison with compositions containing different percentages of the inhibitor stearic acid.

Test Preparation

The conditioned samples were numbered. Black powder was placed in the lower part of each sample, with a coiled tin wire embedded in it. At the test site, a 20-meter-high stand was installed, from which Sample 1 – the pure composition without an inhibitor – was suspended. Two electrical conductors were connected to the ends of the tin wire. A lux meter was positioned 20 meters from the stand to determine the luminous intensity.

Test Procedure

Electric current was applied through the conductors connected to the tin wire, after which the pressed composition was ignited. A stopwatch was used to measure the total burning time, while a lux meter was used to measure the maximum luminous intensity. All samples were ignited in the specified order, and the results were recorded.

2. Results And Calculations Of The Conducted Tests

The burning rate is calculated using the following formula:

$$S = V.T \tag{1}$$

where:
S – length of the pressed composition [mm];
V – burning rate, in [mm/s];
T – burning time [s].
Luminous intensity:

$$Cd = l_x.R^2 \quad (2)$$

where:
Cd – Luminous intensity [candela];
lx – the unit of illuminance [lux];
R – the square of the distance from the lux meter to the stand [m].

Table 1. Results And Calculations Of The Conducted Tests

Sample No.	Length of pressed composition	Burning rate	Burning time	Luminous intensity
1	146 mm	2.4 mm/s	1 m	500,000
2	146 mm	1.4 mm/s	1.40 m	350,000
3	146 mm	1.8 mm/s	1.2 m	400,000
4	146 mm	1.3 mm/s	1.50 m	300,000
5	146 mm	1 mm/s	2.30 m	200,000

3. Analysis Of The Results

Based on the tests conducted, the following conclusions can be drawn:

- Sample 1 – pure composition: an excessively high burning rate, a short burning time, and high luminous intensity were observed. The sample does not meet the requirements specified by the technical parameters;
- Sample 2 – 2.5% stearic acid: a significant reduction in the burning rate was observed, accompanied by a decrease in luminous intensity; however, the reduction was insufficient to fully meet the technical requirements;
- Sample 3 – 1.5% stearic acid: a slight decrease in the burning rate and luminous intensity was observed, but it was insufficient to meet the technical requirements;
- Sample 4 – 2.8% stearic acid: a significant reduction in the burning rate and luminous intensity was observed, fully satisfying the specified technical requirements;
- Sample 5 – 3% stearic acid: an excessive increase in burning time and a significant reduction in luminous intensity were observed, and the sample therefore does not meet the technical requirements.

Conclusion

Based on the analysis of the results obtained from the conducted tests, Sample 4 categorically meets the technical specifications and parameters specified by the customer and fully satisfies the required technical characteristics.

References

1. Дудырева А.С., (*1986) Материалы лекций.,* Москва.
2. Дик В.Н., *Взрывчатые вещества, пороха, боеприпасы, отечественного производства.,* (*2009).*, Минск, Охотконтракт.
3. Саздов.Р., *Наръчник по взривни работи.,* (*1982).*, София, Профиздат.
4. Чивурин.А.В., *Занимательная пиротехника.,* (*2003).*, Харкьов, издателство „Основа".
5. Цонев Ц.Г., Христов Х.А., (2016)., *Конструктивни изменения на основния заряд на 82 mm учебно-практическа мина, предназначена за тренажор за обучение на минохвъргачните разчети.,* Шумен., Университетско издателство „Епископ Константин Преславски"., ISSN 1311-834X.
6. Шидловский А.А. (*1954), Основы пиротехники.,* Москва, Государственное издательство оборонной промышленности.

ANALYTICAL MODEL FOR THE PREDICTIVE DETERMINATION OF SMALL-ARMS SHOT GROUPING IN SINGLE-SHOT FIRING

Conyu G. Conev

AAD and CIS Faculty, National Military University "Vasil Levski", Artillery, Shumen, Bulgaria
coni19@abv.bg

***Abstract**: The paper proposes an analytical model for the predictive determination of small-arms shot grouping in single-shot firing. The model is based on the influence of barrel vibrations on the bullet's angle of departure and, consequently, on shot grouping.*

***Keywords:** small arms barrel, vibrations.*

Introduction

Small arms constitute a part of the weapon systems employed by modern armed forces and are intended for engaging enemy personnel located in exposed positions. Every servicemember, regardless of the branch of the armed forces, possesses some type of small arm in a combat environment.

On the other hand, the increasingly widespread use of individual ballistic protection systems has led to a growing need to improve the tactical and technical characteristics of small arms in order to ensure the effective engagement of enemy personnel equipped with such protection.

During the design of small arms, every weapon needs to meet particular requirements that are set by the purchasing party [6]. Addressing these new requirements imposed on small-arms systems necessitates improved grouping and accuracy, including at maximum effective ranges.

In general, shot grouping is one of the most important technical characteristics contributing to the increased effectiveness of small arms. Therefore, its investigation is of significant importance for the design of modern small-arms systems.

The objective of the present study, and the resulting research task, is to develop an analytical model for the predictive determination of shot grouping in single-shot firing for a small-arms barrel with specified mass, length, and geometry.

For the purpose of simplifying the model, the following assumptions and limitations have been adopted:

- only the influence of the barrel's transverse natural vibrations on shot grouping during single-shot firing is considered, without accounting for the internal damping of the material;
- the shot is considered as a single application of an external force at the location corresponding to the maximum pressure in the barrel bore;
- the barrel is assumed to be rigidly fixed at its connection to the receiver, and the influence of receiver vibrations is not considered;
- the influence of other factors affecting shot grouping during single-shot firing is not taken into account;

- only shot grouping in the vertical plane is considered;
- shot grouping is determined at the standard range adopted in the Republic of Bulgaria for testing small arms: 100 m, and according to the standard procedure;
- the barrel is assumed to be homogeneous in composition.

1. Analytical Model for the Predictive Determination of Small-Arms Shot Grouping in Single-Shot Firing

One of the factors that has a significant influence on shot grouping during single-shot firing is the barrel's natural transverse vibration. The conducted studies have established that, during single-shot firing, second-order vibration modes have the greatest influence on shot grouping. Their amplitude is relatively large, causing significant vertical displacement of the muzzle section of the barrel.

On the other hand, the bullet's time of travel through the barrel approaches half the period of these vibrations. Consequently, even relatively small variations in the firing conditions can readily alter the phase of the transverse vibrations.

Procedure for the Predictive Determination of Small-Arms Shot Grouping in Single-Shot Firing:

1.1. Determination of the External Force Causing Barrel Vibrations

For the development of the analytical model, it is first necessary to determine the magnitude of the external force causing the barrel vibrations. This force is generated by the pressure resulting from the combustion of the propellant.

The magnitude of this force is determined using the following equation:

$$F = P_{max}.S \tag{1}$$

where:

F – force generated by the propellant gases [N];

P_{max} – maximum pressure in the barrel bore [kg/m²];

S – cross-sectional area of the barrel bore [m²].

Due to the presence of rifling in the barrel bore, the cross-sectional area is greater than $\frac{\pi.d^2}{4}$, therefore, for an approximate calculation, the cross-sectional area of the barrel bore of small arms with rectangular-profile rifling is determined using the following formula:

$$S = 0{,}8.d^2 \div 0{,}82.d^2 \tag{2}$$

where:

d – caliber [m].

The point of application of the force is assumed to be the point at which the pressure reaches its maximum value.

1.2. Determination of the vibration amplitude

After determining the magnitude of the external force causing the barrel vibrations, it is necessary to determine the displacement of the muzzle section at the moment the bullet exits the barrel, with the vibration amplitude being determined first.

Based on the assumptions adopted, the effect of the external force is considered as a single impulse acting on the system, and in this case the initial conditions are:

$$x_0 = 0, \qquad v_0 = \frac{I}{m}.P_{max} \tag{3}$$

where:

I – impulse [N·s];

x_0 – initial displacement [m];

v_0 – initial velocity [m/s].

Since the motion is assumed to follow a sinusoidal law, the instantaneous displacement is calculated using the following formula:

$$x = \frac{I}{m.\omega}.sin(n_2.t) \tag{4}$$

where the maximum value is equal to:

$$x_{max} = A = \frac{I}{m.n_2} = \frac{F.t}{m.n_2} \tag{5}$$

where:

m - barrel mass [kg];

A – amplitude [m].

1.3. Determination of the second natural frequency and period of the transverse vibrations of the barrel

After determining the vibration amplitude, it is necessary to determine the second natural frequency and the period of the transverse vibrations of the barrel.

The analytical determination of the second natural frequency of the natural transverse vibrations of the barrel is performed using the following formula:

$$n_2 = k.\frac{4{,}694^2}{2.\pi.l^2}.\sqrt{\frac{E.I_i}{S.\rho}} \qquad \text{[Hz]}, \tag{6}$$

where:

n_2 – second natural frequency of the barrel's transverse vibrations [Hz];

k – correction coefficient accounting for the shape of the barrel;

E – modulus of elasticity [Pa];

I_i – second moment of area of the barrel cross-section about the centroidal axis of the cross-section [m⁴];

ρ – density of the material from which the barrel is manufactured [kg/m³];

l – barrel length up to the point of attachment [m];

S – cross-sectional area of the barrel [m²].

The correction coefficient accounting for the shape of the barrel is determined using the following formula:

$$n_2 = k.\frac{4{,}694^2}{2.\pi.l^2}.\sqrt{\frac{E.I_i}{S.\rho}} \qquad \text{[Hz]}, \tag{7}$$

where:

m_r – barrel mass [kg];

Dts – outside diameter of the barrel at the point of attachment [m];

d – barrel caliber [m].

The period is determined using the following formula:

$$T = \frac{1}{n_2} \quad [s] \tag{8}$$

1.4. Determination of the bullet travel time in the barrel

The bullet travel time in the barrel is determined using the following formula:

$$t_k = \frac{2.l_n}{V_0} \quad [s], \tag{9}$$

where:

t_k – bullet travel time in the barrel [s];
l_n – length of the rifled portion of the barrel [m];
V_0 – initial muzzle velocity of the bullet [m/s].

At the same time, variations in the initial muzzle velocity of the bullets resulting from differences in the mass of the propellant charge and storage conditions must be taken into account.

Accordingly, the time interval Δt_k, during which the bullets leave the muzzle for each individual batch of ammunition, is determined using the following formula:

$$\Delta t_k = t_{k2} - t_{k1} \tag{10}$$

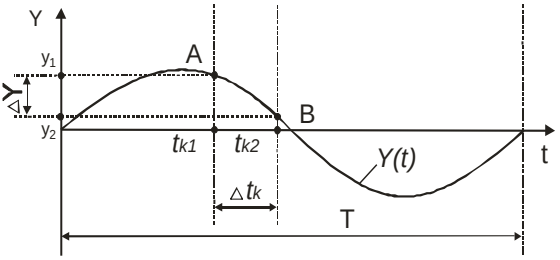


Figure 1: Graph of the transverse vibrations of the muzzle section of the barrel as a function of time.

T – period of the transverse vibrations of the barrel; Δt_k – time interval during which the bullets leave the barrel; t_{k1} – minimum bullet travel time in the barrel; t_{k2} – maximum bullet travel time in the barrel; ΔY – barrel displacement over the time interval Δt_k in the vertical plane; y_1 – lower limit of the barrel displacement; y_2 – upper limit of the barrel displacement.

1.5. Determination of the barrel displacement in the muzzle section

Since the shape of the natural transverse vibrations is described by a sinusoidal law, it is necessary to determine the displacement values within the time interval during which the bullets leave the muzzle. For this purpose, the instantaneous displacement values of the barrel in the vertical plane must be determined for the specified time interval. This is performed using the following formula:

$$x = A.sin(n_2.t) \quad [m] \tag{11}$$

where:

t – time [s];

x – instantaneous displacement of the barrel in the vertical plane [m].

After determining the instantaneous displacement values of the barrel in the vertical plane for the time interval during which the bullets leave the muzzle, the barrel displacement over the time interval Δt_k in the vertical plane is determined using the following formula:

$$\Delta Y = y_1 - y_2 \text{ [m]}, \tag{12}$$

where:

ΔY – barrel displacement over the time interval Δt_k in the vertical plane [m];

y_1 – lower limit of the barrel displacement at time t_{k1} [m];

y_2 – upper limit of the barrel displacement at time t_{k2} [m].

1.6. Determination of the radius containing 100% of the shots

Based on the obtained data, the predicted grouping at 100 m is determined using the formula obtained from the graph in Fig. 2:

$$Y_{100} = \frac{(l+100)}{l} . \Delta Y \text{ [m]}, \tag{13}$$

where:

Y_{100} – diameter of the circle containing 100% of the shots at 100 m.

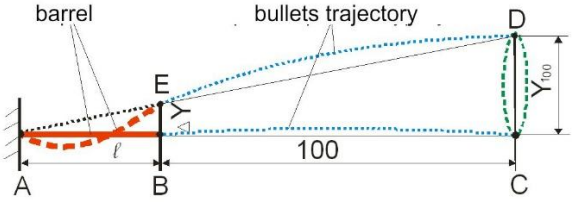


Figure 2: Graph for determining the predicted dispersion at 100 m for single-shot firing.

ΔY – displacement interval of the barrel during the time interval Δtk; Y100 – predicted dispersion at 100 m; l – barrel length.

3. Input data for determining the predicted grouping of a ballistic barrel

Based on the developed model, the predicted grouping of a ballistic barrel with the characteristics given below was determined.

Table 1. Data for the ballistic barrel

Type of ballistic barrel	Barrel mass [kg]	Barrel length up to the point of attachment [m]	Outside diameter of the barrel at the point of attachment [m]	Inside diameter of the barrel [m]
Ballistic barrel, designed for 7,62×39 mm cartridges, Model 1943	1,123	0,496	0,03	0,00762

For the analysis of the two barrels, 50PA steel was used, with the following characteristics:

- modulus of elasticity – 2.16×10^5 MPa;
- material density – 7840 kg/m³;
- yield strength – 748 MPa;
- ultimate tensile strength – 980 MPa;

For the maximum pressure in the bore of the barrel designed for Model 1943 cartridges, the value Pmax = 2800 kg/cm² was adopted. The location of the maximum pressure is 471 mm from the muzzle.

4. Results of calculations based on the analytical model

- cross-sectional area of the barrel – **0.000047032164 m²**;
- magnitude of the external force causing the barrel vibrations – 13639.32756 N;
- amplitude – 0,039 m;
- second natural frequency of the transverse vibrations of the barrel – 411.77 Hz;
- vibration period – 0.002429 s;
- bullet travel time in the barrel:

For 7,62×39 mm Model 1943 cartridges, the maximum bullet travel time in a ballistic barrel with a rifled portion length of 0.470 m, at the minimum permissible velocity, is:

$$t'_{k2} = \frac{2.l_n}{V_0} = \frac{2.0{,}470}{690} = 0{,}001362 \quad \text{s.}$$

For the minimum bullet travel time in the barrel at the maximum permissible velocity:

$$t'_{k1} = \frac{2.l_n}{V_0} = \frac{2.0{,}470}{740} = 0{,}001270 \quad \text{s.}$$

The mean bullet travel time in the barrel is 0,001316 s.

- the time interval during which the bullets leave the muzzle (Δt_k) is 0.000092 s;
- barrel displacement over the time interval Δt_k in the vertical plane, $\Delta Y = 0.0012597$ m;
- predicted grouping – 0.255 m.

5. Experimental firing test with a ballistic barrel

To verify the developed model, an experimental firing test was conducted using a ballistic barrel with the same characteristics.

The objective of the study was to assess the adequacy of the developed model.

The study was conducted on the basis of the Regulations for Testing Defense Products in the Ministry of Defense and the Bulgarian Armed Forces, Sofia, 2005, and was carried out at the Central Artillery Technical Test Range.

The conditions under which the study was conducted were as follows:

- ambient temperature 20 ± 2 °C; relative humidity 65 ± 5%;
- firing was conducted in an enclosed tunnel to eliminate the influence of crosswind;
- the ammunition was to be the standard ammunition for the weapon system under test, new, serviceable, and from the same production batch and year, in order to minimize the influence of factors causing variations in the initial muzzle velocities of the bullets;
- the ammunition was conditioned in a room with a constant temperature for 24 hours prior to firing, without removing the ammunition from its standard packaging;
- firing distance – 100 m (measured from the muzzle to the target screen);
- barrel elevation angle – 0° relative to the horizontal plane.

6. Results of the experimental study

The experimental firing consisted of 10 series of 15 shots per series. The grouping value was taken as the diameter of the circle containing 100% of the shots.

As a result of the firing tests, the mean diameter across all series was 0,212 m.

The relative error between the experimental results and the analytical model was 16.8%.

Conclusions

1. The comparative analysis of the experimental results and the analytical model indicates the presence of additional, unaccounted-for factors associated with barrel vibrations that affect grouping. One such factor is the first-order natural transverse vibration mode, which is not accounted for in the developed model.
2. To improve the developed model, it is necessary to incorporate the effect of the first-order natural transverse vibration mode.

References

1. Beer P.P., Johnstan R.R., (1988). Vector mechanics for engineers dynamics., Mc Graw-NY.
2. Brosh J. T., (1980). Mechanical Vibration and Shock Measurements. Bruel & Kjar.
3. Carlucci D. E., Jacobson S. S., (2007). Ballistics. Theory and design of guns and ammunitions.N.Y.
4. Daniel J. I., (2001). Engineering vibration. N.J.,.
5. Denys J. M., (2000). Passive Vibration control.,Wiley. N. Y.
6. Dimitrow M.P., (2021). Analysis on the Next Generation Assault Rifles and Ammunition Designed for the US Army. Warsaw, Poland. ISSN 2081-5891.
7. Landau L.D., Lefhitz E.M. (2000). Mehanisms. O.

A MODEL FOR DETERMINING A CRITERION FUNCTION

Ivo Georgiev Radulov

Defence Advanced Research Institute, Rakovski National Defence College, Sofia, Bulgaria, i.radulov@rndc.bg

Abstract: *The quality of higher education requires precise management tools. This article presents a specialized mathematical-statistical evaluation model. It was developed to assist quality experts at the Rakovski National Defence College (RNDC).*

The model provides a methodological foundation for the analysis and optimization of multifactorial systems. It is based on modern statistical methods for data processing. Its primary objective is to assist experts at the RNDC in organizing, managing, and monitoring the quality of educational activities to implement the Academy's long-term educational policy.

The model is universal in nature. Its mathematical structure allows it to be applied to various complex systems. In this specific case, the model has been adapted to evaluate the quality of education by surveying the opinions of students from the RNDC's two main faculties: the Faculty of National Security and Defense and the Faculty of Command and Staff.

Keywords: *Aggregated output parameter; methods for modeling or optimizing multifactorial objects; multi-criteria decision-making; Analytic Hierarchy Process (AHP).*

МОДЕЛ ЗА ОПРЕДЕЛЯНЕ НА ЦЕЛЕВА ФУНКЦИЯ (ОБОБЩЕН ИЗХОДЕН ПАРАМЕТЪР)

Иво Георгиев Радулов

Институт за перспективни изследвания за отбраната, Военна академия „Г. С. Раковски", София, Р България, i.radulov@rndc.bg

Абстракт: *Качеството на висшето образование изисква точни инструменти за управление. Настоящата статия представя специализиран математико-статистически модел за оценка на качеството на обучение във висшите военни училища. Той е разработен в помощ на експертите по качеството във Военна академия „Г. С. Раковски".*

Моделът предоставя методологична основа за изследване и оптимизиране на многофакторни обекти. Той стъпва върху съвременни статистически методи за обработка и анализ на данни. Основната му цел е да подпомага експертите от Военната академия при организацията, управлението и контрола на качеството на учебната дейност за реализиране на дългосрочната образователна политика на Академията.

Моделът притежава универсален характер. Неговата математическа структура позволява да бъде приложен към различни сложни управленски системи. В конкретния случай моделът е адаптиран за оценка на качеството на обучение чрез изследване на мнението на обучаемите от двата основни факултета на Военна академия, Факултет „Национална сигурност и отбрана" и Факултет „Командно-щабен".

Ключови думи: *Обобщен изходен параметър; методи за моделиране или оптимизиране на многофакторни обекти; многокритериални решения; метод на Саати.*

Увод

Представения модел за намиране на целева функция е допълнение към методиката за социологически изследвания за мнението на слушателите и студентите от „Випуск 2025“ за качеството на обучението във Военна академия. Тези изследвания се извършват ежегодно на випускниците преди защитата на дипломните им работи или държавните изпити (за обучаващите се в ОКС „Бакалавър“). Моделът е разработен по заявка на отдел „Учебна дейност“ на ВА „Г. С. Раковски“. Той интегрира съвременни статистически методи с експертна оценка, за да превърне субективните качествени измерители в обективен количествен показател.

Моделът интегрира методологична основа, базирана на съвременни статистически методи за изследване и оптимизиране на многофакторни обекти. Предназначен е да подпомогне работата на експертите от Военна академия, чиито задължения са свързани с организацията и управлението на качеството на учебната дейност и осъществяването на образователната политика на Академията.

Моделът е универсален. В конкретния случай изборът на целевата функция (обобщения изходен параметър) е свързан с оценката на качеството на проведеното обучение във Военна академия „Г. С. Раковски“ чрез проучване на мнението на обучаемите от факултет „Национална сигурност и отбрана“ и факултет „Командно-щабен“.

Моделът функционира като система с множество входове (мнения, оценки, фактори) обобщени в индекс на качеството (обобщен изходен параметър). Структурата му за определяне на целевата функция (Y) се състои в изпълнението на следните три етапа (Фиг. 1):

1. Нормализация на входните данни (y_u). Тъй като анкетите съдържат различни качествени оценки, данните се трансформират в безразмерни величини в интервала [-1, 1]. Задължително условие е преди нормализацията, стойностите на изходните параметри да са изчислени априори с методите на математическата статистика.

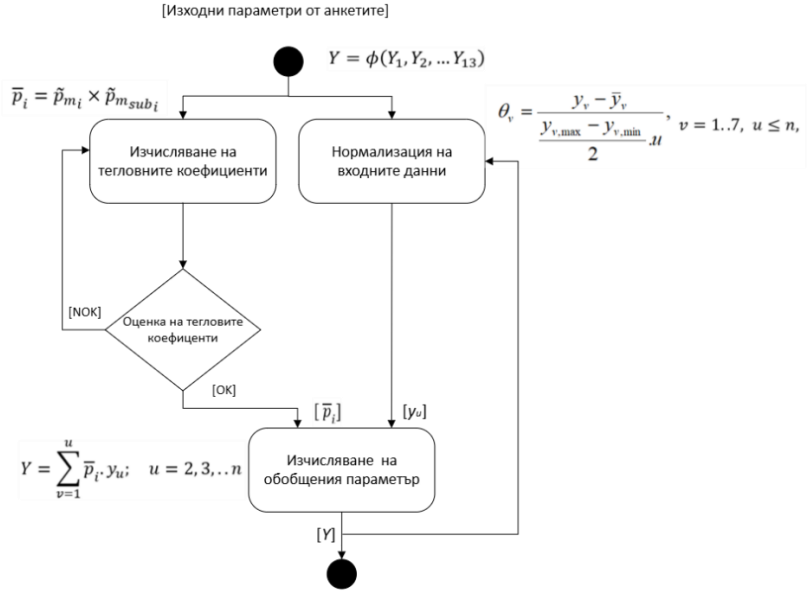
2. Изчисляване на тегловните коефициенти ($\overline{p}_i$). Не всички фактори имат еднаква тежест за обучаемите, затова теглата се определят с помощта на математически методи за вземане на многокритериални решения в случая по метода Аналитичен йерархичен процес (на английски: Analytic Hierarchy Process, AHP) или известен още като метода на Томас Саати.

3. Формулиране на линейната целева функция и изчисляване на обобщения параметър (Y). Крайният обобщен параметър се изчислява като претеглена линейна комбинация с формула от вида:

$$Y = \sum_{v=1}^{u} \overline{p}_i . y_u; \quad u = 2, 3, .. n \tag{1}$$

където y_u са изходните параметри от социологическото изследване за качеството на обучение, а $\overline{p}_i$ са тегловните коефициенти, които отчитат ролята на отделните параметри при количественото характеризиране на целта. Те могат да бъдат положителни величини (когато увеличаването на съответния параметър

съответства на целта) и отрицателни величини (когато увеличаването на съответния параметър води до отдалечаване от поставената цел).



Фигура 1. Модел за определяне на целева функция

Изчисляване на тегловните коефициенти на параметрите

Изчисляването на $\overline{p}_i$ „тегло" на отделните изходни параметри се извършва по метода на Саати. Методът е структурирана техника за подпомагане на вземането на сложни решения. Разработен е от Томас Л. Саати през 70-те години на миналия век и включва няколко основни стъпки за определяне на най-добрата алтернатива [3, 4]. В настоящия модел методът се използва ограничено само за изчисляване на теглата на отделните изходни параметри. Изчисляването на теглата става чрез математически апарат по способа на собствените вектори, чрез които се извеждат относителните тегла на всеки критерий и алтернатива. Методът използва техника за сравнения по двойки, при която експерти или участници в изследването взимат решения, като сравняват елементите на всяко ниво по двойки спрямо тяхната относителна важност или предпочитание към елемента от по-горното ниво. За целта се използва специална скала на Саати. Началото на процеса започва с формиране на матрица на сравнението (Таблица 1) [2, 3, 4]. Резултатите от мнението на специалистите се нанасят в тази матрица.

Таблица 1.

	A1	**A2**	**...**	**Ai**	**...**	**Aj**	**...**	**An**
A1	1	a12	...		...	a1j	...	a1n
A2	a21	1	...		...	a2j	...	a2n
…	...	...	...	...	...	...	...	...
Ai	ai1	ai2	...	1	...	aij	...	ain
…	...	...	...	...	...	...	...	...
Aj	aj1	aj2	...	aji	...	1	...	ajn
…	...	...	...	...	...	...	...	...
An	an1	an2	...	ani	...	anj	...	1

За елементите aij на матрицата важат следните правила:

$$aij = 1 \text{ при } i = j, \tag{1}$$

$$a_{ij} = \frac{1}{a_{ji}} \text{ при } i \neq j \tag{2}$$

Сравнението по двойки на отделните изходни параметри става с използване на 9 степенната скала на Саати (семантично кодирано), при която:

- Ако Ai и Aj са с еднаква важност то aij = 1.
- В случите, когато параметърът Ai е по - важен от Aj кодирането се извършва по следния начин:

aij = 3, ако Ai е незначително по-важен от Aj;
aij = 5, ако Ai е значително по-важен от Aj;
aij = 7, ако Ai е явно (много) по-важен от Aj;
aij = , ако Ai абсолютно превъзхожа Aj по важност.

Следващата стъпка е изчисляване на „Вектора на ранговете" на дадената матрица на сравнения. За целта се умножават n-те броя клети във всеки ред на матрицата на сравнението и се получава матрица P [2, 3, 4].

$$P = \begin{bmatrix} p_1 = a_{11} \times a_{12} \times .... \times a_{1n} = \prod_{j=1}^{n} a_{1j} \\ p_2 = a_{21} \times a_{22} \times .... \times a_{2n} = \prod_{j=1}^{n} a_{2j} \\ ... \\ p_n = a_{n1} \times a_{n2} \times .... \times a_{nn} = \prod_{j=1}^{n} a_{nj} \end{bmatrix} \tag{3}$$

Извлича се корен n-ти от всеки елемент на матрицата P, за да се получи матрица P*.

$$P^* = \begin{bmatrix} p_1^* = \sqrt[n]{p_1} \\ p_2^* = \sqrt[n]{p_2} \\ \cdots \\ p_n^* = \sqrt[n]{p_n} \end{bmatrix} \tag{4}$$

$\sum_{i=1}^{n} p_i^*$ Намира се сумата на всички елементи на вектора-стълб и резултатът се използва за да се нормализира матрицата P^*, с помощта на която се получава матрица $\tilde{P}$.

$$\tilde{P} = \begin{bmatrix} \tilde{p}_1 = p_1^* / \sum_{i=1}^{n} p_i^* \\ \tilde{p}_2 = p_{21}^* / \sum_{i=1}^{n} p_i^* \\ \cdots \\ \tilde{p}_n = p_n^* / \sum_{i=1}^{n} p_i^* \end{bmatrix} \tag{5}$$

Векторът-стълб $\tilde{P}$ е векторът на ранговете с тегловните коефициенти за всеки ранг.

$\tilde{p}_1$- тегловен коефициент на параметъра, класиран на 1-во място;

$\tilde{p}_2$- тегловн коефициент на параметъра, класиран на 2-ро място;

и т.н.

Тези изчисления се правят за основните групи параметри и за всички параметри от всяка подгрупа. Крайната стойност на ранга на всеки параметър се изчислява като:

$$\overline{p}_i = \tilde{p}_{m_i} \times \tilde{p}_{m_{sub_i}} \tag{6}$$

където:

$\tilde{p}_{m_i}$- теглото на основната група на изходния параметър i;

$\tilde{p}_{m_{sub_i}}$- тегло на изходния параметър i, като елемент от подгрупата на разглеждания основен изходен параметър.

Веднъж определени, тегловите коефициенти се използват при изготвянето на сравнителния анализ на обобщения изходен параметър за всички випуски без изменение.

Определяне на изходните параметри и подход за нормализация на входните данни

В конкретния случай, за определяне на качеството на обучението във Военна академия „Г. С. Раковски“, генералната съвкупност на изходните параметри е:

$$Y = \phi(Y_1, Y_2, \ldots Y_{13}); \tag{7}$$

където: Y - качеството на обучение;

Y1 - Степента на обща удовлетвореност от обучението;

Y2 - Материално-техническото осигуряване на обучението;

Y3 - Административното осигуряване на обучението;

Y4 - Информационното осигуряване на обучението;

Y5 - Планирането на учебния процес;

Y6 - Организационните аспекти на ефективността на обучението по изучаваната специалност/специализация;

Y7 - Системата за контрол и оценка на знанията;

Y8 - Удовлетвореност от придобитите компетентности за бъдеща професионална реализация;

Y9 - Удовлетвореност от придобитите знания и умения за реализация в живота като цяло;

Y10 - Задължителните дисциплини, които слушателите и студентите са изучавали през периода на обучението по критериите: актуалност на преподавания материал, практическа насоченост и начин на преподаване;

Y11 - Съдържанието на учебния процес, методиката на преподаване и организацията на обучението под формата на коментари в свободен текст;

Y12 - Проведеното обучение от разстояние в електронна среда;

Y13 - Социално-битовите услуги и удобства във ВА „Г. С. Раковски".

Тези параметри са заложени в анкетната карта, която випускниците попълват в края на обучението си.

Златно правило в статистиката и планирането на проучвания е бройката на изследваните параметри да бъде минимално необходимата за доказване на хипотезата. В нашия случай изброените параметри са 13, твърде голям брой за целите на изследването. Затова е необходимо да се извърши избор на съществените и отстраняване на несъществените.

След извършен анализ по метода „мозъчна атака"1, изборът на значимите изходни параметри за намирането на обобщената функция "Y", определяща качеството на обучение е сведен до избора на следните седем изходни параметъра:

$$Y = \phi(Y_1, Y_2, Y_5, Y_6, Y_7, Y_8, Y_9), \tag{8}$$

където: Y1 - Степента на обща удовлетвореност от обучението;

Y2 - Материално-техническото осигуряване на обучението;

Y5 - Планиране на учебния процес;

Y6 - Организационни аспекти на ефективността на обучението по изучаваната специалност/специализация;

Y7 - Системата за контрол и оценка на знанията;

Y8 - Удовлетвореност от придобитите компетентности за бъдеща професионална реализация;

Y9 - Удовлетвореност от придобитите знания и умения за реализация в живота като цяло.

[1] Анализът е направен от експерти на научна секция „СИСО", ИПИО, с доказан дългогодишен опит в тази област.

Така приети, параметрите на целевата функция, не могат да бъдат описани количествено за всяка комбинация от отчитаните входни фактори. За целта е необходимо да бъдат определени специфичните показатели за всеки от съставните параметри на функция (8). В общия случай всеки от изходните параметри зависи от съставните ѝ m показатели:

$Y_1 = f_1(y_1)$,

$$Y_2 = f_2(y_1, y_2, \dots y_7), \tag{8}$$

$Y_5 = f_3(y_1, y_2, \dots y_6)$,

$Y_6 = f_3(y_1, y_2, \dots y_4)$,

$Y_7 = f_3(y_1, y_2, \dots y_4)$,

$Y_8 = f_3(y_1)$,

$Y_9 = f_3(y_1)$,

Така подбрано, множеството от стойности дефинира областта на определение на целевата функция, като ограничена и дискретна, а избраните параметри, с техните показатели, се отличават с ясен смисъл, простота при измерване и изчисляване, т.е. удовлетворени са основните изисквания при избора на целева функция, а именно:

да се характеризира количествено;

да бъде единствена;

да е статистически ефективна характеристика на целта, т.е. с минимална възможна дисперсия σε2.

Поради природата, размерността и интервалите на определение на отделните параметри y_v и тегловите коефициенти $\overline{p}_i$ приемаме, че обобщеният изходен параметър Y трябва да премине към безразмерна и ограничена величина в интервала (-1, +1).

За тази цел седемте параметъра y1, y2, y5, y6, y7, y8, y9 се преобразуват в нови параметри $\theta_1, \theta_2, \theta_3, \theta_4, \theta_5, \theta_6, \theta_7$, по формулата [1]:

$$\theta_v = \frac{y_v - \bar{y}_v}{\frac{y_{v,\max} - y_{v,\min}}{2}.u}, \quad v = 1..7,\ u \le n, \tag{9}$$

където $\bar{y}_v$ е средната стойност на y_v, за оценка на която може да се вземе величината: [1]

$$\bar{y}_v = \frac{y_{v,\max} + y_{v,\min}}{2}, \tag{10}$$

Величините $y_{v,max}$ и $y_{v,min}$ са съответно максималната и минималната стойности на y_v, а u = 7 е броят на участващите във формирането на обобщената

целева функция параметри. Тогава формула (1) ще добие вида (11), който се прилага за отделните категории обучаеми (бакалаври, магистри и слушатели) във Военна академия „Г. С. Раковски“:

$$Y = \sum_{v=1}^{u} \overline{p}_i . \theta_v = \frac{1}{7} \sum_{v=1}^{7} \overline{p}_i \frac{2y_v - (y_{v,max} + y_{v,min})}{(y_{v,max} - y_{v,min})} \quad (11)$$

При такова преобразуване на отделните изходни параметри коефициентите $\overline{p}_i$ могат да бъдат безразмерни величини, ако и те се избират в интервала [-1, +1], т.е.

$$-1 \leq \overline{p}_i \leq 1, \quad (12)$$

следователно обобщената целева функция Y от формула (11) ще представлява безразмерна величина, чиито стойности са ограничени в интервала:

$$-1 \leq Y \leq 1, \quad (13)$$

Резултати от използването на модела

Моделът е използван за пръв път през 2025 г. при проведено социологическо проучване за мнението на слушателите и студентите от „Випуск 2025“ за качеството на обучение във Военна академия „Г. С. Раковски“.

Резултатите от прилагането на модела са представени както следва:

В Таблица 2 са показани получените теглови коефициенти на избраните значими параметри;

Таблица 3 са представени получените обобщени стойности за качеството на обучение за „Випуск 2025“, по категория обучаеми.

Докладът с резултатите от проучването е приет с протокол № 13/10.11.2025 г. на заседание на научна секция „Стратегически изследвания на сигурността и отбраната“, с протокол № 12/12.11.2025 г. от Съвета на ИПИО и протокол № 14/02.12.2025 г. от Академичния съвет на ВА „Г. С. Раковски“.

Таблица 2.

Параметри:		**Теглови коефициенти:** $\overline{p}_i$
Y1	Степен на обща удовлетвореност от обучението	0.1687
Y2	Материално-техническо осигуряване на обучението	0.0316
Y5	Планиране на учебния процес	0.0544
Y6	Организационни аспекти на ефективността на обучението по изучаваната специалност/специализация	0.0438
Y7	Система за контрол и оценка на знанията	0.0438
Y8	Удовлетвореност от придобитите компетентности за бъдеща професионална реализация	0.3996
Y9	Удовлетвореност от придобитите знания и умения за реализация в живота като цяло	0.2581

Таблица 3.

№	Категория обучаеми „Випуск 2025“	Изходен параметър (стойност)
1.	Бакалаври от специалност „Сигурност и отбрана“ на факултет „Национална сигурност и отбрана“	0.0730
2.	Бакалаври от специалност „Киберсигурност“ на факултет „Командно-щабен“	0.0187
3.	Магистри от факултет „Национална сигурност и отбрана”	0.0869
4.	Слушатели от специалност Стратегическо ръководство на отбраната и въоръжените сили (СРОВС) на факултет „Национална сигурност и отбрана”	0.0673
5.	Студенти магистри от факултет „Командно-щабен“	0.0928
6.	Слушатели от специалност „Организация и управление на военни формирования на оперативно ниво“ (ОУВФОН) на факултет „Командно-щабен“	0.0652

Заключение

Моделът представя авторско виждане за преодоляване на съществуващия дефицит, свързан с определяне на качеството на обучение на випуските от Военна академия „Г. С. Раковски“. Използването му създава методологични предпоставки за осигуряване на научно-аналитични експертни оценки и препоръки при вземане на решения от управленския състав във Военната академия. Той демонстрира възможностите на методите за оптимизиране на многофакторни обекти, приложени към процеса за управление и контрол на качеството на учебната дейност във Военната академия. С негова помощ намирането на измерими, количествени показатели за изпълнението на всички нематериални процеси вече не представлява предизвикателство пред изследователите и заинтересованите лица в Академията.

Използвана литература:

1. Божинов, Е., Вучков, И., “Статистически методи за моделиране или оптимизиране на многофакторни обекти”, София, 1973 г.
2. Neno Hristov, Ivo Radulov, Petko Iliev, Plamena Andreeva “Prioritization Methodology for Development of Required Operational Capabilities,” System Analysis & Studies panel, SAS-081/RSY, NATO Research and Technology Agency (RTA), 26-28 April 2010, Sofia, Bulgaria,
3. https://www.semanticscholar.org/paper/Prioritization-Methodology-for-Development-of-Hristov-Radulov/73dcd76478a67e70d27fa3187a068fc23fa36f01?p2df
4. T. Saaty, Time dependent decision-making; dynamic priorities in the AHP/ANP: Generalizing from points to functions and from real to complex

variables, Published in Mathematical and computer modelling, Volume 46, Issues 7–8, October 2007, Pages 860-891,

5. https://www.sciencedirect.com/science/article/pii/S089571770700098 2?via%3Dihub
6. T. Saaty, Decision-making with the AHP: Why is the principal eigenvector necessary, European Journal of Operational Research, 2003, Volume 145, Issue 1, Pages: 85-91

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

FUNCTIONAL CLASSIFICATION AND COMPARATIVE ANALYSIS OF METHODS FOR THE DEMILITARIZATION OF ARTILLERY ROUNDS AND THEIR COMPONENTS

Miroslav P. Dimitrov

National Military University "Vasil Levski", Artillery, AAD and CIS Faculty
amirodimitrov@abv.bg

Abstract: *This paper examines methods for the demilitarization of artillery rounds and their components according to their place within the overall demilitarization process. A comparative assessment of their applicability, safety, and environmental impact is presented.*

Keywords: *demilitarization, artillery round, functional classification, explosives, disassembly, final disposal.*

ФУНКЦИОНАЛНА КЛАСИФИКАЦИЯ И СРАВНИТЕЛЕН АНАЛИЗ НА МЕТОДИТЕ ЗА ДЕМИЛИТАРИЗАЦИЯ НА АРТИЛЕРИЙСКИЯ ИЗСТРЕЛ И НЕГОВИТЕ ЕЛЕМЕНТИ

Мирослав П. Димитров

Национален военен университет „Васил Левски", факултет „Артилерия, ПВО и КИС"
amirodimitrov@abv.bg

Абстракт*: Докладът разглежда методите за демилитаризация на артилерийски изстрели и техните елементи според мястото им в цялостния технологичен процес по демилитаризация. Извършена е сравнителна оценка на тяхната приложимост, безопасност и въздействие върху околната среда.*

Ключови думи*: демилитаризация, артилерийски изстрел, функционална класификация, взривни вещества, разкомплектоване, окончателно обезвреждане*.

Увод

Боеприпасите с изтекъл срок на експлоатация, влошено техническо състояние или отпаднала необходимост представляват основен проблем за логистичните органи. Тези боеприпаси заедно с елементите към тях се класифицират като излишни. Основните способи за освобождаване от излишните бойни припаси са: търговска реализация и утилизация на същите [12]. Търговската реализация е за предпочитане, но реализацията ѝ е трудно осъществима поради влошените качества на излишните бойни припаси и намаления интерес в световен мащаб към съществуващите у нас номенклатури [11].

Демилитаризацията на артилерийския изстрел включва отнемане на военното му предназначение и унищожаване или преобразуване на съдържащите се взривни вещества, барути и пиротехнически състави [3].

За тази цел се прилагат както методи за непосредствено унищожаване чрез взривяване или изгаряне, така и последователни методи за разкомплектоване, отваряне на корпуса, извличане и окончателно обезвреждане на енергетичните материали. Първите имат по-широка приложимост, но ограничават контрола върху замърсяването на околната среда и възможностите за рециклиране. Последователната обработка от своя страна позволява разделяне и оползотворяване на материалите, но изисква повече технологични етапи, определена материална база и технологично време.

Поради различните резултати, получени при прилагането им, методите не могат да бъдат разглеждани само според физичния принцип на въздействие. В доклада те са класифицирани според мястото им в цялостния процес на демилитаризация и са сравнени по приложимост, безопасност, въздействие върху околната среда и възможности за ресурсно оползотворяване.

Цел на разработката

Целта на доклада е да се разработи функционална класификация на методите за демилитаризация на артилерийския изстрел и неговите елементи според мястото им в технологичния процес и да се извърши сравнителна оценка на тяхната приложимост, безопасност и въздействие върху околната среда.

1. Методически подход и критерии за класификация

Обект на изследването са методите за демилитаризация на комплектования артилерийски изстрел и неговите отделни елементи. Анализът е насочен към мястото на всеки метод в технологичния процес.

В общия случай артилерийският изстрел включва снаряд със съответното снаряжение, взривател, метателен заряд, гилза или картуз, средство за възпламеняване на метателния заряд и допълнителни елементи [1]. Устройството и техническото състояние на отделните елементи, както и видът на съдържащите се енергетични материали, влияят върху избора на метод за демилитаризация.

Методи с широка приложимост, като взривяването, могат да се използват при различни боеприпаси, но прилагането им се ограничава от изискванията за безопасност, условията на площадката за взривяване, въздействието върху околната среда и възможностите за оползотворяване на металните остатъци [3].

Разграничават се методите за окончателно обезвреждане от подготвителните операции по разкомплектоване, осигуряване на достъп до разривния заряд и извличане на взривното вещество.

1.1. Принцип на функционалната класификация

Класификацията се основава на мястото на съответния метод в цялостния процес на демилитаризация.

В зависимост от избрания подход демилитаризацията може да се осъществи чрез унищожаване на комплектования артилерийски изстрел или чрез последователна обработка на неговите отделни елементи. Тази обработка включва разкомплектоване, осигуряване на достъп до разривния заряд, извличане на енергетичните материали и окончателното им обезвреждане. Последващото

оползотворяване на металните части и на други годни за употреба материали може да бъде резултат от прилагането на съответните методи, но не се разглежда като самостоятелна група методи за демилитаризация.

Съобразно етапа на прилагане са обособени четири групи методи: методи за унищожаване на комплектования артилерийски изстрел; методи за разкомплектоване и осигуряване на достъп до разривния заряд; методи за извличане на взривните вещества и метателните състави; методи за окончателно обезвреждане на извлечените енергетични материали.

1.2. Критерии за сравнителна оценка

При сравнението се отчита дали методът се прилага към комплектован артилерийски изстрел, към отделни негови елементи или към предварително извлечени взривни вещества и барути. Изборът на метод се съобразява с конструкцията, калибъра и техническото състояние на боеприпаса, както и с вида на снаряжението и неговата чувствителност към инициране [3, 4].

Степента на демилитаризация се определя според крайния резултат от прилагането на метода.

Безопасността се оценява според риска от непреднамерено инициране, защитата на личния състав и възможността за дистанционно или автоматизирано управление. Оценката по екологични и ресурсни критерии обхваща образуването на вредни газове, замърсени води и твърди остатъци, както и възможността за почистване и рециклиране на металните части. Отчитат се също сложността на технологичния процес, необходимото оборудване и условията за прилагане на метода.

2. Основни групи методи за демилитаризация

Групирането на методите се извършва съобразно вида и последователността на операциите, чрез които се постига демилитаризацията: унищожаване на комплектования артилерийски изстрел или неговото разкомплектоване и последващо обезвреждане на отделените елементи, взривни вещества и барути.

2.1. Методи за унищожаване на комплектования артилерийски изстрел

При непосредственото унищожаване комплектованият артилерийски изстрел не се разкомплектова предварително. Към тази група се отнасят взривяването на открито и унищожаването в детонационна камера, при които се разрушават корпусът и съдържащите се енергетични материали по взривен способ [4].

При взривяването на открито боеприпасът се унищожава чрез контролирана детонация на определена за целта площадка. Методът е приложим за широк набор от боеприпаси с изтекъл експлоатационен срок, силно корозирали, с нараснало взривно вещество или с изключително влошено техническо състояние, което не позволява безопасно разкомплектоване или демилитаризация посредством други методи. Предимствата му се изразяват в сравнително простото изпълнение, високата бързина на действие на метода, широката приложимост и ниските разходи. Основните ограничения са свързани с разпространението на ударна вълна и осколки, високото равнище на шум, замърсяването на въздуха и почвата и

ограничената възможност и нецелесъобразност за събиране на металните остатъци [3].

При унищожаването в детонационна камера взривът протича в затворено и укрепено съоръжение, предназначено за демилитаризация. Камерата е специално пригодена да спира ударната вълна и осколките. Образуваните газове при детонацията могат да бъдат отведени за пречистване, а металните остатъци – събрани след приключване на процеса и рециклирани. Приложението на метода се ограничава от вътрешните размери на камерата и допустимото количество взривно вещество и изисква специализирано оборудване [4].

И при двата способа целта е окончателно безвъзвратно унищожаване на артилерийския изстрел заедно с неговите елементи. Взривяването на открито е лесно осъществим, сравнително евтин и бърз процес, но има негативно влияние върху околната среда. За неговото осъществяване обаче е необходима специално оборудвана площадка.

Детонационната камера позволява по-добър контрол върху процеса и рециклиране на образуваните остатъци. Ограниченията на метода са свързани с капацитета на детонационната камера, необходимостта от специализирана апаратура и високата стойност на необходимата инфраструктура.

2.2. Методи за разкомплектоване и осигуряване на достъп до разривния заряд

В тази група са разгледани механичното разкомплектоване, рязането и пробиването на корпуса, хидроструйното рязане и криогенното фрактуриране. Целта на посочените методи е да се разделят отделните елементи на артилерийския изстрел и да се осигури достъп до разривния заряд, без артилерийският снаряд да бъде непосредствено унищожаван.

Механичното разкомплектоване има за цел да раздели артилерийския изстрел на неговите съставни части, след което те се подлагат на последваща демилитаризация. При механичното разкомплектоване се отделят взривателят, средството за възпламеняване, метателният заряд и останалите части, които могат да бъдат разглобени. Тези операции невинаги осигуряват достъп до разривния заряд. Когато той не може да бъде извлечен през съществуващите отвори, целостта на корпуса се нарушава чрез механичен, хидроструен или криогенен метод.

При хидроструйното рязане корпусът се обработва с водна струя под високо налягане, използвана самостоятелно или с добавен абразив. Липсата на пряк контакт с метален режещ инструмент намалява вероятността от искрообразуване, а операцията може да се управлява дистанционно [7, 9]. Когато водната струя се използва за отмиване на разривния заряд, нейното приложение се отнася към методите за извличане, разгледани в т. 2.3. Получената вода съдържа частици от взривното вещество и трябва да бъде събрана и пречистена [8, 9].

При криогенното фрактуриране корпусът се охлажда до температура, при която пластичността му намалява и се създават условия за крехко разрушаване. След това той се подлага на контролирано механично натоварване за осигуряване на достъп до разривния заряд. На този етап взривното вещество не се обезвреждa, а

след осигуряването на достъп трябва да бъде извлечено и окончателно обезвредено [2].

Изборът на механичен, хидроструен или криогенен метод зависи от конструкцията и материала на корпуса, както и от вида и състоянието на снаряжението.

2.3. Методи за извличане на взривните вещества и метателните състави

След разкомплектоването на артилерийския изстрел и осигуряването на достъп до разривния заряд се пристъпва към неговото извличане от корпуса. Метателните състави се отделят от гилзата или картуза. Тези операции не променят взривните свойства на извлечените материали, поради което представляват подготвителен етап, след който е необходимо окончателното им обезвреждане [3].

При механичното извличане разривният заряд се отделя от вътрешната повърхност на корпуса. Когато конструкцията на снаряда и състоянието на пълнежа позволяват, зарядът може да бъде изваден чрез пресово избутване – цял или раздробен. Опасността от непреднамерено инициране при удар, триене или местно нагряване налага строг контрол върху технологичния процес, дистанционно управление и защита на личния състав [2, 9].

При водоструйното извличане водната струя раздробява и отмива взривното вещество от вътрешната повърхност на корпуса. Получава се смес от вода и частици от взривното вещество, която трябва да бъде събрана и пречистена, а отделеният материал – окончателно обезвреден [8, 9].

Термичното извличане е приложимо само към топими взривни вещества. Чрез контролирано нагряване пълнежът се размеква или стопява и се отделя, без корпусът да бъде разрушаван механично. Температурата трябва да се поддържа в допустимите граници, за да не се предизвика разлагане или възпламеняване, а извлеченото взривно вещество подлежи на окончателно обезвреждане [2, 3].

2.4. Методи за окончателно обезвреждане на енергетичните материали

Към методите за окончателно обезвреждане на извлечените енергетични материали се отнасят изгарянето, детонационното унищожаване, плазменото разрушаване и химичното разграждане.

Изгарянето на открито се прилага предимно за барути и пиротехнически състави. Методът е сравнително лесен за изпълнение, но не позволява улавяне и пречистване на образуваните газове. Съществуват и опасности от възникване на пожар, непълно изгаряне и замърсяване на въздуха и почвата [3, 5]. При изгарянето в затворени пещи горенето протича при контролирани условия, а газообразните продукти могат да бъдат отведени за пречистване, а твърдите остатъци – събрани и обработени. Този начин ограничава въздействието върху околната среда, но изисква специални съоръжения и по-големи разходи [4].

Детонационното унищожаване се прилага към взривни вещества, извлечени от разривни заряди. Методът осигурява необратимо разрушаване на взривното вещество, но е свързан с образуване на ударна вълна, шум, вредни газообразни продукти и опасност от пожар. Тези въздействия могат да бъдат ограничени при извършване на процеса в специално пригодена камера.

При плазменото разрушаване взривните вещества, барутите и пиротехническите състави се подлагат на въздействието на високотемпературна плазма в затворена камера. Органичните съставки се разлагат и окисляват, а неорганичните примеси се разтопяват и се задържат в образуваната шлака. След охлаждането тя се превръща в устойчив твърд остатък, а газовете се отвеждат за пречистване.

Методът позволява обезвреждането да протича в контролирана среда, но изисква сложно оборудване, голям разход на енергия и постоянен технически контрол [6].

Химичното разграждане се основава на преобразуването на взривните вещества и барутите чрез химична реакция. В зависимост от състава на обработвания материал могат да се прилагат хидролиза, неутрализация или окисление [2, 4]. Алкалната хидролиза например се използва за разграждане на нитраминови взривни вещества като хексоген и октоген [10]. Процесът протича в затворено съоръжение, без наличието на взривно превръщане. Необходими са обаче специализирано химическо оборудване, химични реагенти и последващо пречистване на получените течни и твърди продукти [4].

Различните видове енергетични материали в артилерийския изстрел ограничават избора на метод за окончателно обезвреждане. Изгарянето се прилага предимно към барути и пиротехнически състави, детонационното унищожаване – към бризантни взривни вещества, а химичното разграждане – към състави, които могат да бъдат преобразувани чрез химична реакция. Затворените съоръжения позволяват събиране и обработване на образуваните продукти, но приложението им зависи от капацитета и техническите възможности на оборудването.

3. Сравнителен анализ на методите за демилитаризация

Сравнението е извършено между методи със сходно място в процеса на демилитаризация.

Взривяването на открито и унищожаването в детонационна камера могат да бъдат определени като възможни способи за цялостно унищожаване на комплектовани артилерийски изстрели.

Механичните, хидроструйните и криогенните методи могат да бъдат класифицирани като средства за разкомплектоване и осигуряване на достъп до разривния заряд, а механичното, водоструйното и термичното извличане – като начини за отделянето на взривното вещество от корпуса на артилерийския снаряд. Изгарянето, детонационното унищожаване на взривното вещество, плазменото и химичното разграждане са методи, използвани за окончателно обезвреждане на извлечените енергетични материали.

Основната разлика между унищожаването и последователната обработка е дали металните части и енергетичните материали се разделят предварително. При непосредственото унищожаване те се обработват заедно, което ограничава възможностите за събиране и рециклиране на металните части поради тяхното раздробяване и разпръскване при взрива. При последователната обработка

материалите се разделят, но извлечените взривни вещества и барути трябва да бъдат окончателно обезвредени.

3.1. Сравнение на методите по технологична приложимост

При комплектованите боеприпаси унищожаването може да се извърши чрез взривяване на открито или в детонационна камера. Взривяването на открито може да се приложи и при силно повредени или корозирали боеприпаси, които не позволяват безопасно разкомплектоване и при които използването на други методи е невъзможно или нецелесъобразно. Използването на детонационна камера е ограничено от размерите на боеприпаса и ограничението за допустимото количество взривно вещество в съоръжението [4].

При методите за отваряне на корпуса изборът зависи от конструкцията, материала и дебелината на корпуса, а при методите за извличане – от вида и физичното състояние на пълнежа. Механичните и хидроструйните методи въздействат пряко върху корпуса, докато при криогенното фрактуриране той се охлажда преди последващото механично разрушаване. При извличането термичният метод е ограничен до топими взривни вещества, водоструйният – до пълнежи, които могат да бъдат раздробени и отмити, а пресовото избутване – до заряди, които могат да бъдат отделени цели или на по-големи части [2, 9].

Методите за разкомплектоване, осигуряване на достъп и извличане не завършват демилитаризацията, поради което след тях се избира отделен метод за окончателно обезвреждане на извлечения материал.

3.2. Сравнителна оценка на безопасността, въздействието върху околната среда и ресурсната ефективност

При унищожаването характерът на опасните въздействия е пряко свързан с образуваните продукти на взрива. Взривяването е свързано с ударна вълна, осколки и фугасен ефект, а изгарянето на открито – с висока температура, възможност за разпространение на пожар и отделяне на вредни газове [3, 5]. Провеждането на тези процеси в затворено съоръжение не премахва опасността, но ограничава разпространението ѝ извън съоръжението.

При осигуряването на достъп до разривния заряд механичното рязане е свързано с удар, триене, искрообразуване и местно нагряване. При хидроструйното рязане липсва пряк контакт с метален режещ инструмент, което намалява вероятността от искрообразуване [7]. При криогенното фрактуриране са необходими криогенен агент, подходящи средства за защита при работа с него и последващо контролирано механично натоварване. От екологична гледна точка съществено е дали образуваните продукти остават в границите на технологичното съоръжение. При взривяването и изгарянето на открито газовете и твърдите остатъци се разпространяват в околната среда и не могат да бъдат напълно събрани. Затворените детонационни, термични и плазмени съоръжения позволяват отвеждане на газовете за пречистване и събиране на твърдите остатъци [4, 6]. При водоструйните и химичните методи се образуват замърсени води и други течни или твърди продукти, които подлежат на последващо третиране [8].

За ресурсното оползотворяване определящо е дали металните части се отделят преди окончателното обезвреждане на енергетичните материали. При взривяването

на открито металът се раздробява и разпръсква, а в детонационната камера остатъците могат да бъдат събрани, без да се запази тяхната цялост. Механичното разкомплектоване, хидроструйната обработка и криогенното фрактуриране позволяват предварително отделяне на метала, който след почистване може да бъде рециклиран. При тези методи обаче разривният заряд остава необезвреден и трябва да бъде извлечен и подложен на окончателно обезвреждане.

3.3. Сравнителна таблица на методите за демилитаризация

В таблица 3.1 методите са съпоставени според мястото им в процеса на демилитаризация, ограниченията при прилагането им и възможностите за контрол на образуваните отпадъци и оползотворяване на металните части.

Таблица 3.1. Сравнителна характеристика на методите за демилитаризация

Метод	Място в процеса на демилитаризация	Безопасност и основни ограничения	Екологични и ресурсни характеристики
Взривяване на открито	Унищожаване на комплектования артилерийски изстрел или окончателно обезвреждане на отделно извлечени взривни вещества.	Изисква специално оборудвана площадка поради действието на ударната вълна и разпространението на продуктите на взрива. Приложението зависи от характеристиките на площадката и допустимото количество взривно вещество.	Отделяне на вредни емисии в околната среда и ограничени възможности за събиране и рециклиране на металните осколки.
Взривяване в детонационна камера	Унищожаване на комплектовани артилерийски изстрели, техни елементи и взривни вещества в затворена детонационна камера.	Разрушителното действие на взрива е ограничено в детонационната камера. Възможно е дистанционно подаване и управление. Размерите на обработваните изделия и количеството на взривното вещество са ограничени от вместимостта и допустимия заряд на камерата.	Газовете могат да бъдат пречистени, а металните остатъци – събрани.
Изгаряне на открито	Окончателно обезвреждане предимно на барути и пиротехнически състави чрез контролирано изгаряне на открито.	Изисква мерки срещу разпространението на пожар. Провеждането зависи от условията на площадката и допустимите количества.	Газообразните продукти не се улавят и пречистват, а твърдите остатъци не могат да бъдат напълно събрани.
Изгаряне в затворено съоръжение	Окончателно обезвреждане на извлечени енергетични материали и	Процесът протича в изолирано съоръжение и може да бъде контролиран. Необходими са специализирано оборудване и система за пречистване на	Газовете могат да бъдат пречистени, а твърдите остатъци – събрани.

	замърсени отпадъци чрез контролирано изгаряне в затворено съоръжение.	газовете.	
Механично разкомплекто-ване	Разделяне на основните и допълнителните елементи на артилерийския изстрел.	Безопасността зависи от техническото състояние на артилерийския изстрел. Методът е приложим само към елементи, чиято конструкция позволява разглобяване. Необходимо е последващо обезвреждане на отделените взривни вещества.	При самото разкомплектоване не се образуват газообразни продукти от горене или взривяване. Методът позволява разделяне и последващо рециклиране на материалите, когато това е възможно. Необходимо е процесът да бъде строго контролиран, за да се предотвратят прекомерното нагряване и искрообразуването.
Рязане, пробиване и пресоване	Осигуряване на достъп до разривния заряд чрез нарушаване на целостта на корпуса.	Необходимо е процесът да е строго контролиран, за да не се позволи прекомерно нагряване или искрообразуване. Приложимостта зависи от конструкцията, материала и дебелината на корпуса, както и от вида на снаряжението.	Образуват се замърсени твърди остатъци. Металът може да бъде рециклиран след почистване от остатъците от енергетични материали.
Хидроструйно рязане	Рязане на корпуса и осигуряване на достъп до разривния заряд.	Ограничава нагряването, намалява вероятността от искрообразуване и позволява дистанционно управление. Изисква специално оборудване за високо налягане.	Образува се замърсена вода, която трябва да бъде пречистена. Металните части могат да бъдат отделени и рециклирани.
Криогенно фрактуриране	Криогенно охлаждане на корпуса с цел понижаване на неговата пластичност и повишаване на склонността му към крехко разрушаване,	Криогенното охлаждане може временно да понижи чувствителността към удар, но не осигурява окончателно обезвреждане на взривното вещество. Усложняване на метода поради необходимостта от работа с криогенна течност.	При процеса не се използват химични реагенти. Металните части могат да бъдат почистени и рециклирани.

	последвано от контролирано механично натоварване за осигуряване на достъп до разривния заряд.		
Водоструйно извличане	Раздробяване и отмиване на взривното вещество от корпуса.	Позволява дистанционно управление и не предизвиква съществено нагряване на взривното вещество. Необходимо е оборудване за работа с високо налягане, а приложимостта зависи от вида и физичното състояние на взривното вещество.	Образува се значително количество замърсена вода. Металният корпус се запазва за рециклиране.
Термично извличане	Извличане на топими взривни вещества чрез контролирано нагряване.	Необходим е точен контрол на температурата. Методът е приложим само към топими взривни вещества.	Възможно е образуване на пари и замърсени остатъци. Корпусът се запазва.
Плазмено разрушаване	Окончателно разграждане на извлечени енергетични материали и замърсени отпадъци.	Процесът протича в затворено съоръжение. Необходими са значително енергоснабдяване и сложно оборудване.	Газовете могат да бъдат пречистени, а остатъците – събрани. Металите се отделят предварително.
Химично разграждане	Химично преобразуване на предварително извлечени енергетични материали.	Необходим е контрол при работа с реагентите. Приложимостта зависи от химичния състав на обработвания материал. Получават се течни и твърди отпадъци, които изискват последващо третиране.	

Заключение

На база на извършеното сравнение могат да бъдат идентифицирани два основни начина за организиране на демилитаризацията: чрез унищожаване на боеприпаса или чрез последователно разделяне на конструктивните му части и извличане на енергетичните материали.

Взривяването има широка приложимост и е особено подходящо при артилерийски изстрели, чието техническо състояние не позволява безопасно разкомплектоване.

При провеждане на открито взривяване обаче контролът върху газовете и твърдите остатъци е ограничен, а възможностите за оползотворяване на металните части са малки.

Затворените съоръжения не премахват опасните въздействия, но ограничават разпространението им и позволяват пречистване на газовете и събиране на остатъците. Приложението им се ограничава от допустимите размери и количества на обработваните боеприпаси, както и от сложността и разходите за експлоатация.

Последователната обработка създава по-добри условия за отделяне и рециклиране на метала, но увеличава броя на технологичните етапи, а извлечените взривни вещества и барути трябва да бъдат окончателно обезвредени. При осигуряването на достъп до разривния заряд механичните методи са свързани с удар, триене и нагряване, хидроструйните – с образуване на замърсени води, а криогенното фрактуриране – с рисковете при работа с криогенна течност и последващо механично разрушаване. Основният метод при криогенното фрактуриране е промяната на механичното поведение на корпуса при подлагането му на ниски температури, но при метода остава нуждата от последваща обработка на взривното вещество. Поради това методът има място като подготвителен етап за осигуряване на достъп до разривния заряд, след който са необходими извличане и окончателно обезвреждане на енергетичния материал.

Източници

1. Грозев, В. И., Лазов, Н. К., & Казаков, И. Т. (1996). Бойни припаси: Учебник за курсантите от ВВУАПВО „П. Волов“ – Шумен. Шумен: ВВУАПВО „П. Волов“.
2. Wilkinson, J., & Watt, D. (2006). *Review of demilitarisation and disposal techniques for munitions and related materials* (Report No. L-118). Brussels, Belgium: Munitions Safety Information Analysis Center. Retrieved from https://www.msiac.nato.int/publication/l-118-review-of-demilitarisation-and-disposal-techniques-for-munitions-and-related-materials/
3. United Nations Office for Disarmament Affairs. (2021). *IATG 10.10:2021[E]: Demilitarization, destruction and logistic disposal of conventional ammunition* (3rd ed.). New York, NY: United Nations. Retrieved from https://data.unsaferguard.org/iatg/en/IATG-10.10-Demilitarization-destruction-logistic-disposal-IATG-V.3.pdf
4. U.S. Environmental Protection Agency. (2019). *Alternative treatment technologies to open burning and open detonation of energetic hazardous wastes: Final report* (EPA 530-R-19-007). Washington, DC: Office of Resource Conservation and Recovery. Retrieved from https://www.epa.gov/hwpermitting/report-about-alternative-technologies-open-burning-and-open-detonation-hazardous-waste
5. Organization for Security and Co-operation in Europe. (2008). *OSCE handbook of best practices on conventional ammunition*. Vienna, Austria: OSCE. Retrieved from https://www.osce.org/fsc/33371

6. Lasher, M., & Mescavage, G. (2000). Safe disposal of pyrotechnic ordnance using a plasma treatment system. *Waste Management, 20*(5–6), 425–433. https://doi.org/10.1016/S0956-053X(00)00006-4
7. Campos, J., Fernandes, R., Matos, F., & Pires, A. (1997). Abrasive water jet cutting of munitions and explosive incineration in a fluidised bed. In H. H. Krause (Ed.), *Conversion concepts for commercial applications and disposal technologies of energetic systems* (NATO ASI Series, Vol. 14, pp. 227–245). Dordrecht, the Netherlands: Springer. https://doi.org/10.1007/978-94-017-1175-3_26
8. Getty, H. L., Miller, P. L., Cypher, M. S., Lamon, J. H., Hatz, D. P., Garrison, M. M., Hill, L. D., Martinson, D. A., Reynolds, R. E., & Munoz, J. P. (1998). *High pressure washout of explosives agents* (U.S. Patent No. 5,737,709). Washington, DC: U.S. Patent and Trademark Office. Retrieved from https://patents.google.com/patent/US5737709A/en
9. National Academies of Sciences, Engineering, and Medicine. (2019). *Alternatives for the demilitarization of conventional munitions*. Washington, DC: The National Academies Press. https://doi.org/10.17226/25140
10. Павловец, Г. Я., Мелешко, В. Ю., Эпинатьев, И. Д., & Рощин, А. В. (2017). Безопасная ликвидация взрывчатых веществ нитраминового ряда. *Химическая безопасность, 1*(2), 166–175. https://doi.org/10.25514/CHS.2017.2.10991
11. Conev, C. G., & Antonov, S. I. (2021). A conceptual framework for the utilization process of excess ammunition in the Republic of Bulgaria. In *Proceedings of International Scientific Conference "Defense Technologies" DefTech 2021* (pp. 273–278). Shumen, Bulgaria: "Vasil Levski" National Military University. Retrieved from https://dtf.aadcf.nvu.bg/wp-content/uploads/2022/10/DTF_2021_2.pdf
12. Conev, C. G., & Antonov, S. I. (2020). Influence of superfluous material resources class five—ammunition on the modernization of the Bulgarian Army and national security risks arising from the large amount of superfluous ammunition in the army. In *Proceedings of International Scientific Conference "Defense Technology Forum 2020"* (pp. 195–200). Shumen, Bulgaria: "Vasil Levski" National Military University. Retrieved from https://dtf.aadcf.nvu.bg/wp-content/uploads/2022/10/DTF_2020.pdf

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

SURVEY OF THE CONDITION OF TECHNICAL OBJECTS

Andrei I. Bogdanov

Konstantin Preslavski University Of Shumen, Shumen 9712, 115 Universitetska Str
a.bogdanov@shu.bg

Absrtact *A methodology for extending the technical service life of technical objects is proposed. An example is examined in which criteria for assessing the technical condition of the products have been selected and the boundary conditions have been defined. An approach for predicting the condition of technical objects is used.*

Keywords*: technical service, technical condition*

ИЗСЛЕДВАНЕ СЪСТОЯНИЕТО НА ТЕХНИЧЕСКИТЕ ОБЕКТИ

Андрей И. Богданов

Резюме: *Предложена е методика за удължаване срока за техническа годност на технически обекти. Разгледан е пример, при който са избрани критерии за оценка техническото състояние на изделията и са определени ограничителните условия. Използван е подход за прогнозиране състоянието на техническите обекти*

Въведение

В последните години в БА се експлоатират различни образци въоръжение, които имат определен остатъчен ресурс, но се експлоатират и системи чийто ресурс е изтекъл. Това поставя изискването, за удължаване на техният експлоатационен срок, или експлоатационният срок на отделни изделия от системите на въоръжение, като пневматични агрегати, системи за управление и други.

Изложение

Задачата за удължаване срока за техническа годност е отговорна и трудна, защото в много случаи касае живота не само на обслужващия персонал, а при по сложни изделия, като летателни апарати, ракети и самолети, може да засегне живота и на мирни граждани.

При удължаване срока за техническа годност на техническите изделия трябва да се подхожда индивидуално, при отчитане индивидуалните особености на всяко изделие.

Най-важната подготвителна работа, която трябва да се извърши е да се изберат характеристиките, които ще бъдат изследвани и да се изберат граничните условия, до които е допустимо експлоатацията на изделията.

При избора на величини за изследване, те трябва така да бъдат подбирани, че да характеризират основното предназначение на техническият обект или такива

величини, които отчитат тяхното техническо състояние. При избора им трябва да се изхожда от устройството и предназначението на съответния технически обект. Друго важно условие при избора на техническите характеристики е, да бъдат така подбрани, че да могат да бъдат лесно измерими или оценими.

При избора на граничните условия до които се допуска експлоатацията на изделията се изхожда от техните технически задания, указанията на инструкциите за експлоатация, инструкциите за категоризация и други правилници или инструкции, касаещи експлоатацията на изделията. При липса на конкретни гранични стойности за отделни характеристики, могат да се използват стойностите на международно приетите стандарти, от серията ISO, DIN, VDI, BS, CDA и други

При изпитание на изделия, като жироскопи,пневматични уреди и други е лесно да се използват методите на безразрушителният контрол, но съществуват и материали и оборудване, като бронежилетки, при които е невъзможно прилагането на тези методи.

Едно от изделията, за които най-често се налага удължаване срока за техническа годност, това са жироскопите.Те могат да комплектоват системите за управление на пилотни и безпилотни летателни апарати, торпедни комплекси и други.Обикновено се използват тристепенни, астатични жироскопи, служещи да измерват ъгловото разсъгласуване на управлявания обект [2].

Примерът, който ще бъде разгледан е изпитания с жироскопи за направление от системата за управление на безпилотните летателни апарати. За целта се налага да се извършат комплекс от дейности в последователност посочена на Фиг.1.



Фиг. 1: Алгоритъм на операциите при проверка на жироскопични измервателни средства

Спазвайки изискванията на паспортно-техническата документация се извършва автономна проверка на жироскопичните измервателни средства и се дефинират граничните стойности на нарушените параметри

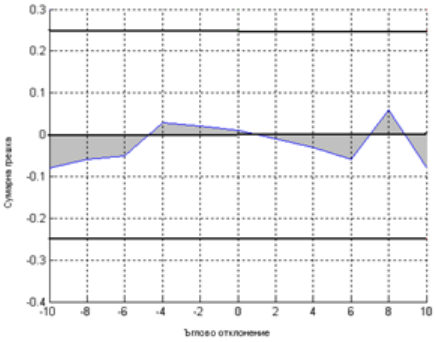
Калибрирането се извършва в работния диапазон, като се вземат в предвид и влиянието на натоварва-щите фактори имащи отношение към оценката за точност. Изработената измервателна верига е показана на фиг2.

За да се получи информация за състоянието но жироскопичните из-мервателни средства се измерва изходният сигнал изработван от уреда при стъпка за задаване на ъглови отклонения от 2 градуса. При построяване на статичната характеристика се получа-ва информация за състоянието на уреда в целия му работен диапазон. Отклоненията на реалната статична характеристика спрямо номиналната характеризират грешката на уреда.



Фиг. 2: Измервателна верига за калибриране

Получената характеристика представя единият от факторите ха-рактеризиращи състоянието на жироскопичните измервателни средства. За да се вземе решение за удължаване техният срок на експлоатация се използва вибрационния спектър генериран при работа на уредите.



Фиг. 3: Статична характеристика на уреда

Приема се условието, че екс-плоатацията на жироскопичните измервателни средства се извършва в интервала от време [*0, T*]. В процеса на работа на уредите чувствителния елемент е подложен на най – големи знакопроменливи натоварвания, предизвикващи нарастване на грешките на измерване и преобразуване. Това налага грешката от контрола да се разглежда като резултат от

външни и вътрешни флуктоации сумирани с грешката от измервателната процедура. За греш-ката е известно, че нейната стойност не превишава определена допустима стойност. При нейното определяне се използва неравенството:

$$|\varepsilon(t)| \le \delta(t), \qquad t \in [t_0, t_p] \tag{1}$$

Контрола се извършва интервала [t_0, t_p], а получения резултат е в отрязъка от реализацията *z(t)* определена от израза:

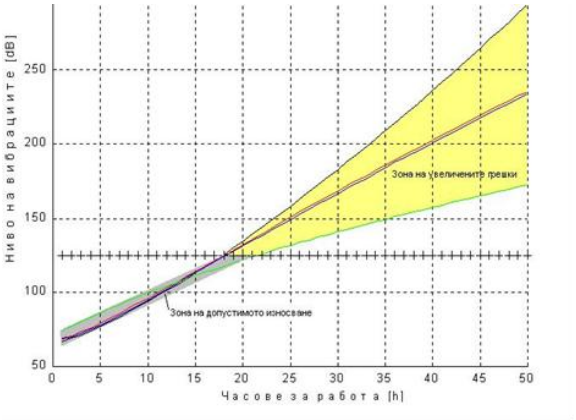
$$z(t) = \le y(t) + \varepsilon(t) \qquad t \in [t_0, t_p] \tag{2}$$

На основата на съотношения (1) и (2) се получава:

$$z(t) - \delta(t) \le y(t) \le z(t) + \delta(t) \quad t \in [t_0, t_p] \tag{3}$$

Следователно в интервала [t_0, t_p] реализацията на линейното ниво на вибрациите се заключва в опреде-лена "зона". Тя е ограничена минимално от функциите $f(t) = z(t) - \delta(t)$, а максимума се фиксира от $g(t) = z(t) + \delta(t)$. В границите на тази "зона" образувана от функциите *f(t)* и *g(t)* се построяват множество от криви от вида $\sum_{i=0}^{m} \alpha_i \phi(t)_i$ които се наричат допустими.

Построяването на такава графика има вида показан на фиг 4.



Фиг. 4. Скала за прогнозиране техническото състояние

Съгласно ISO 2372/74 границата между нивата "удовлетворил" и "допустимо" е *125 dB*. Тази стойност определя двете зони на фиг.4 – "зона на допустимото износване" и "зона на увеличените грешки". Срока за техническа годност на изследваните жироскопични измервателни средства се удължава, ако нивото на

измерените вибрации е в зоната на допустимото износване. Анализа на фигурата показва, че при измерено ниво на вибрациите от *60 dB* срока за техническа годност може да бъде удължен с 20 часа. При измерено ниво на вибрациите над *125dB* удължаване срока за техническа годност не се препоръчва поради увеличаване на грешките над допустимите стойности за този вид измервателни средства.

Заключение

Използването на предложеният подход дава обективен критерии с колко може да бъде удължен срока на техническа годност на изследваните измервателни средства. Той дава възможност да се прогнозира какъв е запасният ресурс на уредите чрез използване на графиките за нарастване нивото ва вибрациите и сумарната грешка.

Литература

1. Абрамов О.В., Розенбаум А. Н., Прогнозирование состояния технических систем, Наука, Москва, 2011.
2. Силин В. Б., Заковряшин А. И., Автоматическое прогнозирование состояния аппаратуры управления и наблюдения, Энергия, Москва, 2003.
3. Свешников А. А., Ривкин С. С., Вероятностные методы в прикладной теории гироскопов, Наука, Москва, 2004.
4. Berry J. E., How to Track Roling Element Bearing Health with Vibratio Signsture Analisis. Sound and Vibration № 11 pp. 24 – 35, 1991
5. Баранов И. А., Галкин В. Е., Родинов Е.М., Рузаев М.П., Исследование частот собственных колебании равножестких сколзящих токоподводов без контактного выступа приборов сб. Гироскопы производство и иследование, Машиностроение, стр.171-174, 1969.
6. ISO 2372: 74, Systems for Faul Detection, Prediction and Analysis on Machinary and Critical Machine Parts
7. Liaw D. S., Yen W. L., Chiz C. C., Nonlinear Control For Mussile Terminal Guidance, Journal of Dynamic Systems, Measurement and Control Vol. 122 Issue 4 December pp. 663 – 668, 2000

ADAPTED ANALYSIS OF THE IMPACT OF CRISES IN THE BLACK SEA REGION ON THE NATIONAL SECURITY OF THE REPUBLIC OF BULGARIA

Anastas M. Chitakov

National Military University "V. Levski", Artillery, "Air Defense and CIS" Faculty
Shumen, "K. Scorpil"str. № 1

Abstract: *This paper analyzes the impact of crises in the Black Sea region on the national security of the Republic of Bulgaria through an adapted SWOT analysis. Based on the research results, the main strengths, weaknesses, opportunities, and threats affecting the resilience of the national security system are systematized. The main risks are identified, and key directions for strengthening national resilience and improving security policies are outlined.*

Keywords: *Black Sea region, national security, SWOT analysis, risks, threats, national resilience.*

АДАПТИРАН АНАЛИЗ НА ВЪЗДЕЙСТВИЕТО НА КРИЗИТЕ В ЧЕРНОМОРСКИЯ РЕГИОН ВЪРХУ НАЦИОНАЛНАТА СИГУРНОСТ НА РЕПУБЛИКА БЪЛГАРИЯ

Анастас М. Читаков

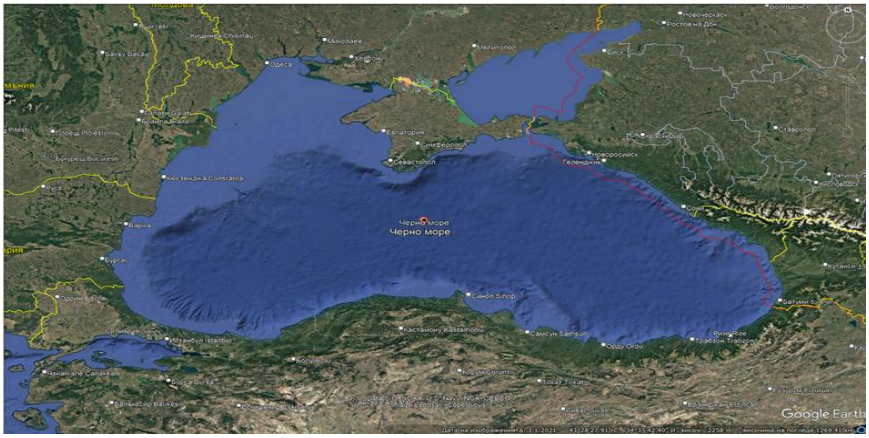
Национален Военен Университет „Васил Левски", Факултет „Артилерия, ПВО и КИС" – гр. Шумен, ул. Карел Шкорпил № 1

Резюме: *Настоящият доклад анализира въздействието на кризите в Черноморския регион върху националната сигурност на Република България чрез адаптиран SWOT анализ. Въз основа на резултатите от изследването са систематизирани основните силни и слаби страни, възможности и заплахи, влияещи върху устойчивостта на националната система за сигурност. Идентифицирани са основните рискове и са очертани ключови направления за повишаване на националната устойчивост и усъвършенстване на политиките за сигурност.*

Ключови думи: *Черноморски регион, национална сигурност, SWOT анализ, рискове, заплахи, национална устойчивост.*

1. Въведение

Черноморският регион се утвърждава като стратегическо пространство с нарастващо значение за европейската и евроатлантическата сигурност. Неговото географско положение, ролята му за енергийните, транспортните и търговските комуникации, както и пресичането на интересите на регионални и глобални актьори формират сложна и динамична среда за сигурност.



Източник: Google Earth

Военните конфликти, геополитическото противопоставяне, енергийните зависимости, хибридните въздействия, кибератаките и трансграничните процеси показват, че рисковете в Черноморския регион имат взаимосвързан и мултифакторен характер. Тяхното въздействие надхвърля националните граници и създава предпоставки за пренасяне на нестабилност между отделните сфери на сигурността. Анализът на кризите в региона показва именно способността на локалните процеси да придобиват регионално и международно значение.

За Република България тези процеси имат непосредствено значение поради географското ѝ положение, членството в Европейския съюз и НАТО и зависимостта на националната сигурност от устойчивостта на регионалната политическа, военна, енергийна и икономическа среда. Това налага не само идентифициране на основните рискове и заплахи, но и оценяване на тяхното въздействие и определяне на възможностите за повишаване на националната устойчивост.

В този контекст целта на настоящия доклад е чрез адаптиран SWOT анализ да бъдат систематизирани основните вътрешни и външни фактори, определящи въздействието на кризите в Черноморския регион върху националната сигурност на Република България, и да бъдат приоритизирани основните рискове чрез прилагане на матрица на риска.

Получените резултати създават основа за извеждане на стратегически направления за ограничаване на уязвимостите и повишаване на устойчивостта на националната система за сигурност.

Методологична основа на анализа

Методологичният подход е насочен конкретно към оценяване на въздействието на рисковете и заплахите, произтичащи от кризите в Черноморския регион, върху

националната сигурност на Република България, а не към цялостна оценка на националната сигурност.

Анализът се основава на съчетаването на системен и сравнителен анализ, SWOT анализ и матрица на риска. Системният подход позволява разглеждането на геополитическите, военните, икономическите, енергийните, социалните, институционалните и киберфакторите като взаимосвързани елементи на средата за сигурност. Сравнителният анализ подпомага установяването на зависимости между отделните фактори, а SWOT анализът систематизира вътрешните силни и слаби страни и външните възможности и заплахи. Разработената в дисертацията методика следва именно комплексното приложение на взаимно допълващи се аналитични инструменти.

За целите на настоящия доклад SWOT моделът е адаптиран към въздействието на кризите в Черноморския регион върху Република България. Вътрешните характеристики се разглеждат като фактори, определящи способността на държавата да реагира на регионални кризи, докато възможностите и заплахите отразяват основни процеси във външната среда.

SWOT анализът се допълва от матрица на риска, основана на два основни показателя – вероятност за проявление и степен на въздействие върху националната сигурност. По този начин се преминава от общо систематизиране на факторите към тяхното степенуване и приоритизиране, което създава аналитична основа за формулиране на конкретни мерки и политики. Този подход е заложен и в методиката на дисертационното изследване.

Адаптиран SWOT анализ на въздействието на кризите в Черноморския регион върху националната сигурност на Република България

За оценяване на въздействието на кризите в Черноморския регион върху националната сигурност на Република България е приложен адаптиран SWOT анализ. Неговото използване позволява систематизиране на вътрешните характеристики на националната система за сигурност и факторите на външната среда, произтичащи от регионалната динамика.

За целите на анализа силните и слабите страни се разглеждат като вътрешни характеристики, определящи способността на държавата да реагира на кризисни въздействия, докато възможностите и заплахите отразяват основните процеси във външната среда. По този начин класическият SWOT модел се адаптира към спецификата на изследването и позволява да се установи връзката между националните способности и рисковете, генерирани в Черноморския регион.

Таблица 1. Адаптиран SWOT анализ на въздействието на кризите в Черноморския регион върху националната сигурност

СИЛНИ СТРАНИ (S)	**СЛАБИ СТРАНИ (W)**
Членство в ЕС и НАТО	Енергийна зависимост
Механизми на колективната сигурност	Демографски проблеми
Геостратегическо положение	Институционални дефицити
Достъп до европейски и съюзнически ресурси	Корупционни уязвимости
ВЪЗМОЖНОСТИ (O)	**ЗАПЛАХИ (T)**
Енергийна диверсификация	Геополитическо напрежение и военна ескалация
Регионално и съюзническо сътрудничество	Хибридни въздействия и дезинформация
Инфраструктурна и транспортна свързаност	Кибератаки
Дигитализация и развитие на националните способности	Миграционен натиск и трансгранични рискове

Източник: Авторска разработка

Резултатите показват, че основните силни страни на Република България произтичат от членството в ЕС и НАТО и свързаните с него механизми за колективна отбрана, политическа координация и достъп до съюзнически ресурси. Геостратегическото положение на страната също има двоен характер – то повишава значението на България за Черноморския регион, но едновременно увеличава непосредственото ѝ излагане на регионални кризи.

Като основни слаби страни се открояват енергийната зависимост, неблагоприятните демографски процеси, институционалните дефицити и корупционните уязвимости. Тяхното значение се определя от възможността външни кризисни процеси да използват или задълбочават съществуващи вътрешни слабости и по този начин да намаляват устойчивостта на националната система за сигурност.

Сред възможностите с най-голямо значение са диверсификацията на енергийните източници и маршрути, задълбочаването на регионалното и съюзническото взаимодействие, развитието на инфраструктурната свързаност и дигитализацията. Реализирането им създава предпоставки за ограничаване на стратегическите зависимости и повишаване на националната устойчивост.

Основните заплахи произтичат от геополитическото противопоставяне и риска от военна ескалация, хибридните въздействия и дезинформацията, кибератаките и миграционния натиск. Специфична особеност е тяхната взаимна обусловеност – военна или политическа криза може едновременно да генерира енергийни, икономически, информационни, кибернетични и миграционни последствия.

Съпоставяне на факторите

Адаптираният SWOT анализ показва, че въздействието върху националната сигурност се определя не само от наличието на отделни заплахи, а от

взаимодействието между външните рискове и вътрешните уязвимости. Това позволява да бъдат изведени четири основни стратегически зависимости:

- **S–O:** използване на членството в ЕС и НАТО за развитие на енергийна, инфраструктурна и отбранителна устойчивост;
- **S–T:** използване на съюзническите механизми и националните способности за противодействие на военни, хибридни и киберзаплахи;
- **W–O:** използване на европейското и регионалното сътрудничество за ограничаване на енергийните и институционалните уязвимости;
- **W–T:** приоритетно намаляване на вътрешните слабости, които могат да усилят въздействието на външните кризисни фактори.

Това съпоставяне придава на SWOT анализа не само описателен, а приложен характер, тъй като създава основа за последващо приоритизиране на рисковете и формулиране на мерки за сигурност.

Адаптираният SWOT анализ показва, че Република България разполага със значими съюзнически и геостратегически предимства, но тяхната ефективност зависи от способността за ограничаване на вътрешните уязвимости. Следователно повишаването на националната устойчивост изисква съчетаване на национални способности, съюзническо взаимодействие, енергийна диверсификация, институционална устойчивост и защита срещу хибридни и киберзаплахи.

Заключение

Проведеният адаптиран SWOT анализ показва, че въздействието на кризите в Черноморския регион върху националната сигурност на Република България се определя от взаимодействието между външните рискове и вътрешните уязвимости на националната система за сигурност. Членството в ЕС и НАТО и механизмите на колективната сигурност създават съществени възможности за повишаване на националната устойчивост, докато енергийните, институционалните и демографските уязвимости могат да усилят въздействието на регионалните кризи.

Резултатите обосновават необходимостта от интегриран подход, основан на ограничаване на стратегическите зависимости, укрепване на институционалната и киберустойчивостта, защита на критичната инфраструктура и задълбочаване на съюзническото и регионалното взаимодействие. Адаптираният SWOT анализ може да се използва като приложен инструмент за систематизиране на факторите на средата и подпомагане на процесите по стратегическо планиране в областта на националната сигурност.

Използвана литература

1. Бек, У. (2001). Световното рисково общество. София: Обсидиан.
2. Манев, Е. (2012). Глобална, регионална и национална сигурност. София: Софттрейд.
3. Слатински, Н. (2010). Петте нива на сигурността. София: Военно издателство.

4. Grotzky, D., & Isic, M. (2008). The Black Sea Region: Clashing Identities and Risks to European Stability. Center for Applied Policy Research.
5. New Strategy Center & LSE IDEAS. (2024). Security Challenges in the Black Sea Region.
6. Atlantic Council. (2024). A Security Strategy for the Black Sea.
7. RUSI – Royal United Services Institute. (2024). The Black Sea's Significance to European Security.
8. NATO. (2024). Annual Report 2023.

MILITARY-TECHNOLOGICAL ASYMMETRY IN THE ALGORITHMIC ERA: RECONCEPTUALIZATION OF STRUCTURAL NEOREALISM AND THE PHENOMENON OF "ALGORITHMIC VETO"

Dilyan Markov

Rakovski National Defence College, Sofia,, Bulgaria, dlnmarkov@gmail.com

Abstract: *This paper examines the transformation of state power and the balance of power driven by digitalization and AI integration in defense systems. Addressing the limits of structural neorealism, it introduces an expanded framework synthesizing "cognitive and computational power" with "structural power". The study conceptualizes the "Algorithmic Veto" as an innovative tool for non-kinetic deterrence and coercion leveraging software and infrastructural dependencies. It further analyzes the security dilemma and challenges to digital sovereignty within an emerging technological bipolar model.*

Keywords: *structural neorealism, military-technological asymmetry, algorithmic veto, security dilemma, structural power, technological sovereignty.*

ВОЕННО-ТЕХНОЛОГИЧНАТА АСИМЕТРИЯ В АЛГОРИТМИЧНАТА ЕРА: РЕКОНЦЕПТУАЛИЗАЦИЯ НА СТРУКТУРНИЯ НЕОРЕАЛИЗЪМ И ФЕНОМЕНЪТ „АЛГОРИТМИЧНО ВЕТО"

Дилян Марков

Военна академия „Г. С. Раковски", София, България, dlnmarkov@gmail.com

Резюме: *Докладът изследва трансформацията на държавната мощ и баланса на силите в условията на дигитализация и внедряване на изкуствен интелект в отбраната. Поради ограниченията на класическия структурен неореализъм е предложена разширена рамка, интегрираща концепциите за „когнитивна и изчислителна мощ" и „структурна власт". Докладът концептуализира феномена „алгоритмично вето" като нов инструмент за некинетично възпиране и геополитическа принуда чрез софтуерна и инфраструктурна зависимост. Анализирани са предизвикателствата пред дигиталния суверенитет и дилемата на сигурността в нововъзникващия технологичен двуполюсен модел.*

Ключови думи: *структурен неореализъм, военно-технологична асиметрия, алгоритмично вето, дилема на сигурността, структурна мощ, технологичен суверенитет.*

Въведение

Навлизането на генеративния и автономния изкуствен интелект в отбранителния сектор отбелязва повратна точка в парадигмата на международната сигурност, сравнима по своя мащаб с появата на ядреното оръжие. Масовата внедреност на алгоритмично целеуказване [8], мултидомейни операции и автономни платформени комплекси променя физическата скорост, динамиката и характера на съвременния военен конфликт. Тази бърза дигитална и технологична

трансформация разкрива сериозен дефицит в класическия обяснителен апарат на структурния неореализъм. Традиционният модел [17], който измерва държавната мощ предимно през обемни и физически кинетични показатели, се оказва недостатъчен да обясни механизмите за некинетичен натиск, асиметрично възпиране и контрол в дигиталната ера. В съвременната международна система критичната зависимост от изчислителни ресурси, базови невронни модели и специфична хардуерна инфраструктура пренаписва традиционните правила за разпределение на силите. В отговор на тези системни промени настоящият доклад си поставя за цел да предложи разширена теоретична рамка за анализ на държавната мощ, обединяваща концепциите за „когнитивна и изчислителна мощ" и „структурна власт". Чрез този подход се изследва дилемата на сигурността в условията на асиметрично технологично поляризиране и появата на т.нар. „алгоритмични сиви зони". В този контекст изследването концептуализира феномена „алгоритмично вето" като нов инструмент за некинетично възпиране и геополитическа принуда.

1. Теоретична деконструкция на държавната мощ: От кинетичен капацитет към когнитивна и изчислителна мощ

Формулираната от Кенет Уолц [17] класическа рамка на структурния неореализъм определя мощта на държавата чрез материални и количествени показатели. В тази традиционна парадигма силата се материализира във физическото упражняване на принуда и защита на държавните граници.

В дигиталната ера обаче, този кинетично ориентиран модел показва сериозна аналитична недостатъчност. Автономизацията и дигитализацията на отбранителните системи налагат преход към нов категориален апарат, изграден около когнитивна и изчислителна мощ. Този нов вектор на държавен капацитет синтезира три фундаментални и взаимосвързани компонента:

– Капацитет за обработка на масиви от данни. Изразяващ се в способността за събиране, филтриране и анализиране в реално време на информация от сензори, спътникови мрежи, киберпространството и открити източници.

– Изчислителен капацитет. За разлика от софтуера и данните, изчислителната мощ притежава ясни физически ограничения [12]. Тя е количествено измерима, физически откриваема и силно зависима от силно концентрирани глобални вериги за доставки. Поради това изчислителният капацитет се превръща в най-надеждния материален измерител за реалните възможности на държавата свързани с ИИ.

– Алгоритмична автономност, отразяваща скоростта, прецизността и автономността на математическите модели при алгоритмично сплитане на сензорни данни и автоматизирана поддръжка за вземане на решения.

Тази трансформация на материалната мощ придобива цялостен теоретичен контур, когато се пречупва през концепцията на Сюзън Стрейндж [16] за „Структурната власт" и в частност нейния стълб, свързан със структурата на знанието и технологиите. Доминиращите държави (технологичните полюси) не просто принуждават своите съперници, а контролират самите протоколи,

алгоритмични стандарти, изкуствен интелект и облачни архитектури, върху които функционира глобалният отбранителен сектор. По този начин технологичният полюс контролира самата когнитивна матрица, през която останалите участници възприемат, анализират и реагират на заплахите в международната среда.

В този контекст се извършва фундаментална промяна в самата топология на държавната мощ - от пространствено-териториална към мрежово-алгоритмична. Ако в класическия неореализъм суверенитетът е физически неделим и се защитава чрез кинетични граници, в дигиталната ера, контролът върху физическата инфраструктура генерира т.нар. „оръжейна мрежовост". Държавите, контролиращи ключовите възли в глобалната дигитална и изчислителна архитектура, придобиват способността асиметрично да наблюдават, филтрират или прекъсват информационните и оперативните потоци на останалите участници. По този начин когнитивната и изчислителната мощ превръщат дигиталната зависимост на по-малките страни в постоянен източник на стратегическа уязвимост.

2. Технологична асиметрия, двуполюсен модел и ускоряване на дилемата на сигурността

Съвременната международна система претърпява процес на асиметрично технологично поляризиране. Изследванията върху геополитиката на изчислителната мощ показват, че за разлика от алгоритмите и данните, компютърните ресурси се характеризират с това, че са физически измерими и изключващи се [14]. Тъй като веригата за производство на напреднали микропроцесори и оборудване разчита на изключително концентрирани вериги за доставки, САЩ инструментализират тази физическа асиметрия чрез регулаторни рамки за разпространение на изкуствения интелект и строг експортен контрол. Тези политики целят пряко възпиране на технологичните конкуренти (като Китай) [2], но същевременно налагат фрагментация и сред съюзниците, включително чрез разделяне на държавите от Европейския съюз на категории за достъп до чипове Регулаторната рамка за разпространение на изкуствения интелект, въведена от САЩ през януари 2025 г., класифицира държавите в три категории. Докато 10 държави - членки на ЕС (главно от Западна и Северна Европа), са поставени в първа категория с неограничен достъп, останалите 17 членки (предимно от Централна и Източна Европа) са поставени във втора категория с количествени квоти за внос на AI хардуер. Това разделение предизвика официални опасения от страна на Европейския парламент и Европейската комисия относно целостта на единния пазар и технологичния суверенитет на Съюза [3].

Същевременно в тази двуполюсна технологична рамка се развиват т.нар. „алгоритмични сиви зони", пространства на конфликт, при които се провеждат интегрирани кампании чрез предимно невоенни средства (включително кибероперации, информационна война и дезинформация), действащи постепенно и под прага на открит конвенционален въоръжен сблъсък [11]. Този тип съперничество пренася геополитическото противопоставяне от традиционния военен театър в критичните дигитални и информационни инфраструктури.

Тъй като подобни действия са проектирани така, че съзнателно да избягват категорични поводи за военна реакция (т.нар. „червени линии"), те генерират значителна стратегическа двусмисленост. В условията на технологична асиметрия тази несигурност допълнително засилва дилемата на сигурността: държавите са принудени да третират всеки цивилен технологичен напредък или експортно ограничение на съперника като потенциална заплаха с двойна употреба, което стимулира последваща фрагментация и превантивна защитна ескалация.

За разлика от класическата реалистична парадигма, в която държавната мощ се измерва предимно чрез физическия обем на конвенционалните въоръжени сили и ядрения арсенал, дигиталната ера трансформира природата на геополитическото съперничество. В киберпространството ниските прагове за навлизане и разпределеният характер на технологиите създават значителна асиметрия. Това позволява на страни с ограничен традиционен военен капацитет да развиват стратегии за несиметрично въздействие. Чрез тях те могат ефективно да парализират критична инфраструктура, да нарушават функционирането на ключови сектори и да подкопават институционалната стабилност на високотехнологично развитите държави, чиято дигитална зависимост генерира нови системни уязвимости [13].

Подобни действия експлоатират вътрешносоциалните и дигитални уязвимости, без да променят фундаментално системния баланс на силите, но съществено ускоряват и задълбочават дилемата на сигурността в глобален мащаб.

В тази високотехнологична среда класическата дилема на сигурността и стратегическата стабилност претърпяват драматично преформатиране. От една страна, това се дължи на специфичната природа на софтуерните технологии, при които внедряването или актуализацията на ИИ алгоритми остава физически труднозабележимо за разлика от традиционното струпване на конвенционални сили. Тази липса на пълна прозрачност генерира системна несигурност и увеличава рисковете от превантивна ескалация, провокирана от автоматизационни предразсъдъци, алгоритмични грешки и ускоряване на вземането на решения [7]. От друга страна, се появява капанът на модернизацията за средните и малките държави. За да оцелеят в анархичната система, държавите са длъжни да модернизират въоръжението си. Тъй като не разполагат с пълен технологичен цикъл (от производство на чипове до облачна инфраструктура), те са принудени да внасят авангардни софтуерно-дефинирани системи. Така самият опит за гарантиране на сигурност чрез внос генерира екзистенциална технологична уязвимост и критична зависимост от външния доставчик.

Допълнително усложнение на дилемата на сигурността възниква от феномена на т.нар. „черна кутия" при отбранителните ИИ среди. Непрозрачността и липсата на пълна обяснимост на дълбоките невронни мрежи, използвани за целеуказване и оперативен анализ, ограничават капацитета при оценка на реалния боен капацитет на потенциалния противник. Това информационно заслепяване стимулира държавите към превантивно надпреварване във въоръжаването и по-ниски прагове за задействане на превантивни кибер и некинетични удари. При средните и малките държави липсата на достъп до суверенни базови модели и зависимостта от

външен затворен код правят невъзможна верификацията на самите отбранителни алгоритми, което ги излага на риск от скрити уязвимости и алгоритмичен саботаж.

3. Моделиране на феномена „Алгоритмично вето" като механизъм за стратегическо възпиране

Традиционната теория за стратегическото възпиране разчита на държавния монопол върху силата, като съчетава възможността за нанасяне на разрушителен ответен удар с политическата воля за контрол върху ескалацията. Масовата интеграция на изкуствен интелект, автономни отбранителни платформи и софтуерно-дефинирани оръжия обаче променя тази логика и въвежда нов феномен, който тук се дефинира като „Алгоритмично вето". Той изразява способността на външен субект (частен технологичен гигант или доминираща сила) да блокира, ограничава или прекъсва провеждането на бойни операции от дадена страна чрез лостовете на софтуерната, инфраструктурната или алгоритмичната зависимост.

Архитектурата на задействане на алгоритмичното вето надхвърля елементарното физическо прекъсване на дадена система. Тя функционира като многослойна матрица от инфраструктурни, софтуерни и когнитивни зависимости, които се разгръщат на три взаимносвързани нива:

– Инфраструктурно вето: Блокиране, ограничаване или критично забавяне на достъпа до физическата и мрежовата среда, в това число спътникова свързаност, геопространствени спътникови данни и облачна изчислителна мощ. Тъй като съвременните концепции за водене на мрежово-центрична война и многодомейни операции разчитат на непрекъсваем поток от данни в реално време, отказът при тези критични канали лишава автономните платформи от позициониране, целеуказване и оперативна съвместимост.

– Лицензионно и софтуерно вето: Инструментализиране на интелектуалната собственост и софтуерния код чрез прекратяване на поддръжката, отказ от предоставяне на критични актуализации, оттегляне на алгоритмични модели за невронни мрежи или задействане на дистанционни системни прекъсвачи. Това генерира т.нар. ефект на технологично „заключване", при който софтуерно-дефинираните оръжия стават функционално неизползваеми или уязвими на кибератаки без пряката санкция на външния разработчик [6].

– Вето върху когнитивния капацитет: Ограничаване или пълно изолиране на дадена държава от фундаменталните масиви от данни, изчислителни клъстери и алгоритмични оптимизации, необходими за постоянното обучение, калибриране и адаптиране на моделите с ИИ към динамична бойна среда. Тъй като предимството в алгоритмичната война зависи от скоростта на машинно обучение, държавите, изключени от водещите софтуерни архитектури и базови модели, изпадат в системна „когнитивна асиметрия" и бърза оперативна деградация [1].

Практическото изражение на алгоритмичното вето надхвърля рамките на държавния апарат, въвеждайки нов тип участници в геополитическото съперничество - частните технологични корпорации. Чрез притежанието на патенти, облачни архитектури и софтуер, те придобиват ролята на „дигитални пазачи" на националната сигурност. В ситуации на криза тези корпорации могат

едностранно, под държавен натиск или въз основа на собствени корпоративни политики да ограничат достъпа на суверенна държава до критични цифрови услуги и разузнавателни масиви. Това превръща алгоритмичното вето не просто в държавен инструмент за възпиране, а в хибриден механизъм за частно-държавна геополитическа принуда.

Алгоритмичното вето трансформира традиционната представа за внос на оръжие: вместо покупката на дълготраен физически актив, държавите придобиват условна услуга, чиято функционалност остава под постоянния геополитически и правен контрол на доставчика.

Чрез тези механизми алгоритмичното вето фундаментално преформатира механиката на стратегическото възпиране, надграждайки класическите концепции за възпиране чрез наказване и възпиране чрез отрицание [5, 15].

Когато дадена държава изгуби доверие в своя независим капацитет за гарантиран ответен удар поради заплахата от външно софтуерно или инфраструктурно блокиране, се формира т.нар. „пролука в кредибилитета". Тази системна несигурност подкопава фундаменталните допускания за стратегическа стабилност, описвани от теорията на реализма [9, 10].

В резултат се утвърждава феноменът на софтуерно и корпоративно-технологично вето. При него държавите - технологични лидери, съвместно с частните технологични гиганти, контролиращи физическата изчислителна инфраструктура и базовите алгоритмични модели, придобиват право на вето върху това кога, къде и как се провеждат военните действия. За по-малките и средно големите държави тази зависимост означава пряка ерозия на суверения капацитет за вземане на независими военно-политически решения и преминаване към структурна технологична васализация.

Естествената структурна реакция срещу този асиметричен натиск е активизирането на борбата за „Дигитален и технологичен суверенитет" - опити за изграждане на суверенни облачни архитектури, независими сензорно-алгоритмични вериги и собствени изчислителни клъстери [4], целящи да неутрализират уязвимостта от външно алгоритмично вето.

Заключение

Дигитализацията и внедряването на алгоритмични системи за управление в отбраната изискват фундаментално преосмисляне на класическия структурен неореализъм. Понятието за държавна мощ вече не може да се изчерпва с количествените и кинетичните показатели. Контролът върху изчислителния капацитет, алгоритмите за ИИ, данните и облачната инфраструктура се превръща в основен източник на структурна власт в международните отношения.

За малките и средни държави (включително държавите от Източния флаг на НАТО и ЕС) анализираните процеси поставят критични предизвикателства пред националното отбранително планиране. Ограниченият финансов и инфраструктурен ресурс прави изграждането на пълен технологичен цикъл нереалистично. Поради това постигането на относителна технологична устойчивост изисква преминаване от пасивен внос на софтуерно-дефинирани

оръжия към стратегии за „споделен технологичен суверенитет" в рамките на съюзи. Това включва инвестиции в специализирани капацитети и изграждане на нормативни гаранции срещу едностранно задействане на алгоритмично вето от страна на външни доставчици.

Феноменът „алгоритмично вето" пренаписва правилата на възпирането: страните, които използват чужд софтуер, могат да бъдат дистанционно парализирани и лишени от правото сами да управляват своите действия. В резултат на това, технологичните държави-полюси и водещите технологични корпорации се утвърждават като краен арбитър на съвременните конфликти, а борбата за „технологичен суверенитет" се превръща в основна дефиниция за национална сигурност в дигиталната ера.

Литература

1. Allen, G. (2022). Choking off China's Access to the Future of AI. CSIS.
2. Bureau of Industry and Security, (2022. Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification.
3. European Parliament, 2025. US export controls of AI chips: debate with the Commission. News European Parliament.
4. Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. Philos. Technol..
5. Freedman, L. (2024). Deterrence.
6. Horowitz, M. (2019). When speed kills: Lethal autonomous weapon systems, deterrence and stability. Journal of Strategic Studies, 42 (6).
7. Horowitz, M. (2026). Artificial Intelligence and the Future of Strategic Stability. TNSR, 9 (2).
8. Ismailovic, M. (2025). Algorithmic targeting: the role of artificial intelligence in Israeli strikes in Gaza and its ethical implications. GRIP.
9. Jervis, R., (1978). Cooperation Under the Security Dilemma. The Johns Hopkins University.
10. Mazarr, M. (2015). Mastering the Gray Zone: Understanding a Changing Era ofConflictConflict. US Army War College.
11. Mazarr, M. (2018). Understanding Deterrence. RAND.
12. Murphy, D. (2025). The geopolitics of compute in the aftermath of the AI diffusion framework. Journal of Cyber Policy, 10 (2).
13. Nye, J. (2017). Deterrence and Dissuasion in Cyberspace.. International Security.
14. Sastry, G. & at al, 2024. Computing Power and the Governance of Artificial Intelligence. arXiv.
15. Snyder, G. (1961). Deterrence and Defense: Toward a Theory of National Security.
16. Strange, S. (1988). States and Markets. Pinter Publishers.
17. Waltz, K. (1979). Theory of International Politics. Addison-Wesley Publishing Company.

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**, Faculty of Artillery, Air Defense and Communication and Information Systems

INSTITUTIONAL, LEGAL, AND SOFTWARE DIMENSIONS OF DEFENSE CONTROL: FROM HARDWARE GEOPOLITICS TO ALGORITHMIC SOVEREIGNTY

Dilyan Markov

Rakovski National Defence College, Sofia,, Bulgaria, dlnmarkov@gmail.com

Abstract: *This report analyzes the shift from individual technological sovereignty to collective models of algorithmic security in defense. It examines the limits of national autonomy, the role of open-source architectures (RISC-V), and the formation of closed allied blocks (AUKUS, NATO DIANA). The main conclusion is that modern control relies on a dual mechanism: operational-software integration within alliances and regulatory filtering for external actors.*

Keywords: *software sovereignty, algorithmic coalitions, digital isolation.*

ИНСТИТУЦИОНАЛНИ, ПРАВНИ И СОФТУЕРНИ ИЗМЕРЕНИЯ НА СТРАТЕГИЧЕСКАТА АВТОНОМИЯ В ОТБРАНАТА: ОТ ГЕОПОЛИТИКА НА ХАРДУЕРА КЪМ АЛГОРИТМИЧЕН СУВЕРЕНИЗЪМ

Дилян Марков

Военна академия „Г. С. Раковски“, София, България, dlnmarkov@gmail.com

Резюме:

Ключови думи: *софтуерен суверенизъм, алгоритмични коалиции, дигитална изолация.*

Въведение

В съвременната динамика на международните отношения и военната стратегия технологичната сфера престана да бъде просто поддържащ фактор за икономически растеж или военен капацитет. Тя се утвърди като първична арена на геополитическо съперничество. Трансформацията на изчислителните системи, автономните алгоритми, изкуствения интелект и микроелектрониката в стратегически ресурси фундаментално преформатира концепциите за държавен суверенитет и национална сигурност. В условията на засилваща се фрагментация на глобалния ред традиционното разбиране за суверенитет, базирано върху териториална цялост и физически контрол над въоръжението, се сблъсква с нови дигитално генерирани уязвимости.

Настоящият доклад анализира парадигмалния преход от стремежа към индивидуален софтуерен и хардуерен суверенизъм към изграждането на нови, колективни модели на алгоритмична сигурност. В първата част се изследват систематичните опити на държавни субекти за скъсване с външната технологична зависимост чрез преодоляване на критични точки на блокиране (EDA инструменти), внедряването на архитектури с отворен код (RISC-V, OpenROAD) и

суверенни операционни среди. Специален фокус е поставен върху физическите, логическите и ресурсните ограничения, които правят абсолютната технологична автономия трудно постижима цел.

Във втората част докладът проследява появата на затворени съюзнически алгоритмични блокове (AUKUS Pillar II, NATO DIANA) и ролята на международните регулаторни инициативи за отговорен изкуствен интелект (REAIM, резолюции на ООН) като механизми за геополитическо и нормативно филтриране.

1. Стратегии за защита, софтуерен суверенизъм и техните физически и кибернетични ограничения

Държавните и военните субекти, които се стремят към пълна стратегическа автономия, предприемат систематични мерки за преодоляване на чуждестранната технологична зависимост. Според анализа на Дъглас Фулър относно софтуерната инфраструктура и геополитическите ограничения, инструментите за автоматизация на електронното проектиране (Electronic Design Automation – EDA) функционират като критична точка на блокиране (chokepoint), чрез която се упражнява екстратериториална юрисдикция и се парализира възможността за самостоятелно разработване на хардуер [7].

Високият праг за навлизане в този отрасъл се дължи на необходимостта от десетилетия научноизследователска дейност, сложни физико-математически алгоритми и тясна интеграция с производствените процеси. Поради тази специфична бариера, създаването на автономни EDA инструменти изисква огромни финансови и времеви ресурси, което прави държавите, обект на санкции, изключително уязвими при прекъсване на лицензионния достъп.

Според съвременните изследвания в областта на международната сигурност, притежанието на физически оръжия и хардуер без пълен контрол върху управляващия ги програмен код, създава критична уязвимост от дистанционно блокиране от страна на производителя [5]. Заплахата от подобна зависимост принуждава държавите да изграждат автономни и затворени технологични екосистеми. Тази реакция обаче разрушава досегашния глобален модел на свързаност и води до разпокъсване на дигиталното пространство на изолирани среди.

За да неутрализират този риск, страните насочват значителни ресурси към разработването на алтернативи с отворен код (Open-Source), които не подлежат на чуждестранни лицензионни режими и експортни ограничения. Основна цел на тези усилия е именно премахването на монопола при специализирания софтуер, управляващ моделирането, симулирането и верификацията на микрочипове.

Водещ пример в това направление е проектът OpenROAD (част от програмата DARPA IDEA), чиято цел е да премахне бариерите на разходите, експертизата и непредсказуемостта, които понастоящем блокират достъпа на създателите на системи до хардуерна имплементация в напреднали технологии. OpenROAD се стреми да разработи напълно автономна верига от инструменти с отворен код за да премине през целия процес от първоначалния програмен код на чипа до крайния

проект, който не съдържа външни патентовани модули и чужда интелектуална собственост [1].

Успоредно с това, Крис Милър посочва, че конвенционалните процесорни архитектури са силно уязвими към екстратериториален и санкционен натиск от страна на притежаващите патентите [10]. За да се неутрализира тази зависимост, в отбранителните производства се преминава към отворената процесорна архитектура RISC-V (Instruction Set Architecture). Функционирайки като универсален и напълно достъпен стандарт, тя осигурява възможност за проектиране на суверенни микропроцесори за критични и космически приложения без патентни такси и без риск от външно въздействие.

Ярък пример за стремежа към правно неутрализиране на технологичния натиск е преместването на юридическото седалище на фондацията RISC-V International от САЩ в Швейцария през 2019 г., предприето именно с цел предпазване на отворената архитектура от екстратериториалните ограничения за износ [13].

За гарантиране на оперативната сигурност във военните мрежи се разработват суверенни операционни системи, базирани на математически верифицирани микроядра с висока степен на защита. Тези среди функционират в пълна изолация в рамките на затворени мрежи без физическа или цифрова връзка с глобалния интернет. Основната цел е пълното неутрализиране на т.нар. „Ефект на Паноптикума" - рисковете, свързани със скрито телеметрично наблюдение, заложени системни вратички (backdoors) и възможности за дистанционно изключване на критични оръжейни системи [6].

Въпреки значителните предимства на отворените архитектури (RISC-V и OpenROAD), по-задълбоченият анализ разкрива, че концепцията за „пълен софтуерен суверенизъм" се сблъсква с три фундаментални уязвимости:

– Физически литографски монопол: Дори софтуерният дизайн и логическата архитектура на един процесор да са 100% суверенни и с отворен код, физическото превръщане на този проект в чип изисква изключително сложни системи. Тъй като глобалният производствен капацитет за авангардни чипове е концентриран в ограничен брой производства, геополитическият натиск върху хардуерните вериги за доставка остава критичен ограничаващ фактор. Софтуерният суверенизъм намалява юридическия и лицензионния риск, но не може да премахне физическата зависимост от литографското производство.

– Уязвимости на веригата за доставки в средите с отворен код: Широкото навлизане на софтуер с отворен код в отбранителната сфера създава специфични рискове за сигурността. Проектите разчитат на глобални общности от разработчици, което отваря възможности за внедряване на злонамерен код, системни грешки или „скрити вратички" в публичните хранилища. Поради това суверенитетът изисква непрекъснат математически одит на програмния код и защита на ядрата.

– Асиметрия в ресурсите и научния капацитет: Поддържането на изцяло автономна софтуерно-хардуерна екосистема налага непрекъснати мащабни инвестиции в научната и развойната дейност. Самостоятелното преодоляване на

технологичното изоставане в областта на алгоритмите, микропроцесорните архитектури и математическата верификация излиза от финансовите и кадрови възможности на една отделно взета държава, освен ако тя не притежава огромен ресурс.

Именно тези фундаментални ограничения показват, че самостоятелният технологичен суверенизъм в рамките на отделната държава е трудна за реализиране цел. Освобождаването от зависимостите на единичния монополист не може да се постигне чрез пълна самоизолация, а налага преход към нов модел на колективна алгоритмична сигурност. Осъзнаването на физическите и кибер ограничения на индивидуалния софтуерен суверенизъм тласка геополитическите субекти към формирането на затворени съюзнически алгоритмични блокове, подкрепени от обща правна рамка, споделени стандарти за сигурност и регулаторно проверяване на технологичния трансфер.

2. Оформяне на затворени съюзнически алгоритмични блокове, правна рамка и регулаторно филтриране

Паралелно с желанията на отделните държави за изграждане на самостоятелен софтуерен суверенизъм, в съвременната архитектура на сигурността се наблюдава дълбока структурна трансформация на военно-политическите съюзи. Анализът на съвременните процеси показва, че класическият модел на военен алианс, традиционно изграден върху географска близост и физическа съвместимост на въоръжението, претърпява парадигмален завой към формирането на т.нар. „алгоритмични коалиции" [17]. Те могат да включват конфигурации от няколко страни от един военно-политически блок, развитие за всички участници в досега действаща структура или сформиране по съвсем различен принцип.

Изследвайки новите съюзнически формати, като Втория стълб на Тристранното партньорство в областта на сигурността (AUKUS) [4] и Ускорителя на иновациите в отбраната на НАТО (NATO Defence Innovation Accelerator for the North Atlantic - DIANA) [12], става ясно, че тези структури не функционират просто като форуми за обмен на знания, а изграждат затворени и строго контролирани дигитални екосистеми. Споделянето на криптиран алгоритмичен код, невронни модели и масиви от разузнавателни данни очертава нов тип периметър на сигурност. В тази различна реалност достъпът до съюзнически действия и коалиционно планиране вече не се определя единствено от географското разположение или дипломатическите договори на една страна, а от нейната способност да се интегрира технологично в общия алгоритмичен контур.

Преходът от физическа към софтуерна интеграция се потвърждава от емпиричните данни, публикувани в официалните доклади [2, 3, 21] от съвместните изпитания в рамките на AUKUS Pillar II. Анализът на полевите изпитания, очертава:

– Оперативна софтуерна взаимозаменяемост: Постига се съвместимост на ниво алгоритми, позволяваща на сензори от една държава (напр. британски разузнавателен БЛА) да захранват с данни в реално време системите за командване

и управление и ударните средства на друга държава (напр. австралийски или американски платформи) през общи карти и оперативни софтуерни архитектури.

– Мигновен трансфер и адаптация на аналитичен капацитет: Военните платформи могат динамично да зареждат, преобучават и изпълняват невронни модели, разработени от съюзнически държави, запазвайки функционалност и координация дори при интензивно радиоелектронно противодействие и спътникови смущения.

Интегрирането на автономни технологии и алгоритмични системи за поддръжка на решения преформатира процесите по планиране на бойните действия в реално време. Използването на изкуствен интелект свива радикално тактическия цикъл за реакция, като същевременно еродира традиционните практически и когнитивни ограничения при прилагането на международноправните принципи за необходимост и пропорционалност. В резултат на тази технологична асиметрия възниква нов механизъм за системно изключване в международните отношения. Държавите и субектите извън тези затворени екосистеми биват ефективно изолирани от общите съюзнически платформи за командване и управление. Липсата на цифрова съвместимост ги прави оперативно „невидими" за провеждане на съвместни високотехнологични операции.

Следва да се отбележи обаче, че изграждането на съюзнически алгоритмични блокове създава риск от вътрешна асиметрия. Поради концентрацията на хипермащабни облачни инфраструктури и изчислителен ресурс в САЩ, по-малките съюзници са изправени пред опасността да заменят традиционната си хардуерна зависимост с нова, алгоритмична в рамките на самия алианс.

Въпреки че изграждането на затворени съюзнически алгоритмични блокове се представя като механизъм за споделена сигурност, задълбоченият анализ очертава сериозен риск от вътрешноблокова асиметрия. Докато в класическите военни съюзи оперативната съвместимост се изразява в уеднаквяване на калибри, радиочестоти, логистични стандарти и др., при софтуерно дефинираната отбрана съвместимостта навлиза в когнитивния контур на вземане на решения. Тази трансформация поражда нов феномен - преход от външна хардуерна зависимост към вътрешноблокова алгоритмична зависимост (алгоритмичен васалитет). В основата на тази асиметрия лежат няколко ключови фактора:

– Концентрация на изчислителен ресурс и инфраструктура: Разработването, обучението и непрекъснатото преобучение на сложни невронни модели изискват хипермащабни облачни среди (Hyper-scale Cloud Infrastructures) и гигантски масиви от данни. Тъй като над 80% от световния капацитет за облачни изчисления и специализиран софтуер за изкуствен интелект се контролират от субекти под американска юрисдикция, по-малките държави от алиансите (включително европейските членки на НАТО) се превръщат в ползватели на „готов" софтуерен продукт, без реално да притежават архитектурния код или изчислителната база за неговия независим одит.

– Загуба на национален софтуерен суверенитет над системите за командване и управление: Когато военните платформи на една държава бъдат интегрирани в обща алгоритмична мрежа, оперативната самостоятелност на национално ниво бива частично ограничена. Ако алгоритмите за приоритетизиране на целите, оценка на заплахите и оптимизация на сензорите са разработени от водещия партньор, по-малките съюзници са принудени да приемат „черната кутия" на чуждия модел за вземане на решения. Това създава риск от стратегическа парализа, ако достъпът до невронните мрежи или техните актуализации бъде ограничен или условно прекъснат.

– Екстратериториален контрол над програмния код: Дори в рамките на затворени коалиции, достъпът до суровите данни и базовите модели остава строго фрагментиран. Търговските тайни на водещите технологични компании и правилата за експортен контрол предотвратяват пълния трансфер на технологии към по-малките партньори.

В резултат на тези динамики съществува реална опасност концепцията за „колективна алгоритмична сигурност" да се превърне в параван за нов вид технологично подчинение. В него по-малките държави си осигуряват физически платформи и оперативни данни, но остават критично зависими от алгоритмичното „ядро" на водещата геополитическа сила. Преодоляването на тази асиметрия изисква не само техническа съвместимост, но и разработването на механизми за съвместна собственост върху моделите, отворени съюзнически стандарти за невронни мрежи и гаранции срещу едностранно изключване от общия софтуерен контур.

В допълнение, аналитичният преглед на изследванията, относно дипломатическите инициативи за „Отговорен изкуствен интелект във военната сфера" [8, 15] показва, че нормативната рамка се превръща в пряко продължение на технологичната надпревара. Международните формати, включително приетият План за действие от Сеул (Seoul Blueprint for Action) [14] и съответните резолюции на Общото събрание на ООН (Резолюция 79/239) [20], изпълняват стратегически функции.

Пряк доказателствен пример за тази трансформационна динамика е Резолюцията на Общото събрание на ООН, относно смъртоносните автономни оръжейни системи. Документът формулира за първи път необходимостта от институционален анализ на хуманитарните, правните и оперативните рискове, свързани с алгоритмичната автономия при воденето на война. Той превръща спазването на Международното хуманитарно право (МХП) в неоспорим глобален ориентир.

Паралелно с това, срещата за „Отговорен изкуствен интелект във военната сфера" (REAIM 2024 в Сеул) и приетият Seoul Blueprint for Action демонстрират прехода от абстрактни етични декларации към институционализиране на нормативни рамки. Анализът на този процес очертава три ключови вектора на въздействие върху международната сигурност:

– Нормативно-етично рамкиране и задължение за човешки контрол: Seoul Blueprint for Action и резолюциите на ООН утвърждават принципа, че крайният контрол и носенето на правна отговорност за вземането на решения относно използването на смъртоносна сила не могат да бъдат делегирани на системи с изкуствен интелект. Провеждането на стриктни правни прегледи става задължителен филтър още в етапа на проектиране, разработка и внедряване на алгоритмични бойни среди.

– Дипломатическо фрагментиране и нормативно филтриране: Независимо от подкрепата за Seoul Blueprint for Action от над 60 държави, ключови глобални страни като Китай и държави от Глобалния юг демонстрират резервираност спрямо правнообвързващите механизми или подкрепят съвсем различен вектор на регулация. Това показва, че нормативните формати REAIM не са просто универсален форум за разоръжаване, а функционален регулаторен инструмент. Чрез тях се утвърждава висок праг за отговорност, който изолира и подлага дипломатически натиск върху държавите, развиващи „нерегулирани" или етично непроверени автономни системи.

– Легитимация на технологичния напредък: За затворените алгоритмични алианси спазването на рамката служи като дипломатически щит. Тъй като техните системи се разработват в съответствие със стандарти за прозрачност, проследимост и намаляване на когнитивното отклонение, те придобиват международна легитимност. От друга страна, всяка държава, внедряваща автономни оръжия без спазване на тези високи стандарти, бива автоматично класифицирана като субект, застрашаващ стратегическата стабилност и подложена на технологични санкции и изолация.

В крайна сметка анализираните международни формати и резолюции потвърждават, че в съвременната епоха контролът се упражнява чрез двукомпонентен модел:

– Технологично-оперативна консолидация: Осъществява се чрез формирането на затворени съюзнически алгоритмични блокове, базирани на пълна софтуерна съвместимост и мигновен трансфер на аналитичен капацитет.

– Нормативно-правно филтриране: Прилага се чрез институционализиране на международни етични и правни стандарти, които очертават границата на легитимната военна автономия и служат като правен лост за системно изключване и изолация на външните субекти.

Паралелно с изграждането на евроатлантическите дигитални среди, незападните геополитически центрове оформят собствени среди за нормативно и технологично противопоставяне. Под натиска на западните технологични санкции Русия все повече разчита на технологично сътрудничество с Китай и рамките на БРИКС и Шанхайска организация за сътрудничество, като важен фактор за бъдещите си способности. Докато Китай използва развитата си технологична екосистема за изграждане на алтернативни рамки и засилване на глобалното си влияние, сътрудничеството му с Москва в дигиталната сфера запазва предимно опортюнистичен характер [9].

В сферата на международното право и регулациите за отговорен изкуствен интелект се наблюдава ясна стратегия на избягване и нормативно филтриране спрямо западните инициативи:

– Дипломатическо дистанциране от западните формати: Приемането на етични рамки и декларации на Seoul Blueprint for Action се среща с открит скептицизъм от страна на Пекин [19]. Отказът на Китай да подпише незадължаващите споразумения на форума REAIM в Сеул (включително ограниченията относно контрола над ядрените арсенали) демонстрира нежеланието на източните сили да подчинят технологичното си развитие на рамки, определяни от САЩ и техните съюзници. Същевременно пълното изключване на Русия от форума поради войната в Украйна допълнително фрагментира глобалния диалог по сигурността на ИИ.

– Противопоставяне на концепцията за екстратериториална сигурност: Китайската дипломация аргументира, че разширяването на концепцията за национална сигурност над микроелектрониката и алгоритмите представлява форма на геополитически монополизъм [18]. Като алтернатива Пекин насърчава стандарти, базирани на отворен код (Open-Source), с цел да привлече държавите от Глобалния юг и да разруши западната хегемония над глобалните регулаторни органи.

– Билатерални консултации и координация в ООН: Институционалното сътрудничество между Русия и Китай се разгръща чрез специализирани двустранни консултации относно военната употреба на ИИ и координация в Групата на правителствените експерти към ООН по отношение на смъртоносните автономни оръжейни системи [11].

Тази динамика потвърждава, че глобалната среда не се движи към единен, унифициран правен режим за управление на военния изкуствен интелект. Напротив, формира се двуполюсна или мултиполярна алгоритмична архитектура, в която източната ос изгражда независими софтуерни и хардуерни вериги за доставка, отхвърляйки западния етично-правен филтър като опит за институционално възпиране.

Заключение

Направеният в доклада анализ води до извода, че в ерата на изкуствения интелект и високотехнологичната асиметрия концепцията за самодостатъчен и напълно изолиран държавен технологичен суверенитет е системно ограничена. Въпреки, че усилията за преодоляване на софтуерните монополи чрез решения с отворен код и верифицирани микроядра намаляват юридическите и лицензионните рискове, те не могат да премахнат физическия монопол над литографското производство, рисковете във веригите за доставки и огромната асиметрия в развойния капацитет.

Тези критични уязвимости тласкат глобалната архитектура на сигурността към нова структуриращa парадигма. Освобождаването от единични монополисти вече не се търси чрез национална самоизолация, а чрез преход към колективна

алгоритмична консолидация. Военно-политическите съюзи претърпяват дълбока трансформационна еволюция, от традиционни географски и хардуерни блокове те се превръщат в затворени алгоритмични екосистеми, в които се постига пълна софтуерна съвместимост, споделяне на невронни модели и мигновен трансфер на аналитичен капацитет.

В тази нова реалност контролът в международната система се упражнява чрез оперативно-технологично приобщаване за държавите, способни да се интегрират в затворените съюзнически дигитални контури и нормативно-правно филтриране за външните участници, при което етичните и международноправните стандарти за отговорен ИИ служат, като ефективен инструмент за изолация, правен натиск и дипломатическо санкциониране.

В крайна сметка бъдещето на националната сигурност вече не се решава единствено от количеството физическо въоръжение, а от способността на една държава да защити своята критична дигитална инфраструктура и едновременно с това да бъде интегрална част от високотехнологичните алгоритмични алианси, които очертават новите цифрови граници на глобалния свят.

Литература

1. Ajayi T., et al. (2019). Invited: Toward an Open-Source Digital Flow: First Learnings, Las Vegas: DAC '19. Available from: https://par.nsf.gov/servlets/purl/10171025 [viewed 2026-08-08].
2. Australian government (2024) „AUKUS trials artificial intelligence in robotic vehicles", Australian government.
3. Defence Science and Technology Laboratory (Dstl) (2024). „AUKUS trial advances AI and autonomy collaboration," Defence Science and Technology Laboratory (Dstl).
4. DiFiore N. (2025). „AUKUS and Allied AI: Building Trilateral Defense Capabilities Across the AI Stack," FAO Journal of International Affairs, Available from: https://faoajournal.substack.com/p/aukus-and-allied-ai-building-trilateral [viewed 2026-08-18].
5. Drezner D., H. Farrell и A. Newman. (2021), The Uses and Abuses of Weaponized Interdependence, Brookings Institution Press.
6. Farrell H., A. Newman (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion, том 44, International Security. Available from: https://doi.org/10.1162/isec_a_00351 [viewed 2026-08-10].
7. Fuller D. (2020) Cutting Off Our Nose to Spite Our Face: US Policy towards Huawei and China in Key Semiconductor Industry Inputs, Capital Equipment and Electronic Design Automation Tools, The Johns Hopkins University.
8. Goussac N. (2025) „Responsible behaviour in military AI starts with responsible procurement," SIPRI. Available from: https://www.sipri.org/commentary/essay/2025/military-ai-responsible-procurement#:~:text=In%20a%20tense%20geopolitical%20environme

nt%20and%20amid,use%20of%20AI%20in%20the%20military%20domain. [viewed 2026-08-18].

9. Hanhijärvi, H. (2026). Artificial Intelligence and Foreign Information Manipulation: Chinese and Russian approaches, Hybrid CoE Paper 29, The European Centre of Excellence for Countering Hybrid Threats. Available from: https://www.hybridcoe.fi/publications/artificial-intelligence-and-foreign-information-manipulation-chinese-and-russian-approaches/ [viewed 2026-08-28].
10. Miller C. (2022). Chip War: The Fight for the World's Most Critical Technology, Scribner.
11. Ministry of foreign affairs of the Russian Federation (2024). On Russian-Chinese consultations regarding the use of AI technologies in the military domain, Press Release. Available from: https://mid.ru/en/foreign_policy/news/1929203/ [viewed 2026-08-28].
12. NATO DIANA. DIANA is the Defence Innovation Accelerator for the North Atlantic, an organisation established by NATO to find and accelerate innovation to provide defence and security effects for the Alliance. Available from: https://www.diana.nato.int/ [viewed 2026-08-18].
13. Nellis S., A. Alper, (2019). „U.S.-based chip-tech group moving to Switzerland over trade curb fears," Reuters. Available from: https://www.reuters.com/article/business/us-based-chip-tech-group-moving-to-switzerland-over-trade-curb-fears-idUSKBN1XZ165/ [viewed 2026-08-12].
14. Sanders L., et al. (2024) „REAIM Summit 2024: Slowly but Surely towards Better Governance of Military Artificial Intelligence? From The Hague to Seoul," ANZSIL Perspective. Available from: https://anzsilperspective.com/reaim-summit-2024-slowly-but-surely-towards-better-governance-of-military-artificial-intelligence-from-the-hague-to-seoul/ [viewed 2026-08-18].
15. Singapore AI Observatory (2024). „Responsible AI in the Military Domain (REAIM) Seoul Summit," Singapore AI Observatory.
16. Shakhanova G. (2026) Russia-China Cooperation amidst the war in Ukraine: From Joint Management of Security in Eurasia to AI Collaboration, EuroHub4Sino Publication. Available from: https://eh4s.eu/publication/russia-china-cooperation-amidst-the-war-in-ukraine-from-joint-management-of-security-in-eurasia-to-ai-collaboration [viewed 2026-08-28].
17. Soare S. (2023) „Software-defined Defence: Algorithms at War," International Institute for Strategic Studies. Available from: https://www.iiss.org/research-paper/2023/02/software-defined-defence/ [viewed 2026-08-04].
18. The organisation for world peace (OWP) (2026). WAICO And The U.S.-China Chip War, OWP Analysis. Available from: https://theowp.org/waico-and-the-u-s-china-chip-war/ [viewed 2026-08-28].

19. Times of India (2024). China refuses to sign agreement to ban AI from controlling nuclear weapons, Times of India / REAIM Summit Coverage. Available from: https://timesofindia.indiatimes.com/world/china/china-refuses-to-sign-agreement-to-ban-ai-from-controlling-nuclear-weapons/articleshow/113235217.cms [viewed 2026-08-28].
20. UN. General Assembly (79th sess. : 2024-2025), „Artificial intelligence in the military domain and its implications for international peace and security : resolution / adopted by the General Assembly," UN. General Assembly (79th sess. : 2024-2025).
21. U.S. Department of Defense (DoD) (2024). „AUKUS Pillar II Milestones Hint at Future Integrated Autonomous, Artificial Intelligence Operations," U.S. Department of War.

THE EFFECT OF VARIABLE FOCAL DISTANCE TO THE ASPEN SAMPLES SURFACE ON CO_2 LASER ENGRAVING PARAMETERS

Daivis Rāviņš, Imants Adijans, Dzintars Rāviņš,

Faculty of Engineering, RTU Rezekne Academy, Rezekne, Latvia
daivis.rav@gmail.com, imants.adijans@rtu.lv, dzintars.rav@gmail.com

***Abstract**: This study aims to investigate the influence of focal position relative to the material surface on the parameters of CO_2 laser engraving of aspen wood at different heat treatment temperatures. Six aspen samples were used in the experiment: one untreated sample and five thermally modified samples treated at temperatures of 180°C, 195°C, 205°C, 214°C, and 225°C. The study focused on the influence of focal position on engraving depth, line width, and visual quality. Additionally, tests were conducted on individual samples with variable laser power and variable scanning speed at a fixed focal position. The goal of the study was to determine the most suitable processing conditions for achieving consistent, high-quality engraving on aspen. The results obtained can be used to improve the efficiency and quality of CO_2 laser processing of wood materials.*

***Keywords:** Insert keyword text, Insert keyword text, Insert keyword text, Insert keyword text*

Introduction

Laser processing of wood materials has recently become widespread in industry, furniture production, decorative and artistic processing, product marking, and the production of functional surfaces. CO_2 laser systems are most widely used in wood processing, as their wavelength is effectively absorbed by organic materials containing cellulose, hemicellulose, and lignin. Due to the high energy localization, laser processing allows for the production of engraved structures with high precision, minimal mechanical impact, and the possibility of automated process control [1], [5], [7].

Unlike traditional mechanical processing methods, laser engraving provides contactless processing of the material, high repeatability of results, and the ability to form complex geometric structures. An additional advantage of laser processing is the ability to precisely control the energy distribution within the impact zone, which is especially important when shaping the surface microrelief and functional structures of wood [8], [9]. However, the quality of laser wood processing is determined by a large number of interconnected process parameters. Key parameters include laser power, scanning speed, pulse frequency, number of passes, focal position, and the physical and chemical properties of the material being processed [1], [2], [5], [7]. Changing any of these parameters directly impacts energy distribution in the processing zone, thermal processes, the degree of surface carbonization, roughness, and the geometric characteristics of the engraved line.

Previous studies have shown that the depth and width of laser engraving on wood depend significantly on laser power and scanning speed. Increasing power generally results in higher energy density and increased engraving depth, while increasing scanning

speed reduces thermal exposure time and material removal depth [1], [5], [13]. In the work of Kubovský et al. [7], it was shown that optimization of the parameters of CO_2 laser processing of wood materials allows for a significant improvement in cutting quality and processing stability. Similar results are presented in the studies of Nguyen-Thi-Ngoc and Dang [5], as well as Gusts and Adijāns [6], where methods for optimizing the parameters of laser engraving of wood based on statistical approaches and analysis of processing modes were considered.

Moreover, changes in processing parameters may be accompanied by the appearance of surface defects, such as excessive carbonization, thermal destruction of the wood structure, changes in surface color, and an increase in the heat-affected zone. In the work of Kúdela et al. [8], it was found that laser irradiation parameters have a significant impact on the surface morphology of oak wood, the depth of thermal impact, and changes in the physicochemical properties of the surface layer. Additionally, studies [9], [10] have shown that CO_2 laser treatment causes changes in surface roughness, carbonization intensity and chemical composition of wood, including changes in the content of carbon-containing components and changes in the color characteristics of the surface.

Particular attention in modern research is given to the influence of thermal modification of wood on the results of laser processing. Heat treatment causes changes in the chemical composition and microstructure of wood, including the degradation of hemicelluloses, changes in moisture content, a decrease in density, and an increase in the content of carbon components [3], [4]. These changes have a significant impact on the processes of laser radiation absorption, heat transfer, and material removal. For thermally modified aspen, it was previously established that increasing the heat treatment temperature can enhance the efficiency of laser irradiation and contribute to an increase in engraving depth [1]. A study by Doğan et al. [11] demonstrated that wood modification significantly affects the parameters of CO_2 laser structuring and alters the nature of the interaction of laser radiation with the surface of the wood material. However, the mechanisms of interaction between laser radiation and thermally modified wood have not yet been fully studied.

One of the most important, yet relatively little-studied, parameters of laser wood processing is the focal plane relative to the material surface. Changing the focal plane changes the laser spot diameter, power density distribution, and the nature of the thermal impact on the surface. When the focal plane coincides with the material surface, maximum energy concentration is achieved, ensuring the most intense material removal. When the laser beam is defocused, the energy density decreases and the spot diameter increases, which can lead to changes in line width, engraving depth, roughness, and visual quality of the surface [2], [12]. Jurek and Wagnerová [12] showed that precise laser beam calibration and focal position have a significant impact on the color change of the wood surface and the uniformity of laser processing.

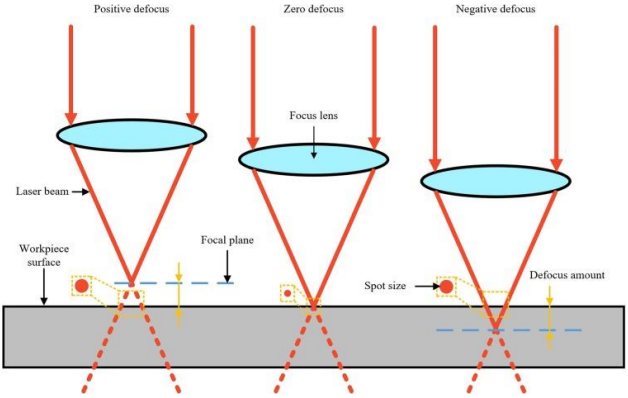


Fig. 1. Change in laser beam geometry depending on focal length. [17]

It should be noted that the influence of the focal position is particularly important when processing wood, as wood is an anisotropic and heterogeneous material with a pronounced dependence of its thermophysical properties on the fiber direction, moisture content, and degree of thermal modification. Even a small change in energy density can lead to significant changes in the nature of the thermal destruction of the material, the intensity of carbonization, and the geometry of the engraved structure. Furthermore, the energy distribution in the impact zone is determined not only by the focal position but also by the geometry of the laser beam, which is close to a Gaussian intensity distribution [12]. Despite this, most existing studies have focused primarily on the effects of power and processing speed, while the influence of focal position on the parameters of CO_2 laser engraving of thermally modified wood has been limitedly studied [14-18].

Aspen was chosen as the material for this study due to its relatively homogeneous structure, good processability, and widespread use in the woodworking industry. Furthermore, aspen lends itself well to thermal modification, allowing for the study of the influence of changes in wood structure on laser interaction processes [3], [4]. Heat treatment of aspen changes its color, density, thermal properties, and chemical composition, making this material a promising candidate for studying laser engraving. Of additional interest is the possibility of investigating the relationship between the degree of thermal modification of the wood, the distribution of laser energy density, and the nature of the engraved structure formation.

Purpose of this study

The purpose of this study is to comprehensively investigate the influence of focal position relative to the material surface on the parameters of CO_2 laser engraving of untreated and thermally modified aspen.

Research Objectives

To achieve this goal, the following objectives were formulated:

- To study the effect of focal position on the width of the engraved line when processing untreated and thermally modified aspen.
- To determine the effect of focal position on the depth of laser engraving of wood at different heat treatment temperatures.
- To conduct a comparative analysis of the behavior of untreated and thermally modified aspen during laser processing.
- To evaluate the effect of thermal modification of wood on the sensitivity of the engraving process to laser beam defocusing.
- To study the additional effects of variable laser power and variable scanning speed at a fixed focus position.
- To determine the most effective CO_2 laser engraving modes for achieving stable geometric parameters and high-quality surface finish.
- To analyze the physical mechanisms of changes in the geometry of the engraved line depending on the distribution of laser radiation energy density, the degree of thermal defocusing, and the degree of thermal defocusing.

Materials and methods

A. Material

The study utilized six aspen samples (Figs. 2, 3, 4): untreated aspen, as well as thermally modified samples treated at temperatures of 180°C, 195°C, 205°C, 214°C, and 225°C. Using samples with different heat treatment temperatures allowed us to evaluate how changes in wood structure affect the laser engraving results.

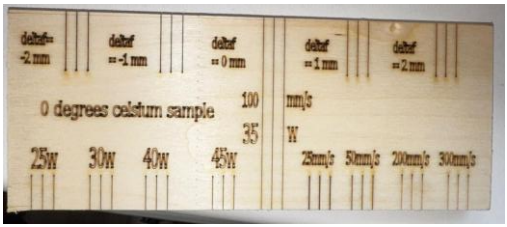


Fig. 2. Sample of untreated aspen



Fig. 3. Sample of thermally modified aspen at a temperature of 180 degrees Celsius.

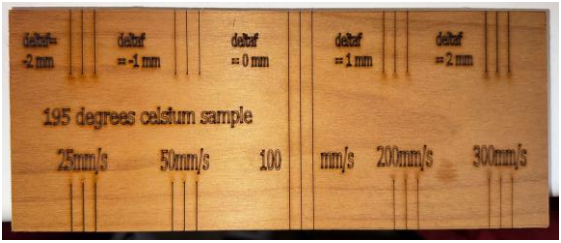


Fig. 4. Sample of thermally modified aspen at a temperature of 195 degrees Celsius.

B. Equipment

Engraving was performed on a CO_2 laser machine (SUNTOP ST-CC9060).



Fig. 5. CO_2 laser system SUNTOP ST-CC9060.

The technical specifications of the SUNTOP ST-CC 9060 laser system are presented in Table 1.

Table 1. Laser system SUNTOP ST-CC9060 technical specifications

Laser type	**CO_2 laser**
Operation mode	CW
Wavelength	10640 nm
Maximum output power	100 W
Workspace (Cutting area)	900 x 600 mm
Precision	0,02 mm
Scan speed	0 – 1000 mm/s
Laser Safety Class	4
Cooling system	Water cooling
Data formats used	dxf, plt, bmp, dst,ai
Total power	1500 W

A laser power of 35 W and a scanning speed of 100 mm/s were chosen as constant process parameters for the main experiment. These parameters were selected based on previously published studies on laser engraving of wood and wood-based materials, where these values are within the working range of processing parameters [5], [6].

For measuring depth (h) and width (b) OLYMPUS OLS5000 was used. (Fig.6.)



Fig. 6. OLYMPUS OLS5000

Mechnical parameters for OLYMPUS OLS5000 laser microscope:

- Max magnification 100x,
- Z measurement pitch: 2μm,
- X and Y axis resolution: +/-1.5% [6].

C. Methodology

The laser power density was calculated using this formula:

$$q_s = \frac{P}{S} \tag{1}$$

where q_s is the power density, W/cm²; P is the laser power, W; and S is the laser spot area, cm².

$$S = \pi \left(\frac{d}{2}\right)^2 \tag{2}$$

where *d* is the laser spot diameter, cm. Laser spot diameter was taken as d=150 μm, which corresponds to 0.015 cm. Therefore, the spot radius is 0.0075 cm, and the laser spot area is:

$$S = \pi \cdot (0.0075)^2 \approx 0.0001767 \text{ cm}^2$$

For a fixed focal position Δf=0, the laser power density q_s was calculated for modes with a power from 25 to 45 W. The obtained power density values are shown in Table 1. and were used to compare laser processing modes with variable power.

Table 2. Calculated laser power density values for variable power at a laser spot diameter of 150 μm.

P, W	25	30	35	40	45
q_s, W/cm²	141471,1	169765,3	198059,5	226353,7	254647,9
$q_s \times 10^5$, W/cm²	1,41	1,70	1,98	2,26	2,55

When the focus is shifted relative to the surface of the material being processed, the power density of the laser radiation changes, since defocusing leads to an increase in the diameter of the laser beam and the density is distributed.

$$q_s(\Delta f) = \frac{P}{S(\Delta f)} \tag{3}$$

where $q_s(\Delta f)$ is the power density at a given focal offset; P is the laser power, W; and S(Δf) is the laser spot area on the material surface at the corresponding focal position.

$$S(\Delta f) = \pi \left(\frac{d(\Delta f)}{2} \right)^2 \tag{4}$$

where $d(\Delta f)$ is the effective laser spot diameter at the given focal offset.

When defocusing, the beam geometry changes, which means the beam is unable to concentrate and this deteriorates the cutting quality.

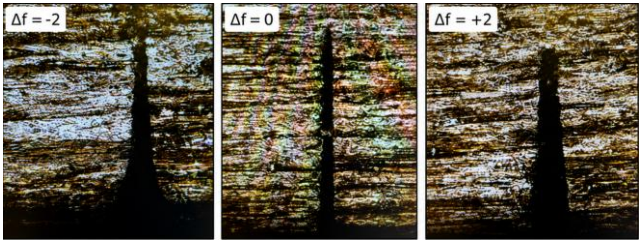


Fig. 7., 8., 9. The influence of focus position on cutting quality

C. Main experiment

The main experiment was aimed at investigating the effect of the focal position relative to the sample surface. Constant process parameters were used for all six samples: laser power of 35 W and a scanning speed of 100 mm/s. The focal position relative to the material surface was varied at five levels: Δf = -2 mm, -1 mm, 0 mm, +1 mm, and +2

mm. Three replicate lines were plotted for each focal position to obtain more accurate results using arrhythmic mean calculation.

D. Additional experiments

Additional experiments were performed on samples in parallel with the main experiment (Figs. 2, 3, 4) to evaluate the effect of variable laser power and variable scanning speed at a fixed focal position Δf = 0 mm. For samples at 0°C, 180°C, and 225°C, engraving was additionally performed with variable laser power. For samples at 195°C, 205°C, and 214°C, engraving was additionally performed with variable scanning speed. For the 0°C sample, both additional series were performed: with variable power and with variable speed.

E. Evaluation parameters

Engraved lines were assessed according to the following criteria: line width b [mm], engraving depth h [mm], and visual quality of the engraved line. Visual quality assessment included analysis of line clarity, edge condition, and the presence of potential thermal damage, such as excessive darkening or scorching.

Results and discussion

Figures 10.–15. show graphs of changes in the width and depth of engraved lines depending on the focal position, laser power, and scanning speed. The analysis was based on the average values of three repetitions for each mode.

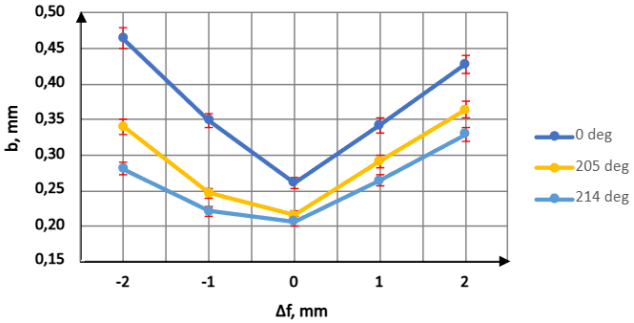


Fig. 10: Dependence of line width b on the focus position Δf for aspen samples with different heat treatment temperatures.

An analysis of the graphs shows that the line width dependence on the focal position is nearly parabolic. Minimum line width values are observed at Δf = 0 mm, which corresponds to the position of maximum laser energy concentration on the material surface. As the focal position shifts, both negatively and positively, the line width increases due to the increase in laser spot diameter.

Of particular interest is the slope of the graphs in different defocusing regions. In the range from Δf = 0 mm to ±1 mm, a relatively sharp increase in line width is observed, indicating the high sensitivity of the engraving process to small changes in focal position. This suggests that even a slight deviation from the focal plane leads to a rapid decrease in power density and redistribution of energy over a larger area.

With further increase in defocusing to ±2 mm, the slope of the curves becomes less pronounced. The decrease in the slope indicates a transition to a mode of partial spot diameter stabilization, where additional focus shifts no longer cause such an intense increase in linewidth. This behavior is characteristic of a Gaussian energy distribution of a CO_2 laser beam.

It's worth noting the difference in slopes for different heat treatment temperatures. For untreated aspen, as well as for samples treated at 180°C and 195°C, the slopes of the curves are steeper, indicating greater sensitivity of the material to changes in energy density. This is likely due to the greater heterogeneity of the wood structure, higher moisture content, and lower degree of carbonation.

For samples at 205°C, 214°C, and 225°C, the slope of the graphs becomes less pronounced, and the absolute widths are smaller. This may indicate changes in the thermophysical properties of wood after heat treatment: a decrease in thermal conductivity, a reduction in the content of volatile components, and an increase in the proportion of carbon structure. As a result, the laser energy is absorbed more locally, and the heat-affected zone is reduced.

The analysis of the slope of the graphs shows that heat treatment of wood affects not only the absolute parameters of engraving, but also the sensitivity of the process to changes in the position of the focus.

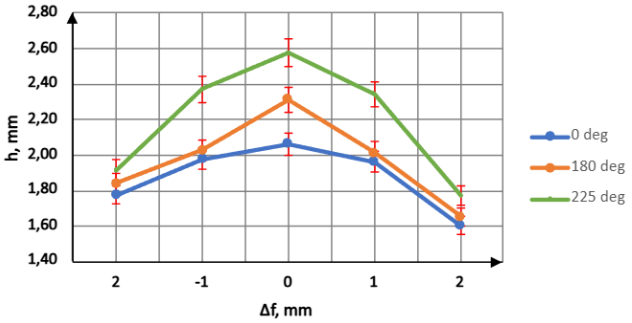


Fig. 11: Dependence of the engraving depth h on the position of the focus Δf for aspen samples with different heat treatment temperatures.

The engraving depth graphs show a distinct maximum at Δf = 0 mm, which corresponds to the maximum laser energy density on the material surface. As the focus deviates toward the negative or positive side, the depth decreases due to energy dissipation and an increase in the laser spot diameter.

An analysis of the curve slopes shows that the depth reduction is most intense in the range from Δf = 0 mm to ±1 mm. The steep negative slope indicates a strong dependence of the ablation process on the energy concentration in the treatment zone. Even slight defocusing leads to a noticeable reduction in the laser penetration depth.

In the range from ±1 mm to ±2 mm, the depth change becomes less abrupt, and the slope of the graphs decreases. This indicates a gradual transition to a mode of reduced material removal efficiency, where further reductions in power density no longer have such a significant impact on engraving depth.

For samples heat-treated at 205°C, 214°C, and 225°C, higher gradients of depth change near the focal point are observed. This may be due to the increased brittleness and altered microstructure of thermally modified wood, resulting in more intense material removal at high energy densities but a faster loss of ablation efficiency during defocusing.

The 195°C sample exhibits a less symmetrical relationship and a more complex pattern of depth change. It's likely that at this heat treatment temperature, transient changes occur in the wood structure associated with the partial decomposition of hemicelluloses and changes in the material's porosity. This may lead to instability in laser energy absorption and inhomogeneity in the material removal process.

From a physical perspective, the slope of the depth graphs reflects the change in local laser power density. The steeper the slope, the more sensitive the process is to defocusing. Therefore, to ensure a stable engraving depth, maintaining the focal position as precisely as possible is essential, especially when processing thermally modified wood.

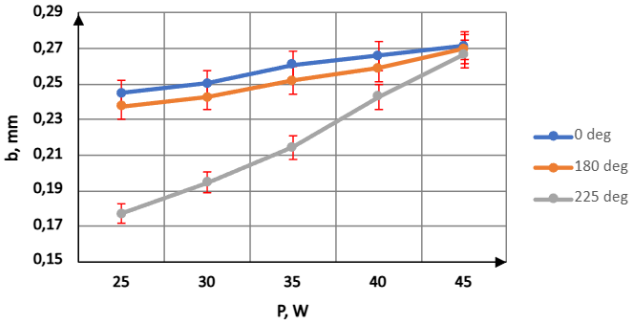


Fig. 12: Dependence of line width b on laser radiation power P at Δf = 0 mm.

The results presented in Fig. 12. demonstrate a consistent trend of increasing line width with increasing laser power for all samples studied. This relationship is due to the increased energy density and the expansion of the thermally affected zone on the wood surface. As power increases, the temperature in the treatment zone increases, intensifying pyrolysis, carbonization, and thermal destruction of the surface layer, leading to an increase in the width of the engraved line.

An analysis of the graph slopes shows that in the initial power range, the increase in line width is relatively gradual. However, as higher power values are reached, the slope of the curves increases, especially for samples with higher thermal modification temperatures. This indicates the nonlinear nature of the process and the increased sensitivity of wood to laser irradiation with increasing energy density.

For untreated aspen and the 180°C sample, the slope of the graphs is more moderate, indicating a relatively stable change in line width with increasing power. It is likely that in these materials, some of the energy is expended on moisture evaporation and thermal decomposition of less modified wood components, partially limiting the expansion of the treated zone.

The most pronounced slope of the curve is observed for the 225°C sample. The more intense increase in line width may be due to changes in the chemical composition of the wood after deep thermal modification. At high heat treatment temperatures, the hemicellulose and moisture content decreases, and the wood structure becomes more brittle and carbon-containing [3], [11]. As a result, local absorption of laser radiation increases and thermal destruction of the material intensifies, leading to a more rapid expansion of the engraving zone with increasing power.

It should be noted that the linewidth/power relationship is not strictly linear. In some areas of the graph, slight deviations from monotonic growth are observed, which may be due to the natural heterogeneity of wood, differences in the density of annual rings, and local variations in the material's thermophysical properties. Furthermore, the Gaussian distribution of laser beam intensity may have an additional effect, with increasing power leading not only to an increase in the maximum energy density but also to an expansion of the effective heat-affected zone.

Thus, analysis of the graph slopes shows that increasing laser power leads to accelerated line width growth, especially for thermally modified samples with high processing temperatures. This highlights the need for precise power selection when performing high-precision laser engraving of wood.

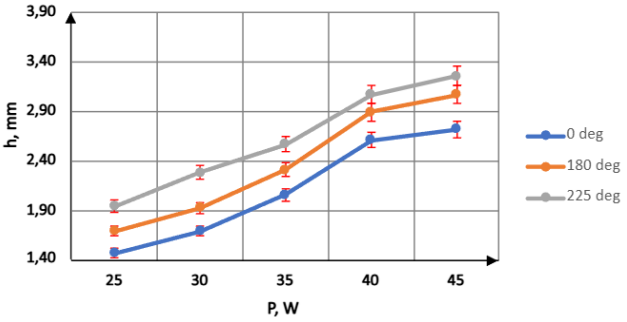


Fig. 13: Dependence of the engraving depth h on the laser radiation power P at Δf = 0 mm.

The graphs in Fig. 13. show that the engraving depth increases with increasing laser power for all samples studied. This result is predictable, as increasing power leads to an increase in the amount of energy transferred to the material and an intensification of the ablation and thermal removal processes of wood [1], [5].

An analysis of the graph slopes shows that the increase in depth is particularly intense in the low-power region. The steep, positive slope at the beginning of the curves indicates the high sensitivity of the engraving process to changes in laser power. In this range, even a small increase in power leads to a significant increase in energy density in the processing zone and accelerated material removal.

With further increases in power, the slope of the graphs gradually decreases, and the increase in depth becomes less steep. This behavior may indicate partial saturation of the material removal process. At high powers, some of the energy begins to be expended not only on ablation but also on secondary processes—heating of surrounding areas, carbonization, reabsorption of radiation by pyrolysis products, and the formation of a heat-affected zone.

The most pronounced increase in depth is observed for the 180°C and 225°C samples. For the 225°C sample in particular, the slope of the graph remains relatively high even with increasing power, indicating increased susceptibility of thermally modified wood to laser irradiation. Thermal modification likely leads to a decrease in thermal conductivity and a change in the structure of the wood, resulting in the energy being concentrated in a smaller volume of the material and facilitating deeper penetration of the laser irradiation [3], [4], [11].

For untreated aspen, the increase in depth is also clearly visible, but the slope of the graph is somewhat less pronounced. This may be due to the higher moisture content and less altered wood structure, which increases heat loss and reduces the efficiency of localized material removal.

It should also be noted that increasing the engraving depth is accompanied by increased thermal processes in the processing zone. At high power, a more pronounced carbonization zone may form and surface roughness may increase, as confirmed by research results [8]–[10].

Analysis of the slope of the graphs shows that the laser power is one of the most critical parameters determining the efficiency of material removal and the depth of wood engraving.

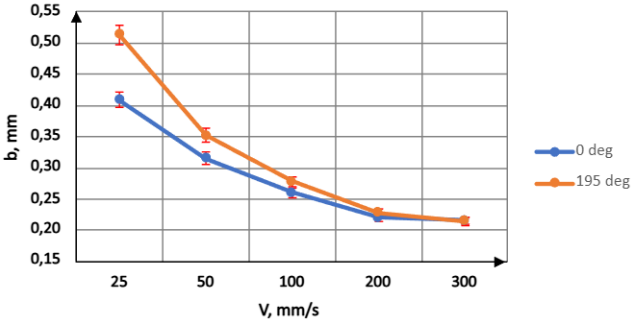


Fig. 14: Dependence of line width b on scanning speed v at $\Delta f = 0$ mm.

The graphs in Fig. 14. demonstrate a consistent decrease in line width with increasing scanning speed for all samples studied. This effect is explained by a decrease in the interaction time of the laser beam with the material as the laser head speed increases. This reduces the amount of energy transferred per unit line length, which reduces the size of the heat-affected zone.

An analysis of the graph slopes shows that the sharpest decrease in line width is observed in the low-speed range—from 25 to 100 mm/s. The steep negative slope in this region indicates the process's high sensitivity to changes in scanning speed. Even a relatively small increase in speed results in a noticeable reduction in thermal exposure time and a decrease in the engraved line width.

As the speed increases further to 200–300 mm/s, the slope of the graphs decreases, and the dependence becomes flatter. This indicates a gradual decrease in the influence of speed on line width. At high speeds, the amount of energy transferred to the material becomes so small that further increases in speed no longer cause significant changes in line geometry.

For thermally modified samples, especially at 225°C, the line width reduction is somewhat less uniform. This may be due to changes in heat transfer and energy absorption mechanisms after heat treatment. Thermally modified wood has an altered microstructure and an increased susceptibility to localized carbonization, which may lead to a more complex formation of the treated zone.

The influence of the Gaussian distribution of laser beam intensity should also be considered. At high processing speeds, material interaction occurs predominantly with the central, most energy-dense portion of the beam, while peripheral zones have a significantly lesser influence on line width formation.

Analysis of the slope of the graphs shows that the scanning speed has a particularly strong influence on the line width in the low speed region, while at high speeds the sensitivity of the process gradually decreases.

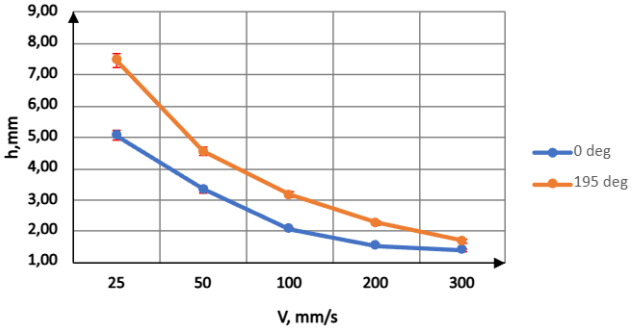


Fig. 15:. Dependence of the engraving depth h on the scanning speed v at $\Delta f = 0$ mm.

As can be seen in Fig. 15., the engraving depth decreases significantly with increasing scanning speed for all the samples studied. This dependence is due to a decrease in laser exposure time per unit line length and a corresponding decrease in the input energy density [5], [6].

An analysis of the graph slopes shows that the sharpest decrease in depth is observed when moving from a minimum speed of 25 mm/s to 50 and 100 mm/s. The steep negative slope indicates the high sensitivity of the ablation process to changes in thermal exposure time. In this range, even a small increase in speed leads to a significant decrease in material removal depth.

At speeds of 200 and 300 mm/s, the slope of the graphs becomes less pronounced, and the reduction in depth occurs more gradually. This is because at high speeds, the amount of energy entering the material is already relatively low, so further increases in speed have a limited effect on the material removal process.

For thermally modified samples, the reduction in depth is particularly pronounced at low speeds. This may be due to the fact that, under prolonged thermal exposure, thermally modified wood absorbs laser energy more intensely and undergoes thermal degradation more rapidly. However, as the speed increases, this effect significantly weakens due to the shorter interaction time.

Furthermore, analysis of the graphs' shapes reveals that the relationship between depth and velocity is nonlinear. This is explained by the complex interaction of heat transfer, evaporation of wood components, carbonization, and material removal. At low velocities, the process is determined primarily by heat accumulation, whereas at high velocities, the lack of energy for effective material ablation becomes dominant.

From a physical perspective, the slope of the graphs reflects the change in the specific energy transferred to the wood per unit line length. The higher the scanning speed, the less energy is transferred to the material and the shallower the engraving depth. Therefore, scanning speed is one of the key parameters for controlling the depth of laser wood processing.

Summary of Results

The conducted study demonstrated that the focal position, laser power, and scanning speed significantly affect the geometrical parameters of CO_2 laser engraving on untreated and thermally modified aspen wood. The obtained results confirmed that all investigated technological parameters are strongly interconnected and jointly determine the quality and efficiency of the engraving process.

The analysis of the influence of focal position showed that both the line width and engraving depth are highly sensitive to defocusing. For all investigated samples, the minimum line width and maximum engraving depth were achieved at the focal position $\Delta f = 0$ mm, where the laser energy density on the material surface is maximal. As the focal position shifted in either the negative or positive direction, the line width increased while the engraving depth decreased due to the enlargement of the laser spot diameter and redistribution of energy over a larger area.

The slope analysis of the focus-dependent graphs revealed that the highest sensitivity of the process occurs in the region close to the focal plane ($\Delta f = 0$ to ± 1 mm). In this range, even small focal deviations caused rapid changes in both engraving width and depth. At larger defocusing distances (± 2 mm), the slopes of the curves became less pronounced, indicating partial stabilization of the laser spot diameter and reduced sensitivity of the process to further focus displacement. The observed behavior corresponds well to the Gaussian energy distribution typical for CO_2 laser beams.

Thermally modified wood samples exhibited different responses to laser processing compared to untreated aspen. Samples treated at 205°C, 214°C, and 225°C generally showed smaller line widths and higher sensitivity of engraving depth to focal changes. These effects are likely associated with thermally induced changes in the wood structure, including reduced moisture content, lower thermal conductivity, degradation of hemicelluloses, and increased carbonization. Such modifications alter the mechanisms of laser energy absorption and heat transfer within the material.

The influence of laser power demonstrated a clear increase in both line width and engraving depth with increasing power levels. The slope analysis showed that at low power levels the engraving depth increased rapidly, indicating high sensitivity of the ablation process to energy input. At higher power levels, the growth rate gradually decreased, suggesting partial saturation of the material removal process due to increased heat losses, carbonization effects, and the formation of a larger heat-affected zone.

The strongest increase in engraving depth with power was observed for samples thermally modified at 180°C and 225°C. Particularly for the 225°C sample, the slope of the depth curve remained relatively steep even at higher power levels, indicating enhanced susceptibility of highly modified wood to laser-induced thermal degradation and ablation.

The analysis of scanning speed showed an inverse relationship between speed and both engraving width and depth. Increasing the scanning speed reduced the interaction time between the laser beam and the material, thereby decreasing the energy delivered per unit length. The most pronounced changes occurred at low scanning speeds (25–100 mm/s), where the curves exhibited steep negative slopes. At higher scanning speeds

(200–300 mm/s), the slopes became less pronounced, indicating a reduced sensitivity of the process to further increases in speed.

The nonlinear character of the obtained dependencies indicates that the laser engraving process is governed by complex interactions between energy absorption, thermal diffusion, carbonization, pyrolysis, and material removal mechanisms. The results also confirmed that thermal modification significantly changes the thermophysical behavior of wood during laser processing.

Overall, the study demonstrated that the most effective engraving conditions for achieving deep and relatively narrow engraved lines are obtained near the focal position $\Delta f = 0$ mm, using carefully optimized combinations of laser power and scanning speed. Precise control of these parameters is especially important for thermally modified wood, where the process sensitivity to energy density changes is significantly higher.

Conclusions

This study investigated the influence of focal position, laser power, and scanning speed on the geometrical parameters of CO_2 laser engraving of untreated and thermally modified aspen wood.

The obtained results demonstrated that the focal position is one of the most critical parameters affecting engraving quality. The optimal engraving conditions were achieved at the focal position $\Delta f = 0$ mm, where the laser energy density reached its maximum value. Under these conditions, the engraved lines exhibited minimum width and maximum depth. Defocusing of the laser beam resulted in increased line width and reduced engraving depth due to the expansion of the laser spot and reduction in local power density.

The analysis of graph slopes showed that the engraving process is highly sensitive to focal displacement in the near-focus region. Small deviations from the focal plane caused significant changes in both width and depth of the engraved structures. This effect was especially pronounced for thermally modified wood samples.

The study also confirmed that increasing laser power leads to an increase in both engraving width and depth, while increasing scanning speed reduces these parameters. However, the relationships were found to be nonlinear due to the complex interaction between laser energy absorption, heat transfer, carbonization, pyrolysis, and ablation mechanisms.

Thermal modification significantly altered the response of wood to laser processing. Samples treated at higher temperatures demonstrated reduced line widths, increased engraving depth sensitivity, and stronger dependence on laser energy density. These effects are associated with changes in the chemical composition and thermophysical properties of wood after thermal treatment, including reduced moisture content, degradation of hemicelluloses, and increased carbonization.

The results indicate that the optimization of CO_2 laser engraving of wood requires simultaneous adjustment of focal position, laser power, and scanning speed. Precise parameter selection is particularly important for thermally modified wood due to its increased sensitivity to laser-induced thermal effects.

The findings of this study contribute to a better understanding of the physical mechanisms governing laser–wood interaction and may be useful for improving the quality and efficiency of laser engraving processes in woodworking, decorative manufacturing, surface structuring, and industrial marking applications. Future research may include investigations of surface roughness, microstructural changes, heat-affected zones, and chemical modifications of laser-processed wood surfaces using advanced characterization methods such as SEM, FTIR, and profilometry.

References

1. D. Rāviņš, E. Yankov, I. Adijans, L. Lazov, and D. Rāviņš, "Investigating the Impactof Laser Power and Scan Speed on Engraving Aspen Thermowood." Volume: 3, pp.351-357 https://doi.org/10.17770/ETR2023VOL3.7250
2. Z. Gochev and P. Vitchev, "The Effect of the Focal Length Position of the Focusing Lens on the Discoloration Roughness of Plywood under Different CO_2 Laser Engraving Modes." Acta Facultatis Xylologiae Zvolen, 66(2), 75–88. Retrieved from https://ojs.tuzvo.sk/index.php/AFXZ/article/view/116
3. D. Kocaefe, S. Poncsak, and Y. Boluk, "Effect of Thermal Treatment on the Chemical Composition and Mechanical Properties of Birch and Aspen." 2008, Bioresurces 3(2):517-537, DOI: 10.15376/biores.3.2.517-537
4. G. Sosins et al., "Aspen Wood Characteristics Following Thermal Modification." G. Materials 2024, 17, 5930. https://doi.org/10.3390/ma17235930
5. H. Nguyen-Thi-Ngoc and T.-V. Dang, "Optimization of Process Parameters for Wood Laser Engraving Based on Taguchi Method Approach.", 2023, MM Science Journal 2023(3), DOI: 10.17973/MMSJ.2023_10_2023053
6. A.-S. Gusts and I. Adijāns, "Optimization of Parameters for Laser Marking and Engraving on Plywood and Pine Wood Materials." DOI: https://doi.org/10.17770/het2021.25.6795
7. I. Kubovský, Ľ. Krišťák, J. Suja, M. Gajtanska, R. Igaz, I. Ružiak, and R. Réh, "Optimization of Parameters for the Cutting of Wood-Based Materials by a CO_2 Laser," Applied Sciences, vol. 10, no. 22, p. 8113, 2020. DOI: 10.3390/app10228113.
8. J. Kúdela, I. Kubovský, and M. Andrejko, "Influence of Irradiation Parameters on Structure and Properties of Oak Wood Surface Engraved with a CO_2 Laser," Materials, vol. 15, no. 23, p. 8384, 2022. DOI: 10.3390/ma15238384.
9. J. Kúdela, I. Kubovský, and M. Andrejko, "Surface Properties of Beech Wood after CO_2 Laser Engraving," Coatings, vol. 10, no. 1, p. 77, 2020. DOI: 10.3390/coatings10010077.
10. J. Kúdela, I. Kubovský, and M. Andrejko, "Discolouration and Chemical Changes of Beech Wood After CO_2 Laser Engraving," Forests, vol. 15, no. 12, p. 2211, 2024. DOI: 10.3390/f15122211.
11. G. A. Doğan, R. Wascher, G. Avramidis, W. Viöl, and C. Gerhard, "Influence of Wood Modification on Parameter Settings and Treatment Results in CO_2

Laser Structuring of Beech Veneers," Journal of Materials Science: Materials in Engineering, vol. 19, article 41, 2024. DOI: 10.1186/s40712-024-00192-6.

12. M. Jurek and R. Wagnerová, "Laser Beam Calibration for Wood Surface Colour Treatment," European Journal of Wood and Wood Products, vol. 79, pp. 1097–1107, 2021. DOI: 10.1007/s00107-021-01704-3.
13. D. Rāviņš, E. Yankov, I. Adijāns, and V. Bakakins, "The Impact of CO_2 Laser Power and Scanning Speed on Various Wood and Thermowood Samples," Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference, 2024. DOI: 10.17770/etr2024vol3.8170.
14. L, Lazov., N. T. Dolchinkov, et al,, 2019, "Study of laser cutting and marking on the filt with the help of a CO2-laser", Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 3, pp. 143–14, https://doi.org/10.17770/etr2019vol3.4202
15. L. Lazov, P. Narica, J. Valiniks, H. Deneva, D. Klavins, 2017 "Optimization of CO2 laser parameters for wood cutting." Vide Tehnologija Resursi Environment Technology Resources Open source preview, 3, pp. 168–173 http://dx.doi.org/10.17770/etr2017vol3.2624
16. L. Lazov, T. Karadzhov, 2021, „Methods for measuring laser power", Vide Tehnologija Resursi Environment Technology ResourcesOpen source preview, 3, pp. 173–180, DOI:10.17770/etr2021vol3.6565
17. N. Angelov, Edmunds Teirumnieks, L. Lazov 2021, Influence of pulse duration on the process of laser marking of CT80 carbon tool steel products, Laser Physics, Volume 31, Number 4, pp. 11-12 DOI 10.1088/1555-6611/abe5af
18. L. Lazov, E. Teirumnieks, N. Angelov, E. Teirumnieka, 2019, **Methodology for automatic determination of contrast of laser marking for different materials**, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 12th International Scientific and Practical Conference, Volume III, 134-136, http://dx.doi.org/10.17770/etr2019vol3.4143

LASER SURFACE HARDENING OF MEDIUM-CARBON STEELS: PROCESS OPTIMIZATION, MICROSTRUCTURAL EVOLUTION, AND INDUSTRIAL APPLICATIONS

Normunds Teirumnieks

University of Transport "Todor Kableshkov", Sofia, Bulgaria,
normunds.teirumnieks@gmail.com

***Abstract**: Laser surface hardening (LSH) has emerged as a transformative surface treatment technology offering precise localized hardening with minimal distortion and self-quenching capability. This review comprehensively examines the current state of LSH for medium-carbon steels (0.30–0.60 wt% C), with particular emphasis on 42CrMo4 (AISI 4140) and C45 (AISI 1045) steels widely used in automotive gear applications. The fundamental mechanisms of laser-material interaction, microstructural transformations, and process parameter optimization are systematically analyzed. Recent advances in high-power diode laser (HPDL) and fiber laser technologies are discussed, highlighting their advantages over conventional CO_2 laser systems. Key process parameters—including laser power, scanning speed, power density, beam profile, and overlapping strategy—are evaluated in relation to hardened case depth, microhardness profiles, and surface integrity. The influence of initial material condition, surface absorptivity, and self-quenching versus polymer-assisted quenching on hardening efficiency is critically assessed. A comparative analysis with conventional hardening methods (induction, flame, carburizing, nitriding) demonstrates the superior geometric flexibility, minimal distortion, and environmental benefits of LSH. Industrial applications across automotive, aerospace, tool and die, and medical sectors are reviewed. Optimization strategy using multi-objective methodologies such as DEFMOT is described. This review identifies current research gaps and proposes future directions, including real-time process monitoring, predictive modeling, and integration with Industry 4.0 frameworks.*

***Keywords:** Laser surface hardening, medium-carbon steel, 42CrMo4, C45, high-power diode laser, martensitic transformation, process optimization, automotive gears, surface integrity.*

Introduction

The intensification of industrial production, combined with growing demand for components with enhanced surface mechanical properties, has driven significant progress in surface heat treatment technologies over the past three decades. Among these technologies, laser surface hardening (LSH) has emerged as one of the most versatile, precise, and environmentally compatible methods for locally strengthening metallic components subject to tribological and fatigue loading [1, 2].

In the automotive industry, components such as gears, camshafts, crankshafts, and transmission elements are subjected to extreme cyclic contact stresses, sliding wear, and fatigue loads [3-5]. The performance and service life of these components are directly linked to the quality of their surface layer. For decades, conventional methods like induction hardening, flame hardening, and carburizing have been the industrial standards [6, 7]. However, these techniques often involve significant drawbacks, including high thermal distortion due to bulk heating, the need for external quenchants (water, oil, polymers), and limited flexibility for complex part geometries [8, 9].

Laser surface hardening offers a transformative alternative. By using a defocused high-power laser beam as a localized heat source, LSH rapidly heats a thin surface layer above the austenitizing temperature, followed by extremely rapid "self-quenching" as heat dissipates into the cold underlying bulk material [10, 11]. This process generates a fine, hard martensitic microstructure exclusively in the irradiated zone, with minimal distortion and no need for external quench media [12-15]. These characteristics make LSH particularly attractive for precision automotive gears manufactured from medium-carbon steels such as 42CrMo4 and C45, where maintaining tight tolerances is critical.

Medium-carbon steels, encompassing compositions with carbon content in the range of 0.30–0.60 wt%, represent one of the most widely used categories of structural steels in mechanical engineering applications. Grades such as C45 (AISI 1045), 42CrMo4 (AISI 4140), 50CrMo4, and 40CrNiMo (AISI 4340) are extensively employed in the manufacture of shafts, gears, camshafts, crankshafts, dies, and tooling components, where the combination of adequate core toughness with a hard, wear-resistant surface layer is essential for reliable long-term performance [20, 21].

The recent development of high-power diode lasers (HPDLs) has been a game changer for industrial LSH applications. These lasers operate at near-infrared wavelengths (808–980 nm), which are absorbed significantly better by ferrous alloys (≈35–45%) compared to CO_2 lasers (≈5–15%). Furthermore, HPDLs provide a "top-hat" beam profile, ensuring uniform energy distribution and a consistent hardened layer without the central overheating characteristic of Gaussian beams [34, 114]. They also boast high electrical-to-optical efficiency (40–65%) and robust, low-maintenance operation. Commercial HPDL hardening systems with powers up to 8 kW and working spot sizes of 5 × 20 mm to 12 × 70 mm are now available, enabling high-throughput industrial processing [34].

Despite the clear advantages of HPDLs, a comprehensive, systematic understanding of their application to 42CrMo4 and C45 steels under realistic industrial conditions remains incomplete. While isolated studies exist on parameter effects, there is a gap in integrated research that links laser parameters (power, scanning speed) to a complete surface integrity assessment, including hardened depth (case depth), microhardness profiles, surface hardness, and three-dimensional surface roughness evolution.

The present review aims to systematically evaluate the effectiveness of laser surface hardening in medium-carbon steels 42CrMo4 and C45. The study synthesizes current knowledge on process parameter optimization within certain operational ranges, while comprehensively characterizing the resulting microstructural transformations and mechanical properties. A comparative analysis against established hardening methods is provided to offer industry-relevant performance metrics and implementation guidelines. The review also examines advanced optimization strategies, including multi-objective methodologies such as DEFMOT, for determining optimal processing parameters that balance case depth, surface hardness, roughness, and microstructural stability.

This paper is organized as follows: Section 1 presents the fundamentals of laser surface hardening, including the mechanism, microstructural transformations, and critical process parameters. Section 2 discusses laser sources and beam shaping technologies suitable for hardening applications. Section 3 examines material-specific considerations,

including the role of chemical composition, initial microstructure, and surface condition. Section 4 provides a comparative analysis with conventional hardening methods. Section 5 reviews industrial applications across various sectors. Section 6 discusses optimization strategies and process modeling. Section 7 identifies research gaps and future directions. Finally, conclusions are presented in Section 8.

1. Laser Surface Hardening: Fundamentals and Mechanisms

1.1. Laser Surface Hardening Mechanism

Laser surface hardening exploits the high energy density of focused laser radiation to rapidly heat the steel surface to temperatures above the austenitizing point (Ac_3), typically between 900 and 1300 °C, followed by ultra-rapid self-quenching as the heat dissipates into the cool bulk material. Unlike conventional hardening, no external quenchant is required. Cooling rates in the order of 10^3–10^4 °C/s are routinely achieved, far exceeding the critical martensite formation rate for medium-carbon steels, resulting in a case-hardened surface layer with hardness values between 550 and 900 HV [25, 26].

The laser beam head scans across the steel surface, forming a martensitic hardened layer, a partial martensite transition zone, and a tempered heat-affected zone above the unaffected pearlitic-ferritic base material [27]. The process involves:

1. **Heating phase**: The laser beam rapidly heats the surface to austenitizing temperature, with heating rates of 10^2–10^3 °C/s [40].
2. **Dwell phase**: The surface is maintained above Ac_3 for a brief period (milliseconds to seconds) to allow carbon diffusion and austenite homogenization [46].
3. **Cooling phase**: Heat dissipates into the cold substrate through thermal conduction, achieving self-quenching at rates of 10^3–10^4 °C/s [48].

Three distinct metallurgical zones develop in the treated cross-section [28, 29]:

(1) Hardened Zone (HZ): Fully austenitized and quenched layer, composed entirely of martensite, sometimes retaining small amounts of austenite. Peak hardness 650–900 HV.

(2) Transition Zone (TZ): Partially austenitized region containing a mixture of martensite, ferrite, and residual pearlite. Hardness decreases progressively towards the substrate.

(3) Heat-Affected Zone (HAZ): Tempered or coarsened region below Ac_1 that has experienced thermal exposure but has not undergone phase transformation. May exhibit slight hardness reduction relative to the base material.

Figure 1 shows a schematic of the laser surface hardening process, illustrating the thermal zones and self-quenching mechanism.

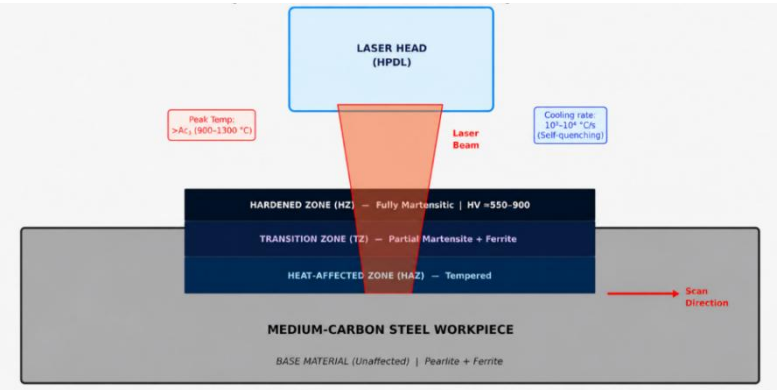


Figure 1: Schematic of the laser surface hardening process showing the laser beam, thermal zones (HZ, TZ, HAZ), and self-quenching mechanism in medium-carbon steel.

1.2. Microstructural Transformations During Laser Hardening

1.2.1. Formation of Austenite

Austenite is formed from the combined pearlite–ferrite or pearlite–cementite structure of α-iron. In equilibrium transformation, austenite starts to form at the Ac_1 temperature (727 °C) in carbon steels and ends at the Ac_3 (Acm) line. Heating rates as high as 1000 K/s are common during laser hardening with a steep temperature gradient [40]. The higher heating rate during laser hardening not only shifts the Ac_3 line up towards higher temperature [41], but also switches the mechanism of austenite formation from carbon diffusion control to a massive mechanism [42].

Considering that the heating rate in laser hardening is rather high, the curve can shift significantly from the equilibrium state, and the Ac_3 line tends to shift upward to a higher temperature. In order to achieve sufficient austenite homogenisation above the Ac_3 (Acm) temperature, the process parameters are usually set to reach a high peak temperature. Because a short thermal cycle may cause insufficient carbon diffusion, the degree of carbon homogenisation in the parent material has a substantial effect on the carbon distribution in the formed martensite and on the resulting hardness profile [43-45].

1.2.2. Homogenization

The transformation of ferrite to austenite, dissolution of cementite (Fe_3C), and carbon diffusion in austenite are all time-dependent, which means the high temperature must be maintained for sufficiently long period to allow diffusion of atoms and microstructure homogenization [46]. The thermal cycle during laser hardening is much shorter than conventional heat treatment, lasting only a few seconds or fractions of a second—not enough for complete dissolution and diffusion of carbon in austenite. Such insufficient time can leave austenite with lower carbon content than in homogenized case, reducing the hardness of the martensite formed. From another point of view, prior-austenite grain

size is also proportional to the time available for homogenization, which directly influences the block and packet size in martensite [47].

1.2.3. Formation of Martensite

Complete martensitic transformation occurs at a relatively high cooling rate—usually tens of degrees Celsius per second or more. Martensite is a supersaturated solid solution of carbon in α-iron, with a body-centered tetragonal (BCT) lattice structure due to slight shift of iron atoms to adjust for trapped carbons, thus providing a barrier to slip. Steel in the martensitic state contains large internal stresses, which make it hard but also brittle [48, 49].

During the cooling phase, the austenite-to-martensite transformation starts at the martensite start temperature (M_s) and ends at the martensite finish temperature (M_f). Martensite forms within a temperature range that depends on the carbon content of the steel. The M_s temperature depends only weakly on the cooling rate. An increased carbon content lowers M_s and M_f, thereby decreasing the required critical cooling rate. Alloying elements such as manganese and nickel also lower M_s [50-52].

Figure 2 illustrates the continuous-cooling-transformation (CCT) diagram for a eutectoid carbon steel, showing the critical cooling rate required for 100% martensite formation.

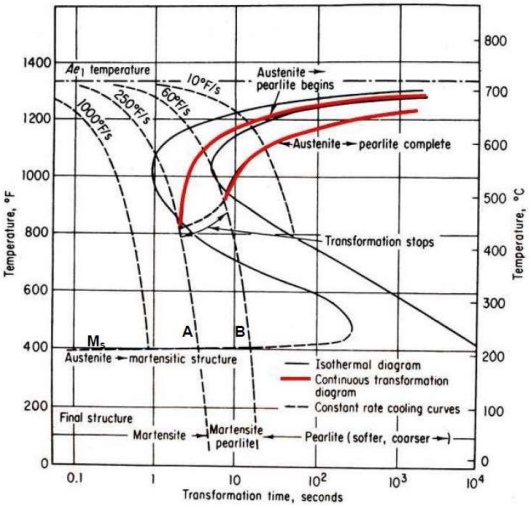


Figure 2: Continuous-cooling-transformation (CCT) diagram for eutectoid carbon steel showing critical cooling rates for martensite formation [48].

Some austenite may remain when cooling to room temperature, thereby reducing the hardness of the steel. Several factors can cause this—for example, local variation in carbon concentration due to material inhomogeneity and the presence of austenite-stabilising elements. As the carbon concentration increases, the M_s and M_f temperatures

are lowered (M_f can even drop below room temperature). When room temperature is reached during cooling, a portion of the austenite may not transform into martensite, and some austenite remains in the structure. Certain alloying elements such as manganese and nickel lower M_s and M_f, so that the amount of retained austenite can increase. As a common practice, retained austenite is converted into martensite by sub-zero treatment (i.e., cooling to -70 °C or even lower) [56].

1.3. Laser Hardenable Steels and Material Properties Affecting Hardening

Not all steels respond equally to laser hardening. The microstructural response is governed primarily by chemical composition—in particular carbon content and alloying element additions—as well as the initial microstructural state [63, 64].

The hardness of the surface after laser surface hardening depends primarily on the hardness of the martensite formed, which is directly proportional to the amount of carbon content in the steel [86]. A minimum carbon content of approximately 0.25 wt% is required to achieve meaningful surface hardness after laser treatment. Below this threshold, the martensite formed is insufficiently hard for most industrial applications. The optimal range for laser hardening is 0.30–0.60 wt% of carbon. Steels with higher carbon content (>0.60 wt%) tend to develop excessive retained austenite and are more susceptible to cracking [64, 65].

Figure 3 shows the typical martensitic microstructure hardness as a function of steel carbon content after quenching.

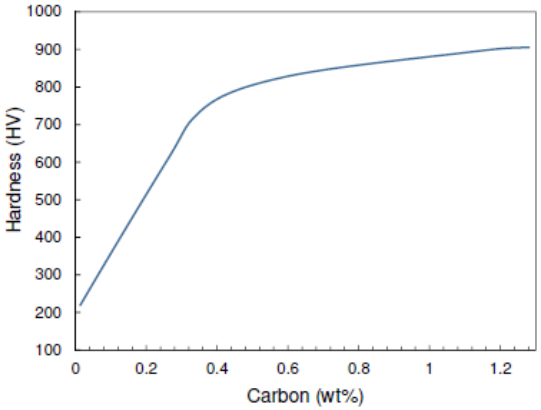


Figure 3: Typical martensitic microstructure hardness as a function of steel carbon content after quenching [86].

1.3.1. Medium-Carbon Steels for Laser Hardening

C45 / AISI 1045 (0.42–0.48 wt% C): The most widely studied and applied medium-carbon steel for laser hardening. Achieves surface hardness of 600–750 HV after LSH under optimal conditions. Used extensively in gears, shafts, axles, and machine tool

spindles. C45, with approximately 0.45% carbon but no strong alloying elements, has limited hardenability, resulting in a steep hardness gradient and a hardened depth highly sensitive to cooling rate [75]. Nonetheless, its cost-effectiveness and good machinability make it ubiquitous for general engineering components [76]. Lesyk et al. [31] demonstrated that C45 achieves case depths of 0.5–0.8 mm at power densities of 40–100 W/mm², with significant wear resistance improvements.

42CrMo4 / AISI 4140 (0.38–0.45 wt% C): The chromium-molybdenum addition significantly improves hardenability, allowing deeper case depths (0.8–1.5 mm) compared to plain carbon steels. 42CrMo4, with additions of chromium (~1%) and molybdenum (~0.2%), exhibits significantly enhanced hardenability, allowing for deep martensite formation even at moderate cooling rates [77]. It is a preferred material for high-stress components such as shafts, gears, and connecting rods [78]. Fan et al. [32] performed detailed FEM and experimental validation of LSH on 42CrMo4, achieving 720–780 HV surface hardness. Gu et al. [79] examined dual-track overlapping hardening of 42CrMo steel, identifying back-tempering zones.

50CrMo4 (0.47–0.54 wt% C): Higher carbon and chromium content leads to improved wear resistance. It has medium hardenability and is intended for medium and large machine components that require high hardness, high strength, and good toughness [80]. Maharjan et al. [33] conducted a systematic study of laser power and scan speed effects on 50CrMo4, demonstrating hardness values of 740–800 HV and case depths up to 1.2 mm.

1.3.2. Role of Alloying Elements

Beyond carbon, the following alloying elements play important roles in laser hardening response [84, 85]:

- **Chromium (Cr)**: Improves hardenability and forms stable carbides, increasing tempering resistance and wear resistance.
- **Molybdenum (Mo)**: Suppresses temper brittleness and enhances hardenability significantly.
- **Nickel (Ni)**: Increases toughness of martensite and reduces the martensite start temperature (M_s), increasing retained austenite fraction.
- **Manganese (Mn)**: Acts as a solid-solution strengthener and lowers M_s temperature.
- **Silicon (Si)**: Inhibits carbide formation, stabilizing martensite against tempering.

1.3.3. Surface Condition and Absorptivity

The efficiency of laser energy absorption depends primarily on the surface characteristics of the material and the wavelength of the applied laser beam. During laser processing, the focused beam delivers energy to the metal surface, where it is absorbed and converted into heat, causing rapid temperature rise. Since metals generally exhibit high reflectivity, the absorption of laser energy can be enhanced through surface modifications, such as applying absorptive coatings or altering the surface condition [87-89].

A material's ability to absorb laser energy is significantly influenced by its surface texture and initial surface condition [90]. Surface roughness promotes multiple reflections of the laser beam within the surface irregularities, resulting in more efficient energy absorption. Consequently, treatments such as sandblasting enhance laser absorptivity by increasing surface roughness.

The absorptance of steel increases as the amount of surface oxide increases. Oxide layers exhibit higher absorptivity than the bare steel surface. Pantsar and Kujanpää [91] reported that the formation of an absorbing oxide layer can significantly increase absorptivity, reducing the laser power required for hardening by up to 50%.

For polished 42CrMo4, absorptivity at 808 nm is ~40% at room temperature, rising to ~60–70% above 700 °C due to oxidation and the temperature dependence of optical constants. Oxide layers, phosphate coatings, or surface roughening can increase absorptivity to 80–95%, significantly affecting process stability [91, 92].

1.3.4. Material Geometry Effects

The geometry of the workpiece has a significant effect on the distribution of heat during laser processing. As a general guideline, the thickness of the workpiece should be at least ten times the required hardening depth to allow effective self-quenching while preventing excessive heating of the underlying material core. Additionally, sufficient distance should be maintained between the laser-treated tracks and the workpiece edges to avoid localized overheating or surface melting. External corners, due to their higher surface-area-to-volume ratio, are more susceptible to rapid heat accumulation and overheating. In contrast, internal corners exhibit the opposite behaviour and are less prone to excessive temperature rise [93-95].

1.4. Laser Parameters

1.4.1. Wavelength and Absorptivity

The absorptivity of a material to laser radiation is highly dependent on the wavelength of the incident laser beam. Steel has relatively low absorptivity and high reflectivity at the wavelength of a CO_2 laser (approximately 10.6 μm). Consequently, absorptive coatings or black paint are often applied to the surface prior to CO_2 laser processing to enhance energy absorption. In general, the absorptivity of metallic materials increases as the laser wavelength decreases. Therefore, lasers operating at shorter wavelengths, such as Nd:YAG, high-power diode (HPDL), and fiber lasers, achieve higher absorption efficiency and require little or no surface pretreatment [96, 97].

Figure 4 shows the absorption of laser radiation at different wavelengths for different metals.

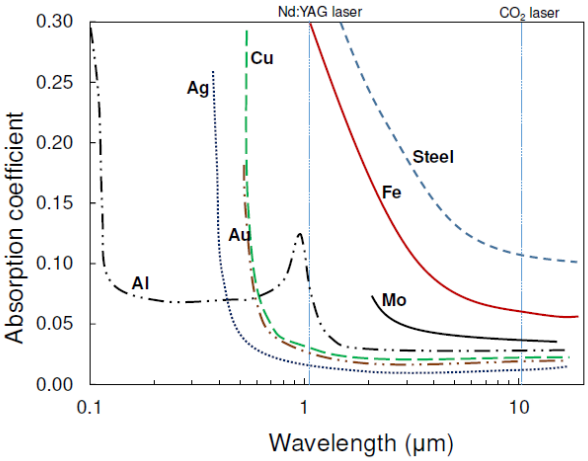


Figure 4: Absorption of laser radiation at different wavelengths for different metals [98].

1.4.2. Laser Power and Power Density

Laser power density should be defined as the laser power delivered per unit area of the laser beam, as it describes the intensity of the incident radiation on the workpiece surface [99-101].

In laser surface hardening, power densities typically range from 10^3 to 10^5 W/cm², which are sufficient to induce phase transformation without causing surface melting. Power density is the single most important process parameter, determining the peak temperature reached at the surface. The optimal range for martensite formation without surface melting is 30–150 W/mm² for typical medium-carbon steels. At power densities above ~200 W/mm² (depending on interaction time), surface melting occurs. At densities below ~20 W/mm², peak temperatures may fall below Ac_3, resulting in insufficient austenitizing [27].

Figure 5 shows the interaction time and power density required for various laser processing methods.

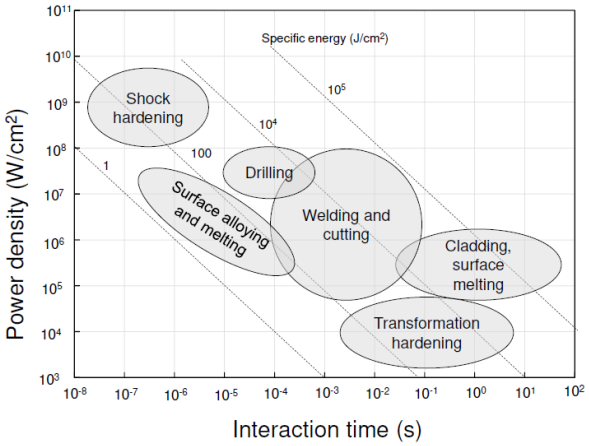


Figure 5: Interaction time and power density required for various laser processing methods [102].

1.4.3. Scanning Speed

Scanning speed controls the interaction time and thus the depth of heat penetration. Slower scanning at constant power increases case depth but raises peak temperatures, increasing the risk of melting and introducing larger HAZs. For C45 steel, scanning speeds of 3–15 mm/s are typical for single-track LSH with HPDL systems at powers of 1–4 kW [34, 39].

1.4.4. Overlapping

When hardening large surfaces, multiple parallel tracks are required with lateral overlap of 20–60%. The overlap region is reheated by the adjacent track and may be tempered back to lower hardness than the first track—the so-called "back-tempering" or "soft band" effect. The back-tempered zone can reduce hardness by 100–300 HV relative to the freshly hardened track, depending on the overlap ratio, power density, and scanning speed [79, 104, 105].

1.4.5. Process Gas

Use of process gas is not mandatory for laser hardening, but it has two main advantages. First, it minimizes oxidation in the laser hardened surface, thus preventing increase in absorptivity and surface overheating. Second, it protects the optics from being contaminated during the process. Generally, argon is used as a shielding gas during laser hardening due to its inert nature. The gas is supplied at the hardened area using a nozzle at the rate of 5-20 L/min [110, 111].

1.4.6. Laser Beam Profiles

The spatial intensity distribution of the laser beam at the workpiece surface—its "beam profile"—has a decisive influence on the uniformity of hardening, the achievable case depth, and the risk of surface melting. Matching the beam profile to the process

requirements is one of the most important aspects of laser hardening system design [114, 115].

An unmodified single-mode laser beam exhibits a Gaussian intensity profile, characterized by a smooth bell-shaped distribution with the peak intensity at the beam centre. For laser hardening, this is generally undesirable: the central region of the beam can exceed the melting temperature while the edges remain below Ac_3, leading to surface melting at the centre and under-hardening at the edges. The conversion of a Gaussian beam to a uniform flat-top (top-hat) distribution is therefore a fundamental requirement for most hardening applications [112, 115].

For specific laser hardening applications, tailored beam profiles can provide additional benefits by optimizing the spatial distribution of heat input. M-shaped (bimodal) beam profiles, which exhibit higher intensity at the beam edges compared with the centre, can promote preheating of edge regions before the maximum thermal load is applied. This controlled energy distribution is particularly beneficial for hardening complex geometries, such as gear tooth flanks, where edge regions are more susceptible to excessive heat loss and over-tempering effects [116, 117].

Figure 6 compares laser beam intensity profiles widely used in laser surface hardening.

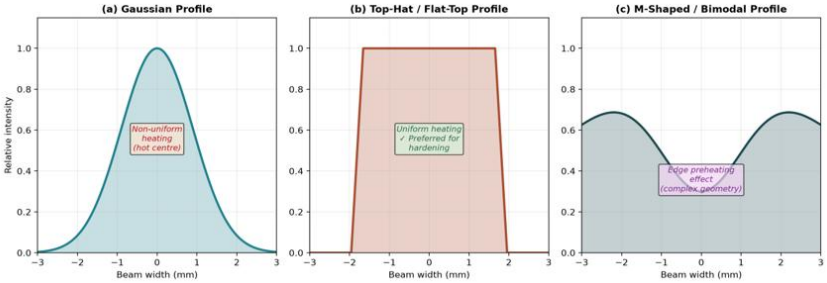


Figure 6: Laser beam intensity profiles used in surface hardening: (a) Gaussian—non-uniform heating with risk of surface melting at centre; (b) top-hat/flat-top—preferred for uniform hardening; (c) M-shaped/bimodal—used for edge preheating in complex geometry hardening.

2. Laser Sources for Surface Hardening

The choice of laser system is one of the most critical decisions in establishing a laser hardening process. Parameters including wavelength, beam quality, power output, electrical efficiency, and beam delivery flexibility all directly affect the quality, productivity, and cost of the hardening operation [114, 121].

2.1. CO_2 Lasers ($\lambda = 10.6$ μm)

CO_2 lasers are high-power gas lasers that have been widely employed in industrial material processing due to their high output power, reliability, and ability to treat large surface areas. However, the long operating wavelength results in relatively low absorptivity for most metallic materials because of their high reflectivity in the infrared

region. Consequently, surface coatings or surface modifications may be required to enhance laser energy absorption during processing. Compared with shorter-wavelength laser sources, CO_2 lasers generally exhibit lower energy coupling efficiency with metals [112, 122, 123].

2.2. Nd:YAG Lasers (λ = 1.064 μm)

Nd:YAG lasers are solid-state lasers that operate at a wavelength of 1.064 μm. Due to their shorter wavelength compared with CO_2 lasers, Nd:YAG lasers exhibit improved absorption characteristics in metallic materials, resulting in more efficient laser energy coupling during material processing. Their good beam quality, capability for continuous and pulsed operation, and compatibility with fibre-optic beam delivery have made them suitable for a wide range of industrial applications, including laser surface hardening. However, Nd:YAG lasers generally have lower energy efficiency and higher operating costs compared with modern fibre and high-power diode laser systems [112, 124-126].

2.3. High-Power Diode Lasers (HPDLs, λ = 808–980 nm)

High-power diode lasers have become the dominant choice for industrial laser surface hardening due to their combination of:

- High wall-plug efficiency (40–65%)
- Compact footprint
- Low maintenance requirements
- Long diode lifetime (>20,000 hours)
- Direct generation of rectangular flat-top beam profiles
- Wavelengths in the 808–980 nm range where steel absorptivity (30–50%) is substantially higher than for CO_2

Commercial HPDL hardening systems are available from Laserline GmbH, Coherent, Lissotschenko Mikrooptik (LIMO), and others, with powers up to 8 kW and working spot sizes of 5 × 20 mm to 12 × 70 mm [34, 114].

Czupryński et al. [34] conducted an extensive study of HPDL-hardened C45 steel, demonstrating hardness of 670–720 HV, case depths of 0.4–0.9 mm, and favourable compressive residual stresses. The absence of surface coating and the direct rectangular beam profile were identified as key practical advantages.

2.4. Fiber Lasers (λ = 1.06–1.08 μm)

Fiber lasers have emerged as the most powerful and versatile laser sources available, with commercial units delivering continuous-wave output up to 100 kW. The active medium is a rare-earth doped optical fiber (typically Yb^{3+}:silica), which enables wall-plug efficiencies >35%, excellent beam quality (BPP ~0.35–4 mm·mrad for single-mode to multi-mode), highly flexible beam delivery via fibre, and near-zero maintenance. For laser hardening, multi-mode fiber lasers with appropriate beam-shaping optics are preferred, as high beam quality alone produces undesirable Gaussian intensity distributions [123, 129].

Reich et al. [123] recently demonstrated laser hardening at 120 kW using a multi-beam fiber laser system, achieving very large treated areas at high scanning speeds. This result establishes a new benchmark for high-throughput surface hardening of large components such as ship propeller shafts.

2.5. Comparative Overview

Table 1 provides a comparative overview of different laser types used in surface hardening applications.

Table 1. Comparison of laser types for surface hardening applications.

Parameter	CO_2 laser	Nd:YAG laser	HPDL	Fiber laser
Laser type	Gas laser	Solid-state laser	Semiconductor laser	Solid-state fibre laser
Wavelength	10.6 µm	1.064 µm	808–980 nm	1.06–1.08 µm
Max power (CW)	≤20 kW	≤4 kW	≤10 kW	≤100+ kW
Wall-plug efficiency	10–15%	3–5%	40–65%	30–40%
Steel absorptivity	5–10%	30–35%	35–55%	30–40%
Absorptive coating required	Yes	Mostly not	No	Mostly not
Beam delivery	Mirror-based	Fibre or free-space	Direct or fibre	Fibre-optic
Beam profile	Gaussian	Gaussian	Rectangular/top-hat	Gaussian or tailored
Maintenance	High	Medium	Low	Very low
Suitability for LSH	Moderate	Good	Excellent	Very good

3. Process Optimization and Parameter Relationships

3.1. Effects of Laser Power and Scanning Speed on Hardening Characteristics

The relationship between laser process parameters and resulting hardening characteristics is complex and interdependent. Systematic experimental studies have

established quantitative relationships between laser power (P), scanning speed (v), and resulting case depth, surface hardness, and surface roughness.

Case Depth: The effective case depth increases with increasing laser power and decreasing scanning speed. For C45 steel, Lesyk et al. [31] demonstrated case depths of 0.5–0.8 mm at power densities of 40–100 W/mm². For 42CrMo4, Fan et al. [32] achieved case depths of 0.8–1.5 mm with surface hardness of 720–780 HV.

Surface Hardness: Surface hardness is maximized when the peak temperature reaches the optimal austenitizing range without exceeding the melting point. For medium-carbon steels, optimal hardness values of 650–800 HV are typically achieved. Higher power densities can lead to surface melting and reduced hardness, while insufficient power densities result in incomplete austenitization.

Surface Roughness: Laser surface hardening generally increases surface roughness due to thermal expansion and contraction cycles, as well as martensitic transformation-induced volume changes. The roughness parameters Sa (arithmetical mean height), Sq (root mean square height), and Sz (maximum height) increase with increasing power density and decreasing scanning speed. However, the roughness increase is significantly smaller than that observed in conventional hardening methods.

3.2. Initial Material Condition Effects

The initial material condition significantly influences the laser hardening response of medium-carbon steels. Two common conditions are:

Normalized Condition: Characterized by a fine pearlitic-ferritic microstructure. This condition provides good hardenability and consistent response to laser treatment. The fine grain size promotes rapid austenitization and uniform martensite formation.

Quenched-and-Tempered (Q&T) Condition: Characterized by a tempered martensitic microstructure. This condition provides higher initial hardness but may require different processing parameters compared to normalized material. The prior martensitic structure can affect austenitization kinetics and the distribution of alloying elements.

3.3. Quenching Strategy Effects

Self-Quenching: The standard LSH approach relies on heat dissipation into the cold substrate for cooling. This method is simple, cost-effective, and produces compressive residual stresses beneficial for fatigue performance. Cooling rates of 10^3–10^4 °C/s are typically achieved.

Polymer-Assisted Quenching: In some applications, additional quenching media (polymer solutions, water, or oil) are applied after laser treatment to increase cooling rates and improve hardness. This approach can enhance hardenability but introduces additional complexity and may increase distortion.

3.4. Multi-Objective Optimization

The optimization of laser surface hardening requires balancing multiple, often conflicting, objectives:

1. Maximizing case depth (for wear resistance and load-carrying capacity)

2. Maximizing surface hardness (for wear resistance)
3. Minimizing surface roughness (for tribological performance and fatigue life)
4. Ensuring microstructural stability (for long-term performance)

Multi-objective optimization methodologies, such as DEFMOT (Design of Experiments for Multi-Objective Optimization), provide systematic frameworks for identifying optimal processing parameter combinations. These methodologies typically involve:

1. Full factorial experimental design covering the main process parameters (laser power and scanning speed)
2. Quantitative relationships between process parameters and response variables
3. Pareto frontier analysis to identify trade-offs between conflicting objectives
4. Validation experiments to confirm optimal parameter combinations

4. Comparison with Conventional Hardening Methods

Laser surface hardening is one of several established surface hardening technologies. Table 2 provides a comprehensive comparison of process parameters and characteristics of conventional surface hardening methods and LSH.

Table 2. Comparison of process parameters and characteristics of conventional surface hardening methods and LSH.

Method	Case Depth (mm)	Distortion	Quench Medium	Cycle Time	Geometric Flexibility	Environment
Laser surface hardening	0.1–2.0	Very low	None (self-quench)	Seconds	Very high	Clean, no fumes
Induction hardening	0.5–6.0	Low	Water/polymer spray	Seconds–min	Medium	Clean
Flame hardening	0.5–6.0	High	Water spray	Minutes	Medium	Combustion gases
Carburizing	0.5–2.0	High	Oil/gas quench	Hours	Low	Gas atmosphere
Nitriding	0.05–0.5	Very low	None	20–100 h	Medium	NH_3 gas
Carbonitriding	0.1–0.75	Low	Oil quench	Hours	Low	Endothermic gas
Electrolytic-Plasma	0.3–1.5	Low	Electrolyte bath	Seconds–min	Low	Electrolyte waste

4.1. Advantages of Laser Surface Hardening

1. **Localized heating and minimal distortion**: Heat is applied only to the area to be hardened, drastically reducing thermal distortion and allowing treatment of finished, precision components without subsequent operations [10].

2. **Self-Quenching**: No external quenching media (water, oil, polymers) are required. This simplifies the process, reduces costs and environmental footprint, and eliminates the risk of uneven hardening or cracking due to excessively rapid cooling [10].

3. **High flexibility and selectivity:** The laser beam can be directed and controlled with high precision (e.g., with robots or galvo-scanners), enabling hardening of complex 3D geometries (such as gear tooth profiles) and even hard-to-reach areas [132, 134].

4. **High productivity:** Laser scanning is a fast process that significantly reduces processing time compared to batch furnace processes [132, 134].

5. **Controllability and reproducibility:** Laser parameters (power, speed, spot size) can be precisely controlled and automated, ensuring high repeatability of results [132, 134].

4.2. Disadvantages of Laser Surface Hardening

1. High initial equipment and operating cost: Laser surface hardening requires expensive laser sources, precision control systems, optical components, and automation equipment. The high capital investment can limit its adoption, especially for small-scale manufacturing operations [130, 132, 134].

2. **Limited hardening depth:** Compared with processes such as carburizing or induction hardening, LSH generally produces a relatively shallow hardened layer (typically from several hundred micrometres to a few millimetres depending on material and parameters). Therefore, it is not suitable for components requiring very deep case hardening [130, 132].

3. **Strict control of processing parameters:** The quality of the hardened layer strongly depends on laser power, scanning speed, beam size, material composition, and heat input. Improper parameter selection can lead to non-uniform hardness, excessive melting, undesirable microstructures, or insufficient hardening [130, 132, 134].

4. **Risk of surface defects and thermal damage:** Although LSH minimizes distortion compared with conventional heating methods, excessive laser energy or improper cooling conditions may cause surface cracking, residual stresses, oxidation, or localized thermal damage [130, 132].

5. Industrial Applications

5.1. Automotive Industry

Laser surface hardening is widely applied to automotive components to enhance their mechanical performance and service life. Typical applications include:

Gears: LSH improves wear resistance, contact fatigue strength, and load-carrying capacity of gear teeth while maintaining dimensional accuracy critical for smooth operation and low noise.

Camshafts and Crankshafts: Localized hardening of cam lobes and bearing journals extends component life under cyclic loading and sliding wear conditions.

Valves and Rocker Arms: Increased fatigue strength and reduced risk of surface-initiated failure under high-temperature, high-stress conditions.

Brake Discs: Enhanced wear resistance and extended service life under severe operating conditions.

Steel alloys, including AISI 4140, AISI 4340, and AISI 52100, are extensively used for these components because of their excellent hardenability [65, 131-133].

5.2. Aerospace Industry

Laser surface hardening and surface modification techniques are widely applied to aerospace components to enhance mechanical performance, durability, and service life under demanding operating conditions [131-134]:

Landing Gear Components: Improved fatigue strength, impact resistance, and resistance to surface damage during repeated loading cycles.

Turbine Blades: Enhanced wear resistance and improved surface durability under high-temperature and erosive environments.

Structural Components: Increased surface strength and damage tolerance while maintaining lightweight design.

Materials commonly processed include nickel-based superalloys (Inconel 718, Inconel 625), titanium alloys (Ti-6Al-4V), and high-strength steels (AISI 4340).

5.3. Tool and Die Industry

Laser surface hardening is extensively employed for improving the performance and service life of tooling components [65, 132-134]:

Moulds and Dies: Increased surface hardness, improved wear resistance, and extended operational lifetime for stamping and injection moulding operations.

Cutting Tools: Enhanced resistance to abrasive wear and improved cutting-edge integrity for high-speed machining applications.

Punches and Cutting Blades: Improved resistance to cyclic loading, edge degradation, and surface damage in metal-forming processes.

Materials commonly used include tool steels (AISI D2, AISI H13, AISI M2) and carbide-based materials (tungsten carbide, cobalt-bonded carbides).

5.4. Medical Equipment

Laser surface treatment techniques are increasingly applied in biomedical applications [37, 2, 38]:

Surgical Instruments: Improved surface hardness, wear resistance, and long-term durability under repeated sterilization and mechanical loading.

Prosthetic Components and Implants: Enhanced wear resistance, corrosion resistance, and biological performance.

Materials commonly used include stainless steels (17-4 PH, AISI 316L, AISI 420) and titanium alloys (Ti-6Al-4V, Ti-Nb-based alloys).

6. Research Trends and Publication Activity

The growing research interest in laser surface hardening is reflected by the increasing number of scientific publications over recent years. Figure 7 illustrates the number of publications on LSH from 2008 to 2024 [135].

The publication trend shows significant growth in research activity, particularly after 2017, indicating the rising interest in this technology from both scientific and industrial

communities. The continuous increase in publications reflects the recognized advantages of laser surface hardening, including high processing speed, precise control of the hardened zone, flexibility in treating complex geometries, reduced thermal distortion, and improved energy efficiency compared with conventional surface hardening methods.

This growth is also associated with the technological development of high-power diode lasers (HPDLs). The introduction of HPDL systems has significantly contributed to the wider acceptance of laser-based surface treatments by providing high electrical efficiency, compact system design, reliable operation, and the ability to deliver large-area, homogeneous heat input.

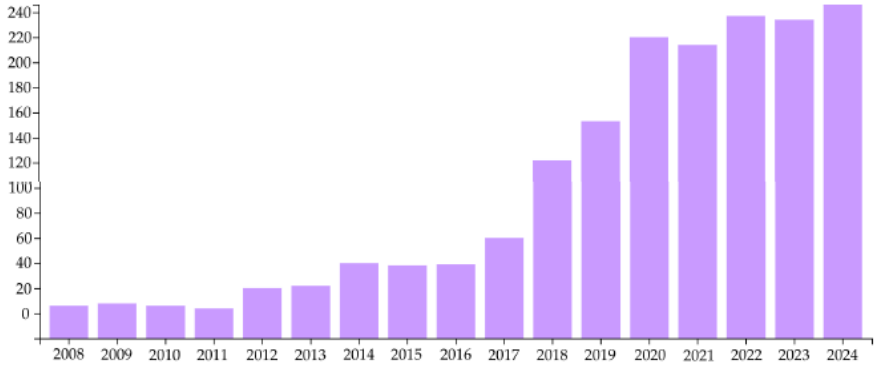


Figure 7: Number of publications on LSH from 2008 to 2024 [135].

7. Research Gaps and Future Directions

Despite the rapid growth in research activities and demonstrated technological benefits, several challenges remain before broader industrial implementation can be achieved. Further investigations are required to:

1. **Establish reliable process guidelines**: Develop standardized procedures for parameter selection specific to different materials and component geometries.
2. **Optimize parameters for specific applications**: Conduct systematic studies linking laser parameters to comprehensive surface integrity assessment for automotive gear applications.
3. **Improve process monitoring and control**: Develop real-time monitoring systems using thermal imaging, pyrometry, and optical coherence tomography for quality assurance.
4. **Integrate LSH with Industry 4.0**: Implement digital twins and machine learning algorithms for predictive process control and optimization.
5. **Address the back-tempering effect**: Develop strategies to minimize hardness reduction in overlapping regions when hardening large surfaces.

6. **Expand material applicability**: Investigate LSH of advanced materials including high-strength steels, cast irons, and titanium alloys.
7. **Develop hybrid processes**: Combine LSH with other surface treatments (shot peening, ultrasonic impact treatment) for enhanced performance.

8. Conclusions

This review has comprehensively examined the current state of laser surface hardening for medium-carbon steels, with particular emphasis on 42CrMo4 and C45 steels widely used in automotive gear applications. The following conclusions can be drawn:

1. **Fundamental Mechanisms**: LSH exploits rapid heating and self-quenching to generate martensitic microstructures with hardness values of 650–900 HV. Three distinct metallurgical zones (hardened zone, transition zone, and heat-affected zone) develop in the treated cross-section.
2. **Process Parameters**: Laser power, scanning speed, beam profile, and overlapping strategy are the primary parameters controlling case depth, surface hardness, and surface integrity. Optimal power densities for medium-carbon steels range from 30–150 W/mm².
3. **Material Considerations**: Medium-carbon steels (0.30–0.60 wt% C) offer the best balance between achievable martensite hardness and workpiece toughness. Alloying elements such as Cr, Mo, Ni, and Mn significantly influence hardenability and hardening response.
4. **Laser Sources**: High-power diode lasers (HPDLs) have become the dominant choice for industrial LSH due to their high efficiency, compact design, and excellent energy coupling with metallic materials.
5. **Comparative Advantages**: LSH offers superior geometric flexibility, minimal thermal distortion, self-quenching capability, and environmental benefits compared with conventional hardening methods.
6. **Optimization**: Multi-objective optimization methodologies provide systematic frameworks for identifying optimal processing parameter combinations that balance case depth, surface hardness, and surface roughness.
7. **Industrial Applications**: LSH is widely applied in automotive, aerospace, tool and die, and medical sectors for enhancing wear resistance, fatigue strength, and component durability.

References

1. Sello, I. O. (2025). Laser Surface Hardening: A Review of Processing Parameters and Their Effects on Hardness and Residual Stresses. International Journal of Engineering Innovations and Research, 14(5), 68-75.
2. Wang, J., Xia, Y., Liu, X., Xu, J., Liu, W., Xiao, Y., ... & Jiao, S. (2024). A comprehensive review of metal laser hardening: mechanism, process, and applications. The International Journal of Advanced Manufacturing Technology, 134(11-12), 5087-5115.

3. Mao, K. (2007). Gear tooth contact analysis and its application in the reduction of fatigue wear. Wear, 262(11-12), 1281-1288.
4. Liu, H., Liu, H., Zhu, C., & Parker, R. G. (2020). Effects of lubrication on gear performance: A review. Mechanism and Machine Theory, 145, 103701.
5. Yu, Z., & Xu, X. (2010). Failure investigation of a truck diesel engine gear train consisting of crankshaft and camshaft gears. Engineering Failure Analysis, 17(2), 537-545.
6. Rudnev, V., & Totten, G. E. (Eds.). (2014). ASM Handbook, Volume 4C: Induction Heating and Heat Treatment. ASM International.
7. Dossett, J. L., & Totten, G. E. (Eds.). (2013). ASM Handbook, Volume 4A: Steel Heat Treating Fundamentals and Processes. ASM International.
8. Lopez-Garcia, R. D., Medina-Juárez, I., & Maldonado-Reyes, A. (2022). Effect of Quenching Parameters on Distortion Phenomena in AISI 4340 Steel. Metals, 12(5), 759.
9. Fechte-Heinen, R., Surm, H., Babb, A., & Steinbacher, M. (2025). Distortion of Gears due to Induction Hardening with the Gap-to-Gap Technique. Proc. ASM 2nd Quenching and Distortion Engineering Conference.
10. Kennedy, E., Byrne, G., & Collins, D. N. (2004). A review of the use of high power diode lasers in surface hardening. Journal of Materials Processing Technology, 155-156, 1855-1860.
11. Ashby, M. F., & Easterling, K. E. (1984). The transformation hardening of steel surfaces by laser beams—I. Hypo-eutectoid steels. Acta Metallurgica, 32(11), 1935-1948.
12. López, V., Fernández, B., Belló, J., Ruiz, J., & Zubiri, F. (1995). Influence of Previous Structure on Laser Surface Hardening of AISI 1045 (C45) Steel. ISIJ International, 35(11), 1394-1399.
13. Mioković, T., Schulze, V., Vöhringer, O., & Löhe, D. (2007). Influence of cyclic temperature changes on the microstructure of AISI 4140 after laser surface hardening. Acta Materialia, 55(2), 589-599.
14. Mioković, T., Schulze, V., Vöhringer, O., & Löhe, D. (2006). Prediction of phase transformations during laser surface hardening of AISI 4140 including the effects of inhomogeneous austenite formation. Materials Science and Engineering: A, 435-436, 547-555.
15. Czupryński, A., Janicki, D., Górka, J., Grabowski, A., Wyględacz, B., Matus, K., & Karski, W. (2022). High-Power Diode Laser Surface Transformation Hardening of Ferrous Alloys. Materials, 15(5), 1915.
16. Dutta Majumdar, J., & Manna, I. (2003). Laser processing of materials. Sadhana, 28, 495-562.
17. Krauss, G. (2015). Steels: Processing, Structure, and Performance (2nd ed.). ASM International.
18. Ion, J. C. (2005). Laser Processing of Engineering Materials: Principles, Procedure and Industrial Application. Elsevier Butterworth-Heinemann.
19. Leitner, H. (2013). Laser Beam Hardening of Steels (Doctoral dissertation). Lappeenranta University of Technology.

20. Lesyk, D. A., Martinez, S., Mordyuk, B. N., Dzhemelinskyi, V. V., Lamikiz, A., & Prokopenko, G. I. (2020). Post-processing of the Inconel 718 alloy parts fabricated by selective laser melting. Surface and Coatings Technology, 381, 125136.
21. El-Awadi, G. A. (2023). Review of effective techniques for surface engineering material modification for a variety of applications. AIMS Materials Science, 10(4), 652-692.
22. Telrandhe, S. V., Bhagyaraj, J., Mishra, S., & Karagadde, S. (2018). A new approach to control and optimize the laser surface heat treatment of materials. Journal of Materials Processing Technology, 262, 492-502.
23. Wang, X. D., Lu, Chen, G. N., Hu, S. G., & Su, Y. P. (2006). Research on the temperature field in laser hardening. Beihang University, Optics and Technology, 8-13.
24. Xiufeng, W. (2003). Application of laser non-melting processing technology in the sheet metal forming (Doctoral dissertation). Beijing University of Aeronautics and Astronautics.
25. Leitner, H. (2013). Laser Beam Hardening of Steels (Doctoral dissertation). Lappeenranta University of Technology.
26. He, Z., Lei, L., Lin, S., Tian, S., Tian, W., & Yu, Z. (2024). Metal Material Processing Using Femtosecond Lasers: Theories, Principles, and Applications. Materials, 17(14), 3386.
27. Dutta Majumdar, J., & Manna, I. (2011). Laser material processing. International Materials Reviews, 56(5-6), 341-388.
28. Santo, A. M. E., Goia, F. A., Lima, M. S. F., & Riva, R. (2007). Laser Surface Remelting and Hardening of an Automotive Shaft Using a High-Power Fiber Laser. Materials Research, 10(4), 461-467.
29. Selvan, A., Subramanian, K., & Nath, A. K. (1999). Effect of laser surface hardening on En18 (AISI 5135) steel. Journal of Materials Processing Technology, 91(1-3), 29-36.
30. Anusha, E., Kumar, A., & Shariff, S. M. (2021). Finite element analysis and experimental validation of high-speed laser surface hardening process. The International Journal of Advanced Manufacturing Technology, 115(7-8), 2403-2421.
31. Lesyk, D. A., Martinez, S., Mordyuk, B. N., Dzhemelinskyi, V. V., Lamikiz, A., Prokopenko, G. I., ... & Tkachenko, O. M. (2020). Effects of laser heat treatment combined with ultrasonic impact treatment on the surface topography and hardness of carbon steel AISI 1045. Wear, 444-445, 203494.
32. Fan, Z., Tan, L., Liu, B., & Wu, X. (2021). Thermal-Metallurgical-Mechanical Modeling of Laser Surface Hardening of 42CrMo4 Steel and Experimental Validation. Advances in Mechanical Engineering, 13(9), 1-18.
33. Maharjan, N., Zhou, W., Zhou, Y., & Wu, N. (2021). Depth-Controlled Laser Hardening of 50CrMo4 Steel. Metals, 11(12), 2015.

34. Czupryński, A., Górka, J., & Żuk, M. (2022). Testing of Properties and Structure of Hardened Layers Obtained by Laser Beam Treatment of Carbon Steel. Materials, 15(5), 1928.
35. Chen, C., Zeng, X., Wang, Q., Lian, G., Huang, X., & Wang, Y. (2020). Statistical modelling and optimization of microhardness transition through depth of laser surface hardened AISI 1045 carbon steel. Optics & Laser Technology, 124, 105976.
36. Yilbas, B. S., Akhtar, S. S., & Karatas, C. (2012). Laser surface treatment of 42CrMo4 steel: Heating and cooling cycle and thermal stress analysis. Optics and Lasers in Engineering, 50(1), 76-81.
37. Moarrefzadeh, A. (2021). Simulation, Modeling and Experimental Study of Laser Surface Hardening Process. Universal Journal of Mechanical Engineering, 9(1), 1-14.
38. Stähli, G. (1981). Physical and materials-related problems in short-time surface hardening of steel using high frequency laser and electron beams. Tribology International, 14, 101-106.
39. Albutt, K. J., & Garber, S. (1966). Effect of heating rate on the elevation of the critical temperatures of low-carbon mild steel. Journal of the Iron and Steel Institute, London, 204, 1217-1222.
40. Cerda, F. M. C., Sabirov, I., Goulas, C., Sietsma, J., Monsalve, A., & Petrov, R. H. (2017). Austenite formation in 0.2% C and 0.45% C steels under conventional and ultrafast heating. Materials & Design, 116, 448-460.
41. Steen, W. M. (2003). Laser Material Processing (3rd ed.). Springer-Verlag.
42. Brooks, C. R. (1992). Principles of the Austenitization of Steels. Springer.
43. Su, W., Zhou, T., Zhang, P., Zhou, H., & Li, H. (2018). Effect of distribution of striated laser hardening tracks on dry sliding wear resistance of biomimetic surface. Optics & Laser Technology, 98, 281-290.
44. Pantsar, H. (2007). Relationship between processing parameters, alloy atom diffusion distance and surface hardness in laser hardening of tool steel. Journal of Materials Processing Technology, 189, 435-440.
45. Prawoto, Y., Jasmawati, N., & Sumeru, K. (2012). Effect of prior austenite grain size on the morphology and mechanical properties of martensite in medium carbon steel. Journal of Materials Science and Technology, 28, 461-466.
46. Porter, D. A., & Easterling, K. E. (1992). Phase Transformations in Metals and Alloys (2nd ed.). CRC Press.
47. Bhadeshia, H., & Honeycombe, R. (2017). Steels: Microstructure and Properties. Butterworth-Heinemann.
48. Sverdlin, A. V., & Ness, A. R. (2006). Steel Heat Treatment Handbook. In G. E. Totten (Ed.), Steel Heat Treatment Handbook (2nd ed., Ch. 3). CRC Press.
49. Grum, J. (2006). Steel Heat Treatment: Equipment and Process Design. In G. E. Totten (Ed.), Steel Heat Treatment: Equipment and Process Design (2nd ed., Ch. 6). CRC Press.

50. Thelning, K.-E. (1984). Steel and Its Heat Treatment (2nd ed.). Butterworth-Heinemann.
51. Zhang, H., Dou, B., Tang, H., He, Y., & Guo, S. (2018). Secondary hardening in laser rapidly solidified Fe68(MoWCrVCoNiAlCu)32 medium-entropy high-speed steel coatings. Materials & Design, 159, 224-231.
52. Krauss, G. (1999). Martensite in steel: strength and structure. Materials Science and Engineering A, 273, 40-57.
53. Komanduri, R., & Hou, Z. B. (2004). Thermal analysis of laser surface transformation hardening — optimization of process parameters. International Journal of Machine Tools & Manufacture, 44, 991-1008.
54. Komanduri, R., & Hou, Z. B. (2001). Thermal analysis of the laser surface transformation hardening process. International Journal of Heat and Mass Transfer, 44, 2845-2862.
55. Skvarenina, S., & Shin, Y. C. (2006). Laser-assisted machining of compacted graphite iron. International Journal of Machine Tools and Manufacture, 46(1), 7-17.
56. Lusquinos, F., Conde, J. C., Bonss, S., Riveiro, A., Quintero, F., Comesana, R., & Pou, J. (2007). Theoretical and experimental analysis of high-power diode laser (HPDL) hardening of AISI 1045 steel. Applied Surface Science, 254, 948-954.
57. Weisheit, A., & Mordike, B. L. (1991). Laser surface modification of materials. Processing IMT Conf., Birmingham.
58. Magazov, N., Satbaeva, Z., Rakhadilov, B., & Amanov, A. (2023). A Study on Surface Hardening and Wear Resistance of AISI 52100 Steel by Ultrasonic Nanocrystal Surface Modification and Electrolytic Plasma Surface Modification Technologies. Materials, 16(20), 6824.
59. Roy, S., Zhao, J., Shrotriya, P., & Sundararajan, S. (2017). Effect of laser treatment parameters on surface modification and tribological behavior of AISI 8620 steel. Tribology International, 112, 94-102.
60. Karamimoghadam, M., Rezayat, M., Conceição, T., Reis, P. N. B., & Mourão, A. (2024). Influencing factors on a recently developed laser surface hardening process of steels: A review. Metals, 14(3), 339.
61. Gnana Sambandam, D. S., Krishnaraj, P., & Muthuramalingam, T. (2021). Machinability analysis of medium carbon steel treated by laser surface hardening. Materials Today: Proceedings, 45, 6873-6877.
62. Lela, B., Bajić, D., & Jozić, S. (2009). Regression analysis, support vector machines, and Bayesian neural network approaches to modeling surface roughness in face milling. The International Journal of Advanced Manufacturing Technology, 42(11-12), 1082-1088.
63. Li, R., Jin, Y., Li, Z., & Qi, K. (2014). A comparative study of high-power diode laser and CO2 laser surface hardening of AISI 1045 steel. Journal of Materials Engineering and Performance, 23, 3085-3091.

64. Martínez, S., Lamikiz, A., Ukar, E., Calleja, A., Arrizubieta, J. A., & de Lacalle, L. N. L. (2017). Analysis of the regimes in the scanner-based laser hardening process. Optics and Lasers in Engineering, 90, 72-80.
65. Sun, P., Li, S., Yu, G., He, X., Zheng, C., & Ning, W. (2014). Laser surface hardening of 42CrMo cast steel for obtaining a wide and uniform hardened layer by shaped beams. International Journal of Advanced Manufacturing Technology, 70, 787-796.
66. Sorgente, D., Corizzo, O., Ancona, A., Scintilla, L. D., Palumbo, G., & Tricarico, L. (2014). Laser hardening of AISI 52100 bearing steel with a discrete fiber laser spot. Proc. SPIE, 8963, 896308.
67. Lee, J. H., Jang, J. H., Joo, B. D., Son, Y. M., & Moon, Y. H. (2009). Laser surface hardening of AISI H13 tool steel. Transactions of Nonferrous Metals Society of China, 19, 917-920.
68. Oh, S., & Ki, H. (2017). Prediction of hardness and deformation using a 3-D thermal analysis in laser hardening of AISI H13 tool steel. Applied Thermal Engineering, 121, 951-962.
69. Mahmoudi, B., Torkamany, M. J., Aghdam, A. R. S. R., & Sabbaghzade, J. (2010). Laser surface hardening of AISI 420 stainless steel treated by pulsed Nd:YAG laser. Materials & Design, 31, 2553-2560.
70. Mai, T. A., & Lim, G. C. (2004). Diode laser hardening of steel surfaces. Surface and Coatings Technology, 187, 106-113.
71. Gu, F., Wu, Y., Zhang, Y., & Lian, S. (2022). Simulation and Experimental Verification of Two-Track Laser Surface Hardening of 42CrMo Steel. Surface Review and Letters, 29(4), 2250039.
72. LUCEFIN. (2021). 50CrMo4 (1.7228): Medium-Carbon, 1Cr-0.2Mo Direct Hardening Alloy Steel. Alloy Digest, 70(11). ASM International.
73. Koyanbayev, Y. (2024). Applying the Hollomon-Jaffe parameter to predict changes in mechanical properties of irradiated austenitic chromium-nickel steels during isothermal exposure. AIMS Materials Science, 11(1), 216-230.
74. Koga, N., Yamashita, T., Ogawa, K., & Umezawa, O. (2022). Statistical Analysis of Influential Factors on the Stability of Retained Austenite in Low Alloy TRIP Steel. Materials Transactions, 63(5), 693-702.
75. Zhai, R., Wang, W., Ma, R., et al. (2020). Hot deformation behavior and processing map of as-cast 40CrNiMo alloy steel. Journal of Materials Engineering and Performance, 29(2), 964-974.
76. Maity, J., Poona, B. S., Kumar, M., Pal, A., Hazra, B., Sahin, S., & Biswas, A. (2023). Quantitative hardness-carbon content-microstructure correlation in normalized plain carbon steel. Materialwissenschaft und Werkstofftechnik, 54(11), 1444-1453.
77. Chen, S., Mostert, R., & Aarnts, M. (2023). Heat treatment effects on microstructure and properties of advanced high-strength steels. Materials Science and Technology, 39(18), 2657-2670.
78. Bergström, D. (2008). The absorption of laser light by rough metal surfaces. Luleå University of Technology.

79. Pantsar, H., & Kujanpää, V. (2006). Effect of oxide layer growth on diode laser beam transformation hardening of steels. Surface and Coatings Technology, 200(16-17), 4880-4888.
80. Bonss, S., Goebel, G., Seifert, M., Brenner, B., & Beyer, E. (2003). Fast and innovative determination of parameters for steel hardening with high power diode lasers. Proc. SPIE, 4831.
81. Pantsar, H., & Kujanpää, V. (2004). Diode laser beam absorption in laser transformation hardening of low alloy steel. Journal of Laser Applications, 16(3), 147-153.
82. Ready, J. (1997). Industrial Applications of Lasers (2nd ed.). Academic Press.
83. Steen, W. M., & Courtney, C. (1979). Surface heat treatment of En8 steel using a 2kW continuous-wave CO2 laser. Metals Technology, 6, 456-462.
84. Ashby, M. F., & Easterling, K. E. (1984). The transformation hardening of steel surfaces by laser beams—I. Hypo-eutectoid steels. Acta Metallurgica, 32(11).
85. Li, W. B., Easterling, K. E., & Ashby, M. F. (1986). Laser transformation hardening of steel—II. Hypereutectoid steels. Acta Metallurgica, 34, 1533-1543.
86. Davis, J. R. (2002). Surface hardening of steels: understanding the basics. ASM International.
87. Grum, J. (2004). Laser Surface Hardening. In G. E. Totten (Ed.), Steel Heat Treatment: Equipment and Process Design (2nd ed., pp. 641-731). CRC Press.
88. Yao, C., Xu, B., Huang, J., Zhang, P., & Wu, Y. (2010). Study on the softening in overlapping zone by laser-overlapping scanning surface hardening for carbon and alloyed steel. Optics and Lasers in Engineering, 48, 20-26.
89. Ion, J. C. (2005). Laser Processing of Engineering Materials: Principles, Procedure and Industrial Application. Elsevier.
90. Romoli, L., Tantussi, G., & Dini, G. (2014). Experimental approach to the laser surface treatment of aluminium alloys with a high-power diode laser. Optics and Lasers in Engineering, 54, 131-139.
91. Ready, J. F. (2001). LIA Handbook of Laser Materials Processing. Springer.
92. Chichkov, B. N., Momma, C., Nolte, S., von Alvensleben, F., & Tünnermann, A. (1996). Femtosecond, picosecond and nanosecond laser ablation of solids. Applied Physics A, 63, 109-115.
93. Steen, W. M., & Mazumder, J. (2010). Laser Material Processing (4th ed.). Springer.
94. Bonss, S., Seifert, M., Beyer, E., Brenner, B., & Hannweber, J. (2021). Beam shaping for laser surface hardening processes. EPIC Workshop on High Power Diode Lasers.
95. Moradi, M., Arabi, S., Jamshidi Nasab, S., & Benyounis, K. Y. (2019). A comparative study of laser surface hardening of AISI 410 and 420 martensitic stainless steels by using diode laser. Optics & Laser Technology, 111, 604-611.

96. Murzin, S. P., Kazanskiy, N. L., & Stiglbrunner, C. (2021). Analysis of the Advantages of Laser Processing of Aerospace Materials Using Diffractive Optics. Metals, 11(6), 963.
97. Zhu, J., Xiong, Y., & Hu, Y. (2022). Beam profile effects on laser transformation hardening of gear flanks. International Journal of Machine Tools and Manufacture, 171, 103814.
98. Möhl, M., Kaldun, D., Kunz, C., Müller, J., Fuchs, F., & Gräf, T. (2019). Tailored focal beam shaping and its application in laser material processing. Journal of Laser Applications, 31(4), 042013.
99. Mann, K., Schäfer, B., & Herwig, I. (2007). Beam shaping for high power diode lasers. Proc. SPIE 6456.
100. Ponticelli, G. S., Guarino, S., & Giannini, O. (2020). An Optimal Genetic Algorithm for Fatigue Life Control of Medium Carbon Steel in Laser Hardening Process. Applied Sciences, 10(4), 1401.
101. Meijer, I. (2004). Laser beam machining (LBM), state of the art and new opportunities. Journal of Materials Processing Technology, 149(1-3), 2-17.
102. Reich, M., Schumann, J., Wießner, M., & Wetzig, A. (2024). High-throughput laser surface hardening using a 120 kW multi-beam fiber laser system. Procedia CIRP, 130, 217-222.
103. Moradi, M., Arabi, S., Karami Moghadam, M., & Benyounis, K. Y. (2019). Enhancement of surface hardness and metallurgical properties of AISI 410 by laser hardening process; diode and Nd:YAG lasers. Optik, 194, 163096.
104. Borki, A. K., El Ouafi, A., & Chebak, A. (2019). Experimental Investigation of Laser Surface Transformation Hardening of 4340 Steel Spur Gears. Journal of Manufacturing and Materials Processing, 3(3), 72.
105. Svelto, O. (2010). Principles of Lasers (5th ed.). Springer.
106. IPG Photonics. (2023). High Power Fiber Lasers for Industrial Surface Treatment. Technical Report.
107. Babu, P. D., Balasubramanian, K. R., & Buvanashekaran, G. (2011). Laser surface hardening: a review. International Journal of Surface Science and Engineering, 5(2/3), 131-151.
108. Senthil Kumar, P., Jegadheesan, C., Somasundaram, P., et al. (2023). State of the art: Review on laser surface hardening of alloy metals. Materials Today: Proceedings.
109. Santhanakrishnan, S., & Dahotre, N. B. (2013). Laser Surface Hardening. In ASM Handbook, Volume 4A: Steel Heat Treating Fundamentals and Processes.
110. Dahotre, N. B., & Harimkar, S. P. (2008). Laser Fabrication and Machining of Advanced Materials. Springer.
111. Telasang, G., Majumdar, J. D., Padmanabham, G., & Manna, I. (2014). Structure–property correlation in laser surface treated AISI H13 tool steel for improved mechanical properties. Materials Science and Engineering: A, 599, 255-267.

112. Guo, C., Zhou, J., & Chen, J. (2012). Laser surface treatment of titanium alloy for biomedical applications: A review. Surface & Coatings Technology, 206(23), 4630-4637.
113. Candel, J. J. B., & Amigó, V. (2011). Recent advances in laser surface treatment of titanium alloys. Journal of Laser Applications, 23(2), 022006.
114. Vollertsen, F., Sprenger, A., Kraus, J., & Arnet, H. (1999). Extrusion, channel, and profile bending: a review. Journal of Materials Processing Technology, 87(1-3), 1-27.
115. Sagdoldina, Z., Baizhan, D., Buitkenov, D., Tleubergenova, G., Alibekov, A., & Bolatov, S. (2026). The Effect of Laser Surface Hardening on the Microstructural Characteristics and Wear Resistance of 9CrSi Steel. Materials, 19(2), 423.
116. Bonss, S., Seifert, M., & Brenner, B. (2012). Laser beam surface hardening with high power diode lasers and their industrial applications. Proc. SPIE 8239.
117. Bonss, S., Seifert, M., Willsch, C., & Beyer, E. (2005). Advantages of diode lasers for hardening and soldering. Proc. Third Int. WLT-Conf. Lasers in Manufacturing.
118. Shin, H. J., Yoo, Y. T., Ahn, D. G., & Im, K. (2007). Laser surface hardening of S45C medium carbon steel using Nd:YAG laser with a continuous wave. Journal of Materials Processing Technology, 187-188, 467-470.
119. Łach, Ł. (2024). Recent Advances in Laser Surface Hardening: Techniques, Modeling Approaches, and Industrial Applications. Crystals, 14(8), 726.
120. Lambiase, F., Aghajani Derazkola, H., & Simchi, A. (2020). Friction Stir Welding and Friction Spot Stir Welding Processes of Polymers-State of the Art. Materials, 13(10), 2291.
121. Jurči, P. (2020). History, Developments and Trends in the Heat Treatment of Steel. Materials, 13(18), 4003.
122. Parrish, G. (1972). Flame Hardening. Springer.
123. Semiatin, S. L., & Stutz, D. E. (1986). Induction Heat Treatment of Steel. ASM International.
124. Qi, Z., Luo, X., Liang, F., Chai, F., Ge, Q., Zhan, Z., ... & Liu, Y. (2025). Effect of Induction Heating Temperature on the Uniformity of Mechanical Properties of Bulb Flat Steel Sections in the Quenched State. Materials, 18(11), 2626.
125. Babič, M., & Marinković, D. (2022). Prediction of Laser Hardening Parameters by Artificial Neural Network and Fractal Analysis. Applied Sciences, 12(5), 2458.
126. Rudnev, V. I., & Loveless, D. (2014). Basic Principles of Induction Hardening. In G. F. Krauss (Ed.), Comprehensive Materials Processing, Vol. 12: Thermal Engineering of Steel Alloy Systems. Elsevier.
127. Lichioiu, V. (2022). Pack Carburizing Effect on Microstructure and Hardness of 1.7131 Steel. RECENT, 68, 112-117.
128. Furlani, M. R., de Carvalho, S. M., de Siqueira, R. H. M., & de Lima, M. S. F. (2022). Reduced Coefficient of Friction of Laser Surface Hardened AISI 4130

Steel Substrates. Material Design & Processing Communications, 2022, 7541853.
129. Pye, D. (2003). Practical Nitriding and Ferritic Nitrocarburizing. ASM International.
130. Parrish, G., & Harper, G. S. (1985). Production Gas Carburising. Pergamon Press.
131. Roliński, E. (2015). Plasma-Assisted Nitriding and Nitrocarburizing of Steel and Other Ferrous Alloys. In Thermochemical Surface Engineering of Steels (pp. 413-457). Woodhead Publishing.
132. Gupta, P., Tenhundfeld, G., Daigle, E. O., & Ryabkov, D. (2007). Electrolytic plasma technology: Science and engineering—An overview. Surface and Coatings Technology, 201, 8746-8760.
133. Kluczyński, J., Jasik, K., Łuszczek, J., & Pokropek, J. (2025). Laser Surface Hardening of Carburized Steels: A Review of Process Parameters and Application in Gear Manufacturing. Materials, 18(15), 3623.
134. Vollertsen F., Sprenger A., Kraus J., and Arnet H., "Extrusion, channel, and profile bending: a review," Journal of Materials Processing Technology, vol. 87, no. 1-3, pp. 1-27, 1999.
135. Kluczyński J., Jasik K., Łuszczek J., Pokropek J., "Laser Surface Hardening of Carburized Steels: A Review of Process Parameters and Application in Gear Manufacturing" Materials 2025, 18(15).

A MISO 2×1 SOFTWARE-DEFINED RADIO MODEM WITH ALAMOUTI TRANSMIT DIVERSITY: DESIGN AND EXPERIMENTAL EVALUATION

Ivan P. Ivanov

Defence Institute "Professor Tsvetan Lazarov", Sofia, Bulgaria, i.p.ivanov@di.mod.bg

Abstract: *A multiple-input single-output (MISO) packet QPSK software-defined radio modem with two coherent transmit chains and one receive antenna is presented. A preamble from one antenna and orthogonal training slots give the receiver both transmit-channel estimates for the Alamouti combiner. Indoor over-the-air runs with single-chain and unaligned-start controls show that an aligned timed start of the transmit chains is what makes the space-time code decode.*

Keywords: *software-defined radio, transmit diversity, Alamouti code, space-time block coding, QPSK, over-the-air measurement*

Introduction

Communication and information systems (CIS) are a fundamental part of the contemporary national security system, and radio communication is the part of them that realises mobility. Crisis management [1] is where this is felt first: the situation changes faster than infrastructure can be laid, and the traffic that matters most travels while at least one end is moving. A link with a moving end is a link through a fading channel, and the moving end is the one least able to carry a second antenna, so the diversity that makes the link dependable is bought at the station.

A packet radio link indoors loses frames in the deep fades of one propagation path rather than in its average signal-to-noise ratio. Spatial diversity is the remedy, but the two ends of the link are rarely equally able to carry it. The transmitting side is usually the better provisioned one — a fixed station, a mast or a vehicle has the room and the power budget for a second antenna, whereas the terminal is where those budgets are tightest — so placing the second antenna at the transmitter buys diversity where it is affordable and leaves the terminal with one antenna, which is the case addressed here. The orthogonal space-time block code (STBC) for two transmit antennas [2] sends two symbols over two channel uses in a pattern whose rows are orthogonal, so a receiver with a single antenna separates them by a linear combination and reaches second-order diversity with no channel knowledge at the transmitter. The extension to more antennas keeps the orthogonality but not the unit rate [3], so the two-antenna case is the simple and rate-preserving one. The fading analysis is standard [4], and the matched-filter and multiple-antenna foundations are given in [5]. Transmit-side diversity has an older route: pre-RAKE processing, which combines the multipath in the transmitter and needs the channel known there through time-division duplex reciprocity; its noise immunity was studied for a class of mobile cellular systems [6]. The space-time code keeps the transmitter-side placement and drops the channel knowledge, which is what makes it usable on a link that carries none back.

On a software-defined radio (SDR) platform the coding itself is a few lines of a program [7], and the difficulty moves into the hardware: the two radio-frequency (RF) transmit chains have to be mutually coherent, and they have to begin radiating at the same instant.

Implementation-oriented SDR work has approached this from neighbouring directions: a single-channel π/4 differential quadrature phase-shift keying (π/4-DQPSK) modem modeled, simulated and implemented on SDR [8], a later two-branch implementation with diversity at the *receiving* end by equal-gain combining with fixed coefficients [9], and the official single-stream quadrature phase-shift keying (QPSK) packet examples of GNU Radio [10].

Public implementations sit on either side of the case reported here. A commercial toolbox ships a matched pair of examples that transmit and receive the code live on USRP radios [11]: the closest counterpart, but closed, with two receive antennas, and with the part this paper is about — how the two transmit chains are made to start together — hidden inside the toolbox radio object. In open code the scheme appears as building blocks, not as a modem: estimator and combiner blocks without examples or measurements [12], and the equivalent space-frequency form inside a standard-specific layer of an open cellular stack [13]. No packet modem was found that radiates the code from two coherent chains, estimates both channels from its own training at one antenna and validates every frame; this bounded survey does not establish global absence.

This paper reports the design, simulation and indoor over-the-air (OTA) evaluation of the two-antenna STBC on one SDR device with two coherent transmit chains and a single receive antenna. The contribution is not a new code: it is the reproducible packet-modem realization — frame protocol, orthogonal training, combining and packet validation — with two controls that isolate the practical precondition for it.

1 Transmit-diversity theory

Let s_1 and s_2 be two consecutive QPSK symbols. The two-antenna STBC [2] transmits them over two channel uses:

$$\mathbf{S}=\frac{1}{\sqrt{2}}\begin{bmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{bmatrix}, \tag{1}$$

where the columns are the antennas, the rows are the two channel uses, $(\cdot)^*$ denotes complex conjugation, and the factor $1/\sqrt{2}$ keeps the radiated energy per channel use equal to that of a single-antenna transmitter. With flat channel coefficients h_1 and h_2 that stay constant over the two channel uses, the single receive antenna observes [2], [4]

$$r_1=\frac{h_1 s_1+h_2 s_2}{\sqrt{2}}+w_1, \qquad r_2=\frac{-h_1 s_2^*+h_2 s_1^*}{\sqrt{2}}+w_2, \tag{2}$$

where w_1 and w_2 are zero-mean complex noise samples of equal variance. From the channel estimates $\hat{h}_1$ and $\hat{h}_2$ the receiver forms the two combiner outputs [2]

$$\hat{s}_1=\hat{h}_1^* r_1+\hat{h}_2 r_2^*, \qquad \hat{s}_2=\hat{h}_2^* r_1-\hat{h}_1 r_2^*. \tag{3}$$

With exact estimates the cross terms cancel and both outputs carry the same positive real gain [2], [4], so a QPSK decision is the sign of the real and imaginary parts:

$$\hat{s}_k = \frac{|h_1|^2+|h_2|^2}{\sqrt{2}}\, s_k + \tilde{w}_k. \tag{4}$$

The gain is the sum of two independent channel powers — second-order diversity without channel knowledge at the transmitter — and the price is that each antenna radiates half of the total power. For independent unit-power Rayleigh coefficients and coherent Gray QPSK, with $\mu(\bar{\gamma}) = \sqrt{\bar{\gamma}/(1+\bar{\gamma})}$, the two bit-error probabilities are [4], [5]

$$P_{b,1} = 1/2\,(1-\mu(\bar{\gamma})), \qquad P_{b,2} = 1/4\,(2-3\mu+\mu^3)\big|_{\mu=\mu(\bar{\gamma}/2)}, \tag{5}$$

where $\bar{\gamma}$ is the mean bit signal-to-noise ratio (SNR) at the receiver; the halved argument is the three-decibel cost of splitting the power between two antennas. The expressions assume independent coefficients, perfect channel knowledge and a channel constant within a code block; residual carrier-frequency offset (CFO), estimation error and correlated antennas reduce the gain. They are a simulation reference, not a claim about the indoor channel.

2 System model and architecture

An SDR unit is built from two constructive parts: a computing device, which runs the whole signal processing as a program, and an RF front end, which converts between analogue and digital and moves the signal in frequency [7]. Figure 1 places the modem across that boundary. The transmitter is the unit that differs: its front end is doubled, both chains belong to the same device, share the local oscillator and the sample clock, and are armed for a common future device time. The receiver keeps one computing device and a single-chain front end.

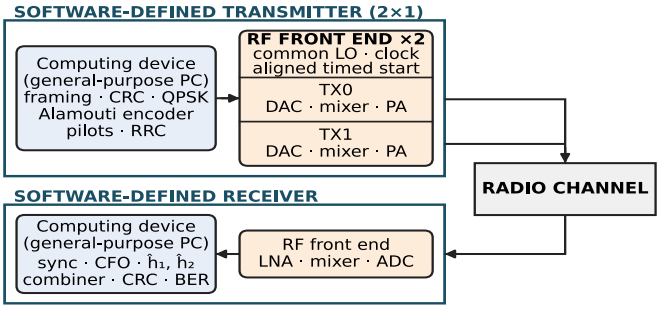


Figure 1: Constructive architecture of the modem.

Sharing an oscillator leaves a single carrier offset, the one between transmitter and receiver, so the carrier-recovery chain of the single-antenna modem is reused unchanged,

and a fixed amplitude or phase difference between the chains is absorbed into the estimated channels.

What the code does require is separate estimates of both transmit channels at a receiver that has one antenna. Figure 2 shows the frame that provides them. The preamble comes from one antenna only, so acquisition never depends on the sum h_1+h_2, which can fall into a deep fade; the small loss of preamble power is accepted in exchange. The training field is orthogonal in the transmit antennas: with a known pilot block t, the first slot sends $+t$ from both antennas and the second sends $+t$ and $-t$. Writing b_A and b_B for the two received slots, the least-squares estimates [2], [5] are

$$\hat{h}_1=\frac{\langle b_A,t\rangle+\langle b_B,t\rangle}{2\|t\|^2}, \qquad \hat{h}_2=\frac{\langle b_A,t\rangle-\langle b_B,t\rangle}{2\|t\|^2}, \tag{6}$$

where $\langle\cdot,\cdot\rangle$ is the inner product with the known pilot block. The sum and the difference of the two slots separate the two channels. The training slots are radiated without the $1/\sqrt{2}$ of the code block, so the estimates are of the channel coefficients themselves and the combiner output carries the scaling of the data alone, as written in Section 1.

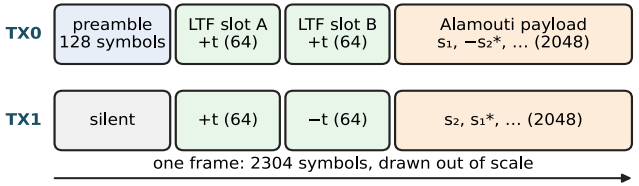


Figure 2: Frame on the two transmit chains.

Figure 3 gives the functional chain. The transmitter builds a deterministic packet, appends a cyclic redundancy check (CRC-32), maps Gray-coded QPSK symbols, encodes symbol pairs into the space-time pattern and applies root-raised-cosine (RRC) pulse shaping on both chains. The receiver detects the frame and estimates the carrier offset from the repeated-half preamble [14], estimates both channels from the training slots, combines, slices and validates the payload by bit comparison and by CRC.

3 Simulation

The companion Jupyter notebook implements Gray QPSK, additive white Gaussian noise, independent unit-power flat Rayleigh coefficients and perfect channel knowledge. For every E_b/N_0 point it processes 1,000,000 payload bits with a fixed seed, at equal total radiated power, and compares the Monte Carlo points with the expressions of Section 1. Figure 4 is generated by the executed notebook.

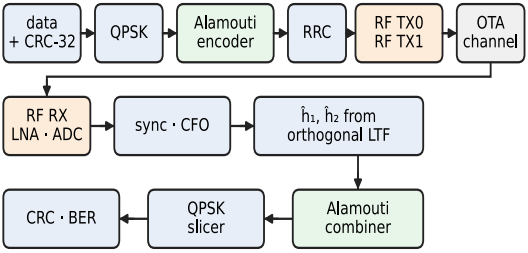


Figure 3: Functional block diagram of the modem.

At a mean E_b/N_0 of 10 dB the simulated bit-error rate (BER) is 2.33×10^{-2} without diversity and 5.52×10^{-3} with the two-antenna code, a factor of 4.2; the analytical values are 2.33×10^{-2} and 5.53×10^{-3}, and the gap widens with E_b/N_0 at the second-order slope. This is an ideal-model reference: it contains no synchronization loss, no estimation error and no hardware imbalance.

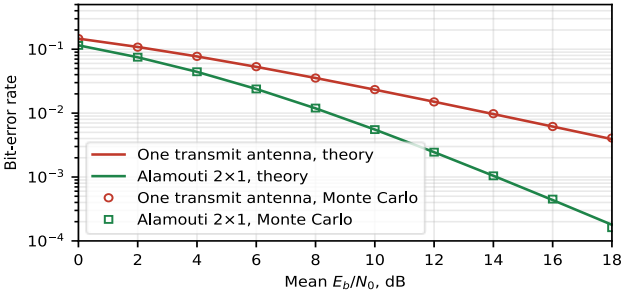


Figure 4: Simulated bit-error rate in flat Rayleigh fading.

4 Practical implementation

The demonstrator uses two Universal Software Radio Peripheral (USRP) B210-class SDR units [15]. The transmitting unit drives both chains from one streamer, which is what makes them coherent within the device; the receiver uses a single antenna. Table 1 lists the parameters of the waveform and of the live experiment.

Table 1: Modem and experiment parameters.

Parameter	**Value**
Topology	Two coherent transmit chains, one receive antenna
Carrier frequency	3.320 GHz
Sample / symbol rate	2 MS/s / 250 ksym/s
Samples per symbol	8

Parameter	**Value**
Modulation and shaping	Gray QPSK; RRC, roll-off 0.35, span 10 symbols
Preamble	128 symbols, transmit chain zero only
Training	128 symbols in two orthogonal slots
Payload and validation	4096 bits per frame; pseudorandom test field; CRC-32
Frame length	2304 symbols
Per-antenna scaling	$1/\sqrt{2}$ on the code block; equal total radiated power
Transmit start	Common future device time on both chains

The last row is the practical core of the implementation. Two chains of one device are coherent in frequency by construction, but not in time: each begins to radiate when its own first packet is accepted. The implementation therefore resets the device clock and marks the first sample packet of both chains with the same future device time, as a coherent multi-channel receiver is armed. Without that step the two rows of the code matrix no longer belong to the same channel use, and the orthogonality the combiner depends on is destroyed.

5 Experimental results and evaluation

Table 2 reports three indoor OTA runs of the same waveform, receiver and room, each of 300 detected frames and 1,228,800 payload bits, none logging a stream overflow or a dropped batch. The error-vector magnitude (EVM) column holds means over frames.

Table 2: Over-the-air runs and controls.

Configuration	**Chains**	**Aligned**	**TX gain**	**CRC valid**	**Payload BER**	**EVM**
Aligned timed start	2	yes	52 dB	300 / 300	none observed	11.9%
Single chain	1	—	42 dB	0 / 300	2.69×10^{-2}	49.1%
No aligned start	2	no	42 dB	0 / 300	4.38×10^{-1}	63.5%

With the aligned start and adequate link margin every frame passed the CRC and no payload bit error was observed in 1,228,800 bits. A zero-error observation is reported as the one-sided upper confidence bound 2.44×10^{-6} rather than as a true BER of zero. Both estimated transmit channels stood well above the noise floor, so both antennas were radiating and both were received.

The two diagnostic runs share their transmit gain, so they form a power-matched pair, and they answer what a working run cannot. With a single chain the same encoder, receiver and combiner still decode, and the estimated second channel is at the noise floor. With both chains radiating but without the aligned start the bit-error rate rises by more than an order of magnitude, no frame passes the CRC, and the link is worse than with one antenna alone. A second transmit antenna therefore makes the link worse until the two chains start together: the aligned start is a precondition of transmit diversity on this platform, not a refinement of it.

The evidence boundary is stated explicitly. The aligned run had more link margin than the two controls and is not compared with them. The runs are single indoor realizations and do not measure a diversity order, which would need a fading ensemble and an attenuator sweep. Coherence is demonstrated inside one device, not between devices. No live run retained raw samples, so the logged events and aggregates are the final evidence.

Conclusion

A packet QPSK modem with two coherent transmit chains and one receive antenna has been implemented and measured on air. In the aligned configuration every detected frame passed the packet check with no observed payload bit error, while the diagnostic runs show that two transmit chains without a common start are worse than one chain alone. The result is twofold: the transmit-diversity chain is reproducible on ordinary software-defined radio hardware, and its enabling condition is the aligned start of the chains, not any part of the decoding arithmetic. That is the cost of placing diversity where a link can usually afford it — at the transmitting station rather than at the terminal.

Acknowledgments

This work was supported by the National Scientific Program Security and Defense, funded by the Ministry of Education and Science of the Republic of Bulgaria under grant agreement no. D01-74/19.05.2022.

References

1. Ivanov, V., & Manchev, A. (2021). Crises and some possibilities for their successful management [in Bulgarian]. International Scientific Conference "Contemporary Research and Technologies for Defence ARTDEF 2021", Nikola Yonkov Vaptsarov Naval Academy, Varna, I-86–I-93. ISSN 2815-2581.
2. Alamouti, S. M. (1998). A simple transmit diversity technique for wireless communications. IEEE Journal on Selected Areas in Communications, 16(8), 1451–1458. doi:10.1109/49.730453
3. Tarokh, V., Jafarkhani, H., & Calderbank, A. R. (1999). Space-time block codes from orthogonal designs. IEEE Transactions on Information Theory, 45(5), 1456–1467. doi:10.1109/18.771146
4. Simon, M. K., & Alouini, M.-S. (2005). Digital Communication over Fading Channels (2nd ed.). Wiley.
5. Sklar, B., & Harris, F. J. (2021). Digital Communications: Fundamentals and Applications (3rd ed.). Pearson Education.
6. Angelov, M. (1999). Study of the noise immunity of pre-RAKE diversity reception for a class of mobile cellular systems [in Bulgarian]. National Conference with International Participation TELECOM'98, Vol. I, 631–637.
7. Ivanov, I. P. (2025). Software-Defined Radio Communication Systems [in Bulgarian]. Defence Institute, Sofia. ISBN 978-619-90024-8-3.

8. Ivanov, I. (2023). Modeling, Simulation and Implementation of pi/4-DQPSK Modem on SDR. Proc. XXXII International Scientific Conference Electronics (ET 2023), IEEE, 1–5. doi:10.1109/ET59121.2023.10278732
9. Ivanov, I., & Angelov, M. (2024). Design and Implementation of Software-Defined pi/4-DQPSK Modem with Receive Antenna Diversity. Environment. Technology. Resources, 3, 101–104. doi:10.17770/etr2024vol3.8108
10. GNU Radio Project. (2026). Packet Communications. GNU Radio Wiki. https://wiki.gnuradio.org/index.php/Packet_Communications (accessed 29.08.2026).
11. MathWorks. (2026). Alamouti Coding Based MIMO Transmitter and Receiver Using USRP Radio. https://www.mathworks.com/help/comm/usrpradio/ug/alamouti-coding-based-mimo-transmitter-using-usrp-radio.html (accessed 29.08.2026).
12. Ettus, M. (2022). gr-simpleMIMO: MIMO blocks for diversity and space-time block coding. GitHub repository, commit db60e10. https://github.com/MattEttus/gr-simpleMIMO
13. srsRAN Project. (2026). srsRAN_4G: transmit-diversity precoding in the LTE physical layer. GitHub repository, commit 6bcbd9e. https://github.com/srsran/srsRAN_4G
14. Schmidl, T. M., & Cox, D. C. (1997). Robust frequency and timing synchronization for OFDM. IEEE Transactions on Communications, 45(12), 1613–1621. doi:10.1109/26.650240
15. Ettus Research. (2026). UHD and USRP Manual: USRP B2x0 Series.

RFNOC-BASED FMCW WAVEFORM GENERATION FOR USRP SDR

Ivan P. Ivanov, Sevdalin Spassov

Defence Institute "Professor Tsvetan Lazarov", Sofia, Bulgaria, i.p.ivanov@di.mod.bg, s.spasov@di.mod.bg

Abstract: *An FPGA-resident RFNoC source for the USRP X310 generates CW and configurable FMCW waveforms. Unlike host streaming, Ethernet carries only control and status. The design provides phase control, packet-safe stopping, and backpressure handling. Host tests, six XSim scenarios, X310 implementation and timing closure, and initial hardware operation validate the architecture for a future SDR-based FMCW radar.*

Keywords: *software-defined radio, RFNoC, FMCW generator, FPGA, USRP X310*

Introduction

Software-defined radio (SDR) transfers radio functions from fixed-purpose hardware to programmable processing. The resulting platform can change waveform, bandwidth, modulation, and signal-processing algorithms without redesigning the complete radio-frequency (RF) chain. This flexibility has made SDR an established instrument for rapid prototyping of communications, sensing, and radar systems. A previous practical implementation demonstrated a continuous-wave (CW) Doppler radar using a USRP front end and GNU Radio and confirmed that an SDR platform can support experimental radar development with limited additional RF hardware [1].

The conventional host-centric SDR model nevertheless becomes less attractive as instantaneous bandwidth and sample rate increase. A host must generate or receive continuous complex in-phase and quadrature (IQ) streams, move them through memory, and transport them through Ethernet, USB, or PCI Express. The transport demand is proportional to sample rate, sample width, number of channels, and operating time. For example, a 160 MS/s stream represented as 16-bit I and 16-bit Q samples contains 5.12 Gbit/s of payload before packet overhead. Such a stream may be technically transportable over an appropriate interface, but it is inefficient when every sample is determined by a small set of waveform parameters. Host scheduling and transport buffering also complicate deterministic timing and can cause underflow or overflow.

The growth of field-programmable gate array (FPGA) capacity has consequently led to a heterogeneous SDR model. Algorithms are partitioned between general-purpose host software and programmable logic located close to the analog-to-digital converter (ADC), the digital-to-analog converter (DAC), and the RF interface. Functions with high data rates, strict timing, regular arithmetic, or low control bandwidth are particularly suitable for FPGA execution. The software still defines radio behavior, but it does so by configuring hardware processing blocks instead of calculating every sample. FPGA offloading has been demonstrated for RFNoC-based channel sounding, where sequence generation and parallel correlation were moved into the USRP FPGA to exploit wide bandwidth and reduce host processing [2]. Similar work uses RFNoC to accelerate

physical-layer operations while retaining software-level control [3]. This development can be viewed as a movement of selected SDR functions from the central computer back toward the radio front end, more precisely into the digital baseband immediately adjacent to it.

RF Network-on-Chip (RFNoC) provides a framework for this partitioning. It represents FPGA modules as processing nodes with standardized control and streaming interfaces, while the network-on-chip fabric handles routing, flow control, and packet transport [4]. A software application constructs and configures a graph that may include both custom and standard blocks. This reduces the integration effort compared with modifying a monolithic FPGA design and allows a custom block to be reused in different image cores.

Frequency-modulated continuous-wave (FMCW) radar is a suitable application for local waveform generation. A linear chirp is completely described by starting frequency, slope, duration, amplitude, repetition mode, and phase policy. The standard RFNoC SigGen block produces constant, sinusoidal, and noise waveforms, but it does not provide a parametrically controlled linear frequency sweep. Replay-based generation avoids continuous host streaming but requires waveform storage and loading. Earlier studies have implemented FMCW radars with GNU Radio and USRP devices [5]–[8], and FPGA-resident direct digital synthesis (DDS) generation has also been demonstrated [9]. However, the reviewed standard RFNoC block set does not provide a reusable FMCW source that can be connected directly to the X310 digital upconverter (DUC) and radio.

This paper addresses that gap by presenting an out-of-tree RFNoC FMCW generator for the USRP X310. Its contributions are: (1) an FPGA-resident parametric generator supporting CW, up-chirp, down-chirp, and triangular modes; (2) explicit control of repetition and phase continuity; (3) correct RFNoC packet formation and operation under downstream backpressure; (4) integration with USRP Hardware Driver (UHD) host control, the DUC, and the Radio block without host waveform streaming; and (5) a verified, reproducible path from source code through simulation and X310 FPGA-image generation to hardware execution. The remainder of the paper presents related implementations, the signal model, the proposed architecture, and the verification results.

1 Related Work

Early SDR FMCW systems emphasized rapid implementation in GNU Radio and offline processing. Prabaswara, Munir, and Suksmono used GNU Radio for a weather-surveillance FMCW radar [5]. Aulia, Suksmono, and Munir subsequently considered stationary and moving targets with a triangular linear-frequency-modulated waveform and MATLAB processing [6]. Mathumo, Swart, and Focke developed a GNU Radio and Python toolkit around a USRP B210 and reported that phase drift could appear as an undesired Doppler shift, motivating real-time phase equalization [7]. More recent work by Doly et al. demonstrated a flexible real-time FMCW system with sawtooth and triangular waveforms and adaptive waveform optimization [8]. These implementations establish the flexibility of host software but also expose synchronization, phase stability, and continuous-streaming considerations.

Two publications are especially close to the present hardware partition. Singh, Bhoi, and Khilar implemented a short-range FMCW transmitter in the FPGA of a USB-connected USRP to avoid consuming the limited interface bandwidth with transmit samples [9]. Their DDS/CORDIC (coordinate rotation digital computer) realization operated at 2.4 GHz with a 15 MHz sweep and detected a target at 20 m. Stasiak and Samczynski presented an FMCW radar on a USRP X310 with FPGA real-time processing and PC offline processing, validated in laboratory and outdoor measurements [10]. These works show that FPGA-resident FMCW processing is feasible. The distinction of the present work is its implementation as a reusable RFNoC source with a UHD controller, standardized graph integration, multiple sweep modes, explicit stream semantics, and a documented X310 out-of-tree build and verification process.

Other studies identify practical issues that will affect the complete radar built around the generator. Butt et al. measured transmitter-to-receiver leakage and crosstalk in USRP-based FMCW configurations and showed their effect on target dynamic range [11]. This result motivates the separation between the waveform-generation contribution evaluated here and future receiver calibration, leakage suppression, and range-Doppler processing [12].

2 FMCW Signal Model

For a complex discrete-time generator with sampling frequency F_s, the output is

$$x[n] = A\, e^{j\phi[n]}. \tag{1}$$

where A is the normalized amplitude and $\phi[n]$ is the accumulated phase. The phase is updated by

$$\phi[n+1] = \left(\phi[n] + \frac{2\pi f[n]}{F_s}\right) \bmod 2\pi. \tag{2}$$

For an up-chirp of N samples, the instantaneous frequency is

$$f[n] = f_0 + n\Delta f, 0 \le n < N. \tag{3}$$

where f_0 is the starting baseband frequency and Δf is the frequency increment per sample. For a sweep bandwidth B and chirp duration $T = N/F_s$,

$$\Delta f = \frac{B}{N-1}, k = \frac{B}{T}. \tag{4}$$

where k is the continuous-time chirp slope. A down-chirp applies a negative increment. Triangle mode alternates the increment sign at the sweep endpoints.

The hardware uses a $\boldsymbol{P}$-bit phase accumulator. Frequency and slope are represented by signed tuning words

$$W_f = \text{round}\left(\frac{f_0}{F_s} \cdot 2^P\right), W_k = \text{round}\left(\frac{\Delta f}{F_s} \cdot 2^P\right). \tag{5}$$

The implemented value is $P = 48$, giving fine baseband frequency resolution while the 24 most significant phase bits drive the DDS sine/cosine lookup implementation. Repeated sawtooth chirps reset the frequency word at the boundary. The phase accumulator remains continuous by default, avoiding an unnecessary phase discontinuity. An optional reset flag is available when a deterministic initial phase is required.

3 Proposed RFNoC FMCW Generator

The architecture is shown in Fig. 1. The custom block is a source: it accepts control transactions but does not require a sample input. Its output contains complex sc16 values and is connected to a standard DUC and then to the X310 Radio block. The DUC interpolates the selected generator rate to the radio rate and may apply an additional digital frequency shift. Ethernet is therefore a control path for waveform parameters, graph configuration, enable/disable commands, and status counters; the waveform sample path remains within the device.

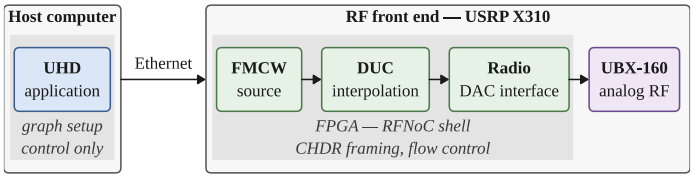


Figure 1: Signal and control architecture of the proposed RFNoC FMCW generator.

3.1 Datapath and operating modes

The core contains a 48-bit phase accumulator, a signed instantaneous-frequency word, a signed slope word, chirp and packet counters, and a DDS sine/cosine stage. The DDS output is amplitude-scaled and packed as a 32-bit complex sample. CW mode holds the frequency word constant. Up- and down-chirp modes increment or decrement it after each accepted sample. Triangle mode reverses the direction at the endpoints and holds each endpoint for the turnaround sample, keeping the sweep inside the specified interval.

The design supports repeated and one-shot operation. In repeated mode, generation continues until disabled. In one-shot mode, the enable state is cleared after the configured chirp completes. The control interface exposes enable, samples per packet, mode, amplitude, start-frequency and slope words, chirp length, repeat and phase-reset flags, and generated-sample and chirp counters.

3.2 Packetization and backpressure

RFNoC transports samples in CHDR (Condensed Hierarchical Datagram for RFNoC) packets. The packet length is fixed when the first word enters the framing stage; consequently, stopping a source in the middle of a packet can produce malformed packets or cleanup warnings. The proposed core separates waveform enable from packet draining. After a host disable command or the end of a one-shot chirp, the source

completes the current packet before becoming idle. A change in samples per packet is accepted only when the source and the DDS pipeline are fully drained.

The output uses a registered ready/valid stage. If the downstream DUC deasserts ready, sample data and the end-of-packet indication remain stable until transfer resumes. Chirp state advances only on an accepted sample. Thus, backpressure changes wall-clock delivery but cannot silently skip frequency steps or corrupt packet boundaries. For a one-shot chirp whose length is not an integer multiple of packet length, the final packet is completed with samples from the phase-continuous restart, and the status counter reports every emitted sample.

3.3 Host control and image integration

The C++ block controller converts physical parameters—sampling frequency, bandwidth, chirp duration, offset, and amplitude—into tuning words and register values. It validates finite values and hardware ranges and uses a high-low-high retry when reading the 64-bit sample counter. A command-line application discovers the FMCW block, creates the FMCW → DUC → Radio graph, configures RF frequency, gain, rates, and waveform parameters, commits the graph, and enables generation. Python bindings are also provided.

The image integration uses an RFNoC block descriptor, an image-core YAML topology, out-of-tree hardware description language (HDL) source lists, and the X310 FPGA build system. Because the complete path is version-sensitive, a reproducible recipe records the UHD FPGA tree, Vivado 2021.1 AR76780 environment, image-builder arguments, intellectual property (IP) cache location, preflight tests, implementation command, and output artifacts. Each promoted image is associated with a Git revision and SHA-256 manifest. These details are implementation support rather than a separate contribution, but they make the reported result repeatable and distinguish source revision, generated image, and image actually tested in hardware.

4 Verification and Results

Verification was performed at four levels: host software, register-transfer level (RTL) simulation, X310 synthesis/implementation, and hardware execution. The host library and applications built successfully, and two CTest cases verified the phase modulus, register addresses, and enumerated mode values. The RFNoC XSim testbench executed six scenarios covering register access and defaults, CW output, repeated up-chirp packetization, down-chirp behavior, triangular endpoints, and one-shot operation with backpressure and a non-aligned packet boundary. All six scenarios passed.

An X310 synthesis check completed with zero errors. Full X310_HG and X310_1G image builds also completed. For the versioned X310_HG implementation, all user timing constraints were met; post-route setup and hold slack were positive. The complete image used 72,112 slice LUTs (28.37%), 99,696 slice registers (19.61%), 265 block-RAM tiles (33.33%), and 119 digital signal processing (DSP) slices (7.73%) of the XC7K410T. These values describe the complete X310 image, including standard infrastructure, rather than the incremental cost of the FMCW core. The corresponding 1

Gigabit Ethernet image used 68,972 LUTs, 96,018 registers, 263 block-RAM tiles, and 119 DSP slices. Table 1 collects the verification outcomes.

Table 1: Verification results.

Level	Result
Host build and unit tests	Passed, 2/2 tests
RFNoC/XSim behavioral tests	Passed, 6/6 scenarios
X310 RTL synthesis check	Passed, 0 errors
X310_HG implementation	Completed; timing constraints met
X310_1G implementation	Completed; timing constraints met
Hardware discovery and generation	FMCW block found and generator operation confirmed on USRP X310

The FPGA image was loaded on a USRP X310 equipped with a UBX-160 daughterboard. The custom block was discovered through UHD, the graph was configured, and the generator produced output while its sample and chirp counters advanced. This establishes end-to-end control and execution on the target platform. The latest image includes subsequent packet-drain and triangle-endpoint corrections and has passed simulation and implementation; quantitative over-the-air characterization of this revision remains the next experimental step.

The architectural transport reduction follows directly from local generation. At 160 MS/s, continuous sc16 host generation would require 5.12 Gbit/s of payload for one channel. With the proposed block, the host sends a bounded register configuration and occasional status/control transactions, so control traffic does not grow with waveform duration. This property reserves host and transport capacity for received radar data and higher-level processing. It also removes host scheduling and network delivery from the sample-generation timing path.

Conclusion

This paper presented a reusable RFNoC block for parametric FMCW waveform generation in the FPGA of a USRP X310. The design fills a functional gap between the constant, sinusoidal, and noise modes of the standard RFNoC signal generator and the linear sweeps required by FMCW radar. It supports four waveform modes, configurable amplitude and timing, continuous or reset phase, repeated or one-shot operation, correct packet draining, and stable behavior under backpressure. The host configures the signal but does not transport its samples.

Host tests, six behavioral simulations, X310 synthesis, full image implementation, timing closure, and initial operation on the target radio validate the architecture. The work also illustrates a broader SDR trend: as FPGA resources and integration frameworks develop, data-intensive and timing-critical functions increasingly move from a central host into programmable logic close to the RF interface. Future work will perform quantitative over-the-air characterization and integrate the generator with receiving, dechirping, and range-Doppler blocks to form a complete SDR-based FMCW radar.

Acknowledgments

This work was supported by the National Scientific Program Security and Defense, funded by the Ministry of Education and Science of the Republic of Bulgaria under grant agreement no. D01-74/19.05.2022.

References

1. Ivanov, I., & Aleksandrova, K. (2024). Design and implementation of software-defined Doppler radar. *Environment. Technology. Resources*, 3, 105–108. https://doi.org/10.17770/etr2024vol3.8159
2. Gokalgandhi, B., Maddala, P., & Seskar, I. (2022). Implementation of FPGA based channel sounder for large scale antenna systems using RFNoC on USRP platform. *arXiv*. https://doi.org/10.48550/arXiv.2201.04471
3. Kislal, A. O., Yilmaz, O. M., Keskin, B. B., Hokelek, I., & Gorcin, A. (2026). RFNoC-based FPGA offloading for fully programmable PHY acceleration. *arXiv*. https://doi.org/10.48550/arXiv.2605.07704
4. Braun, M., Pendlum, J., & Ettus, M. (2016). RFNoC: RF Network-on-Chip. *Proceedings of the GNU Radio Conference, 1*(1). https://pubs.gnuradio.org/index.php/grcon/article/view/3
5. Prabaswara, A., Munir, A., & Suksmono, A. B. (2011). GNU Radio based software-defined FMCW radar for weather surveillance application. In *2011 6th International Conference on Telecommunication Systems, Services, and Applications (TSSA)* (pp. 227–230). IEEE. https://doi.org/10.1109/TSSA.2011.6095440
6. Aulia, S., Suksmono, A. B., & Munir, A. (2015). Stationary and moving targets detection on FMCW radar using GNU Radio-based software defined radio. In *2015 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)* (pp. 468–473). IEEE. https://doi.org/10.1109/ISPACS.2015.7432817
7. Mathumo, T. W., Swart, T. G., & Focke, R. W. (2017). Implementation of a GNU Radio and Python FMCW radar toolkit. In *2017 IEEE AFRICON* (pp. 585–590). IEEE. https://doi.org/10.1109/AFRCON.2017.8095547
8. Doly, S. A., Gubash, G., Heino, M., Chiriyath, A., & Bliss, D. W. (2024). Real-time FMCW radar system for waveform optimization using SDRs. *Proceedings of the GNU Radio Conference, 9*(1). https://pubs.gnuradio.org/index.php/grcon/article/view/149
9. Singh, M., Bhoi, S. K., & Khilar, P. M. (2018). Short-range frequency-modulated continuous wave radar using Universal Software-Defined Radio Peripheral. In P. K. Sa, M. N. Sahoo, M. Murugappan, Y. Wu, & B. Majhi (Eds.), *Progress in intelligent computing techniques: Theory, practice, and applications* (pp. 559–565). Springer. https://doi.org/10.1007/978-981-10-3376-6_60

10. Stasiak, K., & Samczynski, P. (2017). FMCW radar implemented in SDR architecture using a USRP device. In *2017 Signal Processing Symposium (SPSympo)* (pp. 1–5). IEEE. https://doi.org/10.1109/SPS.2017.8053654
11. Butt, F. A., Ritchie, M., Griffiths, H., Li, W., & Naqvi, I. H. (2021). Crosstalk in modern software defined radio for the implementation of frequency modulated continuous wave radar. *IET Radar, Sonar & Navigation, 15*(12), 1607–1621. https://doi.org/10.1049/rsn2.12150
12. Iliev, M., Bedzheva, M., Boyanov, P., Bedzhev, B., & Tsankov, T. (2019). Application of number theoretic transformations for signal processing in radar sensors. In *2019 29th Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEEIE)* (pp. 1–5). IEEE. https://doi.org/10.1109/EAEEIE46886.2019.9000451

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

A SIMO 1×2 SOFTWARE-DEFINED RADIO MODEM WITH MAXIMUM-RATIO COMBINING: DESIGN AND EXPERIMENTAL EVALUATION

Ivan P. Ivanov

Defence Institute "Professor Tsvetan Lazarov", Sofia, Bulgaria, i.p.ivanov@di.mod.bg

Abstract: *A single-input multiple-output (SIMO) packet QPSK software-defined radio modem with one transmit path and two coherent receive paths is presented. Preamble-based channel estimates drive symbol-domain maximum-ratio combining before packet validation. An executed benchmark and an indoor over-the-air implementation show consistent reliability improvement over either receive branch.*

Keywords: *software-defined radio, SIMO, receive diversity, maximum-ratio combining, QPSK, bit-error rate*

Introduction

The contemporary national security system [1] rests on its communication and information systems (CIS), and within CIS radio communication is the part that admits movement: an element that leaves the fixed network stays in the system only as long as a radio link reaches it. Crisis management tests this first: the actors are scattered, the situation shifts, and there is no time to lay infrastructure. The link studied here is the exposed one: a single-antenna terminal on the move, transmitting through a fading channel to a vehicle or a post with room for two. The moving end cannot be changed; the receiving end can observe the same transmission twice and combine.

Receive diversity improves reliability by observing the same transmitted waveform through more than one propagation branch. Selection combining keeps one observation, equal-gain combining (EGC) assigns fixed or equal-magnitude weights, and maximum-ratio combining (MRC) rotates and weights every branch according to its channel quality. The foundational linear-combining treatment [2] and fading-channel analysis [3] show that MRC maximizes post-combining signal-to-noise ratio (SNR) for known branch coefficients and noise powers. The matched-filter, fading-diversity and multiple-antenna foundations are given in [4], the wideband model in [5], the implementation-oriented digital signal processing (DSP) chain in [6], and the software-defined radio (SDR) system-design and model-based implementation context in [7]. A single-input multiple-output (SIMO) 1×2 link still carries one symbol stream: the gain is reliability, not rate. The combiner works against the multipath channel, for which the digital transmission methods were studied directly [8] and the effect of multipath and fading on a class of mobile cellular systems was analysed [9]. Combining need not sit at the receiver at all — pre-RAKE processing moves it into the transmitter, at the price of requiring the channel to be known there [10] — but the terminal-side placement is the one evaluated here.

Implementation-oriented SDR work covers separate parts of this receiver chain. A single-channel π/4 differential quadrature phase-shift keying (π/4-DQPSK) modem was modeled, simulated and implemented on SDR [11], while a later two-branch implementation introduced receive diversity using EGC with fixed coefficients $c_1=c_2=0.5$ [12]. Official GNU Radio material provides a single-stream quadrature phase-shift keying (QPSK) chain and packet-framing components [13], and a full GNU Radio 4.0 packet modem provides QPSK with root-raised-cosine shaping but retains one complex receive input and no diversity combiner [14]. A public E310 project evaluates MRC offline on recorded frequency-modulation (FM) branches [15], whereas standard-specific cellular SDR software implements real-time MRC within a New Radio (NR) multiple-antenna receiver [16]. No ready-to-run generic QPSK packet modem was identified that combines two coherent live receive streams online and reports same-frame branch and combined packet-validity and bit-error controls; this bounded survey does not establish global absence.

This paper closes that gap. The contribution is not a new combining law but the reproducible design, simulation and indoor over-the-air (OTA) evaluation of symbol-domain MRC on two coherent receive channels, with the two individual branches retained as controls.

1 Receive-combining theory

For one transmit antenna and two receive antennas, the standard complex-baseband diversity model [2], [4], [5] gives the sample at branch i as

$$y_i(k)=h_i(k)x(k)+w_i(k), \qquad i\in\{0,1\}, \tag{1}$$

where $x(k)$ is the transmitted symbol, $h_i(k)$ is the complex channel coefficient, and $w_i(k)$ is zero-mean complex noise. The same linear-combining model [2], [5] forms

$$z(k)=\sum_{i=0}^{1} c_i(k)y_i(k). \tag{2}$$

For independent branch noise with variance σ_i^2, the MRC coefficient is proportional to the conjugated channel divided by its noise variance [2], [3], [5]:

$$c_i(k)=\frac{\hat{h}_i^*(k)}{\sigma_i^2}. \tag{3}$$

With equal branch-noise variance, the normalized MRC decision variable [3], [5] used in the modem becomes

$$\hat{x}(k)=\frac{\hat{h}_0^*(k)y_0(k)+\hat{h}_1^*(k)y_1(k)}{\left|\hat{h}_0(k)\right|^2+\left|\hat{h}_1(k)\right|^2}. \tag{4}$$

Here, $(\cdot)^*$ denotes complex conjugation, $\hat{h}_i$ is the channel estimate for branch i, and σ_i^2 is its noise variance. The numerator co-phases the useful components and the

denominator restores their amplitude. Under perfect channel knowledge, the instantaneous output SNR is additive [2], [3]:

$$\gamma_{MRC}=\gamma_0+\gamma_1. \tag{5}$$

For coherent Gray-coded QPSK in independent flat Rayleigh fading, let $\mu=\sqrt{\bar{\gamma}/(1+\bar{\gamma})}$, where $\bar{\gamma}$ is the mean bit-energy-to-noise ratio per branch. The exact single-branch and two-branch average bit-error probabilities are [3]:

$$P_{b,1}=\frac{1}{2}(1-\mu), \qquad P_{b,2}=\frac{1}{4}(2-3\mu+\mu^3). \tag{6}$$

The high-SNR slope changes from first to second order. The result assumes independent branches, equal average power and perfect channel state information; antenna correlation, branch imbalance, residual carrier offset and channel-estimation error reduce the gain. It is a simulation reference, not a claim that the indoor channel realizes diversity order two.

2 System model and architecture

A software-defined radio has two constructive parts: a computing device, which runs the whole signal processing as a program, and a radio-frequency (RF) front end, which converts between analogue and digital and moves the signal in frequency [7]. Figure 1 places the SIMO 1×2 modem across that boundary. The transmitter uses one computing device and one RF transmit chain. The receiver has a doubled front end: both receive chains of the same transceiver share the receive local oscillator, the device clock and one timed stream, which makes them coherent within one Universal Software Radio Peripheral (USRP) B210 device [17]. Its computing device stays single and takes both sample streams, so alignment, estimation and combining are one program over two synchronous streams.

Figure 2 presents the functional chain. The transmitter creates a deterministic packet, appends a cyclic redundancy check (CRC-32), maps Gray-coded QPSK symbols and applies root-raised-cosine (RRC) pulse shaping. Each receive branch performs RF down-conversion, matched filtering, frame detection, timing recovery and carrier-frequency-offset correction. The known preamble provides one complex channel estimate per branch and packet. MRC is applied to aligned symbols before the QPSK slicer, payload comparison and CRC decision. The uncombined receive channel 0 (RX0) and receive channel 1 (RX1) paths pass through the same decision and validation stages, so they are proper controls.

For a known preamble $p(k)$ of length N_p, each packet uses the standard least-squares training estimate [4], [6]:

$$\hat{h}_i=\frac{\sum_{k=0}^{N_p-1} p^*(k)y_i(k)}{\sum_{k=0}^{N_p-1}|p(k)|^2}. \tag{7}$$

In (7), $p^*(k)$ is the conjugated known preamble symbol, N_p is the preamble length, and $\hat{h}_i$ is the resulting packet estimate for branch i.

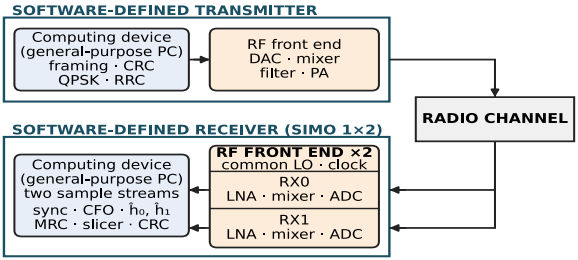


Figure 1: Constructive architecture of the modem.

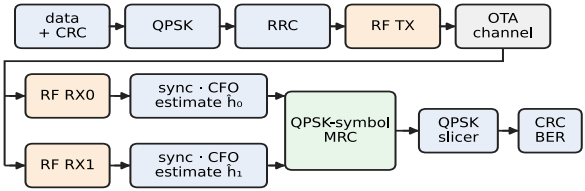


Figure 2: Functional block diagram of the modem.

Table 1 gives the parameters of the implemented waveform and live experiment. The 4096 payload bits include a deterministic pseudorandom test field and the physical-layer CRC, which makes both bit-error rate (BER) and packet-error rate (PER) directly observable.

Table 1: Modem and experiment parameters.

Parameter	**Value**
Topology	SIMO 1×2; one TX and two coherent RX channels
Carrier frequency	3.320 GHz
Sample / symbol rate	2 MS/s / 250 ksym/s
Samples per symbol	8
Modulation and shaping	Gray QPSK; RRC, roll-off 0.35, span 10 symbols
Preamble	128 QPSK symbols
Payload and validation	4096 bits per frame; pseudorandom binary sequence (PRBS) test field; physical-layer CRC-32
Frame length	2176 symbols; 17,488 complex samples

Parameter	**Value**
Combining point	Symbol domain, after synchronization and branch estimation
Radio path	Indoor OTA; internal clock and time source

3 Simulation

The companion Jupyter notebook implements Gray QPSK, additive white Gaussian noise, independent unit-power flat Rayleigh coefficients and perfect channel knowledge. For every E_b/N_0 point it processes 1,000,000 payload bits with a fixed seed and compares the Monte Carlo points with the expressions in Section 1. Figure 3 is generated by the executed notebook.

At 10 dB per branch the executed notebook gives BER=2.34×10^{-2} for one branch and 1.61×10^{-3} after MRC, a 14.5-fold reduction; the corresponding analytical values are 2.33×10^{-2} and 1.6×10^{-3}. At 12 dB the simulated pair is 1.53×10^{-2} and 7.07×10^{-4}. Agreement with the analytical curve checks the combiner and demonstrates the expected change of BER slope. The simulation is a controlled ideal case and does not reuse the measured OTA samples.

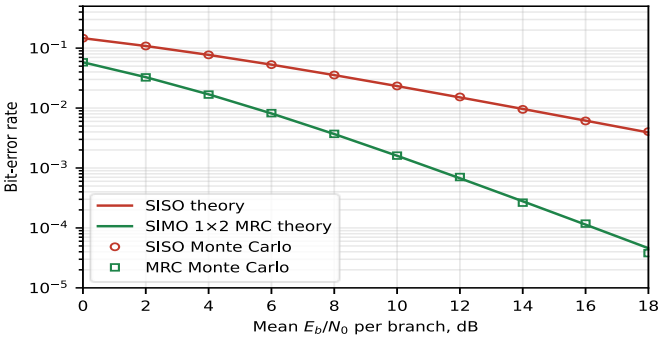


Figure 3: Simulated bit-error rate in flat Rayleigh fading.

4 Practical implementation

The practical demonstrator in Figure 4 consists of two B210-class SDR units and a host computer. The transmitter occupies one RF chain; the receiver connects two antennas to its two coherent receive inputs.

The receiver was implemented as an online stream: detection, estimation, branch decoding, MRC decoding and logging ran while samples arrived.



Figure 4: Practical SDR demonstrator.

The principal 692-frame run did not retain raw in-phase/quadrature samples; its logged live events and aggregate file are therefore the final evidence for that run, not material for later re-decoding.

5 Experimental results and evaluation

Table 2 reports one uninterrupted indoor OTA execution. All three paths evaluated the same 692 detected packet instances; the receiver logged zero stream overflows and zero dropped batches. The error-vector magnitude (EVM) column holds medians over packets.

Table 2: Same-frame branch and MRC results.

Path	CRC valid	Payload errors / bits	BER	EVM
RX0	187 (27.0%)	2090 / 2,834,432	7.37×10^{-4}	29.8%
RX1	684 (98.8%)	8 / 2,834,432	2.82×10^{-6}	20.9%
SIMO MRC	692 (100%)	0 / 2,834,432	0 observed	18.9%

Relative to the better branch RX1, MRC lowers the median EVM, converts eight additional packets into CRC-valid deliveries and leaves no payload bit error observed. The zero-error cell is not interpreted as a true BER of exactly zero: with N=2,834,432 observed payload bits and zero errors, the one-sided 95% binomial upper bound is $-\ln(0.05)/N=1.06\times10^{-6}$, which is what the finite observation interval supports.

A separate 449-frame OTA execution supplies a stronger test against the explanation "MRC merely selected the better antenna". In that run MRC produced 448 CRC-valid frames, compared with 423 on the better branch. Direct evaluation of the same-frame CRC flags found 15 packets for which both RX0 and RX1 failed but MRC succeeded. Those packets require information from both observations and therefore demonstrate actual combining rather than selection.

The practical result remains bounded to this implementation, these two coherent inputs and the recorded indoor channel realizations. It does not estimate diversity order from an independent fading ensemble, prove performance with correlated or distributed receivers, or establish a receiver-sensitivity curve; an attenuator sweep and repeated spatial realizations are the next experiments for those claims.

Conclusion

An SDR packet modem with one transmit path and two coherent receive paths has been evaluated. Channel-aware symbol-domain MRC improves error rate, constellation quality and successful packet delivery relative to either individual branch. The simulation agrees with the analytical fading-channel benchmark, while live validation shows packets recovered only through joint use of both observations. The implementation therefore advances the earlier fixed-EGC receiver to a reproducible MRC chain with strict bit and packet checks. The result is a measured reliability gain for the tested indoor coherent receiver; it does not imply higher spatial data rate or universal diversity order.

Acknowledgments

This work was supported by the National Scientific Program Security and Defense, funded by the Ministry of Education and Science of the Republic of Bulgaria under grant agreement no. D01-74/19.05.2022.

References

1. Ivanov, V., & Manchev, A. (2022). Possibilities for improving the national security system [in Bulgarian]. Eleventh International Scientific Conference HEMUS 2022, Plovdiv, VI-114–VI-124. ISSN 1312-2916.
2. Brennan, D. G. (1959). Linear diversity combining techniques. Proceedings of the IRE, 47(6), 1075–1102. doi:10.1109/JRPROC.1959.287136
3. Simon, M. K., & Alouini, M.-S. (2005). Digital Communication over Fading Channels (2nd ed.). Wiley.
4. Sklar, B., & Harris, F. J. (2021). Digital Communications: Fundamentals and Applications (3rd ed.). Pearson Education.
5. Schulze, H., & Lüders, C. (2005). Theory and Applications of OFDM and CDMA: Wideband Wireless Communications. Wiley.
6. Schwarzinger, A. O. (2021). Digital Signal Processing in Modern Communication Systems (2nd ed.). Author.
7. Ivanov, I. P. (2025). Software-Defined Radio Communication Systems [in Bulgarian]. Defence Institute, Sofia. ISBN 978-619-90024-8-3.
8. Angelov, M. (1998). Digital methods for information transmission in multipath radio channels [in Bulgarian]. Scientific Works of Vasil Levski Higher Military School, 67, 77–84.
9. Suslekov, E. T., & Angelov, M. S. (2000). Influence of multipath and fading on the performance of mobile systems with code-division multiple access and time-division duplex reception on a single frequency [in Bulgarian]. National Conference with International Participation TELECOM 2000, 11–13 October 2000.
10. Angelov, M. (1999). Study of the noise immunity of pre-RAKE diversity reception for a class of mobile cellular systems [in Bulgarian]. National Conference with International Participation TELECOM'98, Vol. I, 631–637.
11. Ivanov, I. (2023). Modeling, Simulation and Implementation of pi/4-DQPSK Modem on SDR. Proc. XXXII International Scientific Conference Electronics (ET 2023), IEEE, 1–5. doi:10.1109/ET59121.2023.10278732

12. Ivanov, I., & Angelov, M. (2024). Design and Implementation of Software-Defined pi/4-DQPSK Modem with Receive Antenna Diversity. Environment. Technology. Resources, 3, 101–104. doi:10.17770/etr2024vol3.8108
13. GNU Radio Project. (2026). QPSK Mod and Demod; Packet Communications. GNU Radio Wiki. https://wiki.gnuradio.org/index.php?title=QPSK_Mod_and_Demod; https://wiki.gnuradio.org/index.php/Packet_Communications (accessed 28 August 2026).
14. Estévez, D. (2024). gr4-packet-modem: A packet-based modem for GNU Radio 4.0. GitHub repository, commit 4d5c27d. https://github.com/daniestevez/gr4-packet-modem (accessed 28 August 2026).
15. Diamantides, K. (2018). Diversity Techniques for Riverside Wireless Sensor Nodes over Software Defined Radios. GitHub repository, commit 4f1cbc6. https://github.com/themightykay/18WSD030-Advanced-Project (accessed 28 August 2026).
16. Saaifan, K. A., et al. (2021). NR MIMO Feature Implementation into OpenAirInterface. 25th International ITG Workshop on Smart Antennas, 1–6.
17. Ettus Research. (2026). UHD and USRP Manual: USRP B2x0 Series.

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**, Faculty of Artillery, Air Defense and Communication and Information Systems

INVESTIGATION OF THE TECHNOLOGICAL PROCESS IN TRANSFORMING PET WASTE INTO FDM FILAMENT

Martin G. Dimitrov

National Military University "Vasil Levski", Faculty of Artillery, Air Defense and CIS, Shumen, Bulgaria, dimitrovm938@gmail.com

***Abstract**: This paper presents an experimental study on the process of transforming PET waste into a functional filament for FDM 3D printing. The primary focus is placed on the geometric deformation of a flat plastic strip with a rectangular cross-section into a solid filament with a circular cross-section and a diameter of 1.75 mm. Critical process parameters are analyzed, including cutting geometry, drying, extrusion temperature regimes, pulling speed, controlled air cooling, and diameter tolerance measurement. The impact of material moisture content and subsequent drying on the quality of the final 3D printed parts is evaluated.*

Keywords: PET recycling, FDM filament, thermoforming, extrusion parameters, filament drying, 3D printing

ИЗСЛЕДВАНЕ НА ТЕХНОЛОГИЧНИЯ ПРОЦЕС ПРИ ТРАНСФОРМАЦИЯ НА PET ОТПАДЪЦИ ВЪВ FDM ФИЛАМЕНТ

Мартин Г. Димитров

Национален Военен Университет „Васил Левски“, Факултет „Артилерия, ПВО и КИС“, Шумен, България, dimitrovm938@gmail.com

***Абстракт:** Настоящият доклад представя експериментално изследване на процес за трансформиране на PET отпадъци във функционална нишка за FDM 3D принтиране. Акцентът е поставен върху геометричната деформация на плоска пластмасова лента с правоъгълно напречно сечение до плътна нишка с кръгло сечение и диаметър 1.75 mm. Анализирани са критичните параметри на процеса, включващи геометрия на рязане, сушене, температурни режими при екструзия, скорост на изтегляне, контролирано въздушно охлаждане и измерване на толеранса в диаметъра. Оценено е влиянието на влажността на материала и последващото сушене върху качеството на крайните 3D отпечатани детайли.*

***Ключови думи:** рециклиране на PET, FDM филамент, термоформоване, параметри на екструзия, сушене на филамент, 3D принтиране*

Въведение

Пластмасовите отпадъци от полиетилентерефталат (PET), основно от бутилки за еднократна употреба, представляват един от най-значимите глобални екологични проблеми, но същевременно притежават висок потенциал за повторна употреба [1]. В последните години развитието на адитивните производствени технологии и по-специално моделирането чрез разтопено отлагане (FDM) разкрива нови възможности за локално затваряне на цикъла на рециклиране [2].

В предходно изследване на автора бе представена концепцията, хардуерният дизайн и електромеханичната конструкция на системата Compact PET Filament Machine [3]. Изработването на устройството обаче представлява само първия етап от внедряването на технологията. Постигането на повторяеми резултати и качествен краен продукт изисква прецизно дефинирана методика за работа и задълбочено разбиране на физико-механичните и термодинамичните трансформации, протичащи в материала [4].

Настоящият доклад има за цел да разгледа и експериментално да изследва пълния технологичен процес по преработката на PET отпадъци - от подготовката на бутилката, през пластичната деформация от правоъгълно към кръгло сечение, до финалното сушене и 3D принтирането на функционални детайли.

1. Подготовка и механика на изрязване (Лента с правоъгълно сечение)

Технологичният цикъл започва с превръщането на полутвърдата триизмерна бутилка в непрекъсната двуизмерна лента с правоъгълно напречно сечение (На фигура 1 е показана снимка на подготвена PET бутилка и инструмента за рязане (PET Bottle Cutter), показваща процеса на изтегляне на лентата.

Предварителна обработка на суровината е от съществено значение за чистотата и качеството на получения филамент [5].

- Процесът на подготовка включва:

1) Почистване и обезмасляване: Задължително отстраняване на външните етикети, лепилни остатъци и мастни замърсявания, които при термичната обработка могат да предизвикат нагари и запушване на дюзата [6].

2) Първично подсушаване: Отстраняване на повърхностната влага от бутилката преди рязане.



Фигура 1: Изрязване на лента с правоъгълно сечение от PET бутилка.

Не всички PET бутилки са еднакво подходящи за производство на филамент. В зависимост от производствената технология (степен на раздуване), дебелината на стената варира значително [5]. Прозрачните бутилки (без оцветители) притежават

най-висока термична стабилност. Цветните бутилки съдържат пигменти, които при повторно стопяване при 260˚C могат да променят вискозитета на стопилката [6]. Наличието на остатъци от лепила на хартиени/пластмасови етикети е критично. При температура 260˚C в дюзата, лепилото карбонизира (въглеродни сажди), което води до микрозапушвания и неравномерно налягане при екструзия [5, 6]. Дъното и гърлото на бутилката съдържат значително по-дебел и неравномерен слой пластмаса. Затова бутилката се отрязва прецизно в цилиндричната си част.

Основният механизъм при рязането е получаването на лента с постоянна ширина $\boldsymbol{W}$. Тъй като дебелината на стената на бутилката $\boldsymbol{t}$ варира (обикновено в границите 0.25 – 0.35 mm в зависимост от производителя), ширината на лентата трябва да бъде прецизно калибрирана [7].

За постигане на стандартен филамент с диаметър Ø1.75, се използва принципът за запазване на обема на материала. Ширината на лентата $\boldsymbol{W}$ се определя от зависимостта:

$$W = \frac{\pi . d^2}{4 . t} \qquad [mm] \tag{1}$$

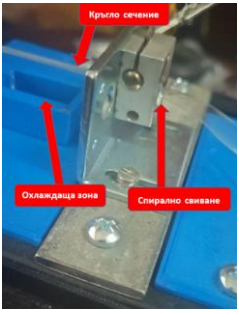
Където:

- $\boldsymbol{d}$ = 1.75 [mm] - желаният краен диаметър;
- $\boldsymbol{t}$ - средна дебелина на стената на бутилката.

При стандартна дебелина $\boldsymbol{t}$ = 0.30 [mm] необходимата ширина на лентата е приблизително $\boldsymbol{W}$ ~ 8.00 [mm]. В инструмента за рязане тази ширина се регулира чрез дистанционни подложки (шайби) под острието [3].

2. Технологичен процес на екструзия

След получаването на лентата с правоъгълно напречно сечение следва критичният етап от технологичната верига - непрекъснатото преобразуване в хомогенна нишка с кръгло сечение.



Фигура 2: Зона на екструзия и контролирано охлаждане на системата Compact PET Filament Machine.

За разлика от индустриалните екструдери, които разтопяват гранулат чрез шнек (screw extrusion), системата Compact PET Filament Machine използва метода на затвореното спирално свиване [3, 4].

Когато лентата навлезе в коничната зона на нагревателния блок, оформена от дюзата, високата температура омекотява полимера, преминавайки над температурата му на стъкловане ~ 67-81 ˚C и наближавайки точката на топене ~ 250-260 ˚C [6, 7].

Под действието на надлъжната сила на изтегляне $\boldsymbol{F_{pull}}$, упражнявана от мотора с редуктор JGY-370 [3], крайните ръбове на лентата започват да се подвиват навътре.

Лентата се навива на спирала (подобно на тръбичка), след което в най-тесния участък на дюзата 1.75 mm въздушното пространство в центъра се свива напълно. Материалът се монолитизира под действието на повърхностното напрежение и термичното налягане, образувайки плътна нишка с кръгло сечение.

Регулирането на температурата в нагревателния се извършва чрез термостатичен контролер със сензор тип K (термодвойка) [3]. Оптималният температурен прозорец за PET е тесен (~ 255-265˚C).

При $\boldsymbol{T}$ < 250˚C: Вискозитетът на PET е твърде висок. Нараства съпротивлението при изтегляне, което води до претоварване на мотора JGY-370, приплъзване на зъбните колела или скъсване на лентата [4].

При $\boldsymbol{T}$ > 265˚C: Започва термична деградация на полимера. Загубва се вискозитетът (материалът „тече"), появяват се мехурчета от термична разпадност и филаментът губи якостните си свойства [5, 6].

Непосредствено след излизане от дюзата, горещият филамент преминава през охлаждащия модул с вентилатор 4020 [3]. Бързото охлаждане е критично, за да се замрази цилиндричната геометрия на нишката преди тя да достигне ролката за навиване. Ако охлаждането е недостатъчно, нишката се сплесква под действието на опъна върху ролката.

За осигуряване на стабилен 3D печат е необходимо измерване на толеранса на готовия филамент. Измерванията се извършват с дигитален шублер през интервали от 1 $\boldsymbol{m}$ по дължината на ролката.

Таблица 1:Експериментални данни при калибрация на диаметъра на филамента

Опит №	Температура [°C]	Скорост [m/min]	Измерен Ø [mm]	Отклонение [mm]	Оценка на геометрията
1.	245	0.8	1.83	+ 0.08	Недостатъчно свиване
2.	255	1.2	1.69	- 0.06	Прекомерно разтегляне
3.	260	0.8	1.74	- 0.01	Оптимално кръгло
4.	270	0.8	1.68	- 0.07	Наличие на микрошупли

3. Управление на влажността и подготвителен етап за печат

Полиетилентерефталатът (PET) е силно хигроскопичен полимер. Молекулите му абсорбират влага от околната среда, което представлява един от основните проблеми при повторната му преработка [5, 8].

Когато влажен PET филамент навлезе в екструдера на 3D принтера при температура (~ 250 - 260˚C) водата в структурата му мигновено кипи и се превръща в пара под високо налягане. Това води до два основни проблема:

1) Деструкция на полимерните вериги (Хидролиза): Водните молекули разкъсват естерните връзки на полимера, намалявайки молекулното му тегло и механичната якост на крайния детайл [8].

2) Дефекти при печат: Изпаряването на водата предизвиква характерно „пукане" в дюзата, екструзия на мехурчета, микрошупли в нишката и лошо залепване между слоевете (poor layer adhesion) [7, 8].

За неутрализиране на влагата е разработена и приложена двуетапна методика:

Етап 1: Сушене на суровината (предварително): Почистените бутилки се подсушават преди нарязване. Наличието на капки вода по повърхността пречи на равномерното рязане и вкарва влага в нагревателя.

Етап 2: Вторично сушене на готовия ролен филамент (критичен етап): След като филаментът е екструдиран и навит на макарата, той задължително се подлага на термично сушене в дехидратор / сушилня за филамент [8].

Параметри на сушене:

- Температура: ~ 60 - 65˚C (под температурата на стъкловане за да се избегне залепване на съседните витки на ролката).
- Време за престой: 3 - 5 часа
- Съхранение: Навитата ролка се прехвърля незабавно в херметичен плик с индикаторен силикагел.

Заключение

В настоящия доклад е разработена и експериментално потвърдена цялостна преработка на PET отпадъци до нишка за FDM 3D печат чрез системата Compact PET Filament Machine [3]. Изследването обхваща пълния технологичен цикъл - от рязане на бутилките на ленти, през термоформоването им до нишка с кръгло сечение, до контрола на влажността и крайния печат.

Установено е, че правилното съотношение между дебелината на бутилката и ширината на лентата е критично за постигане на стандартен диаметър от 1.75 *mm*. Поддържането на температурен режим от ~ 255-265˚C в комбинация с контролирано въздушно охлаждане осигурява геометрична стабилност на нишката с минимални отклонения от ± 0.03 *mm*.

Експериментите потвърдиха, че задължителното сушене на готовия филамент при ~ 60 - 65˚C предотвратява хидролитичната деградация и гарантира висока междуслойна адхезия при отпечатване.

Разработената методика доказва, че малките модулни системи за рециклиране могат да превръщат битовите пластични отпадъци в ценна суровина за бързо прототипиране и инженерни приложения. Постигнатите резултати разкриват реален потенциал за внедряване на концепцията в образователния и научноизследователския процес на НВУ „Васил Левски".

Литература

1. World Economic Forum. The New Plastics Economy: Rethinking the future of plastics, 2016. https://www.weforum.org/publications/the-new-plastics-economy-rethinking-the-future-of-plastics/[Accessed September 1, 2026]

2. Singh, N., Hui, D., Singh, R., Ahuja, I. P. S., Feo, L., & Fraternali, F. Recycling of plastic solid waste: A state of art review and future applications. Composites Part B: Engineering, 115, 409–422, 2017. https://www.sciencedirect.com/science/article/abs/pii/S1359836816318601[Accessed September 1, 2026]
3. Димитров, М. Г. Система за преработка на PET отпадъци с приложение във FDM технологиите. Сборник доклади от международна научна конференция, НВУ „Васил Левски", Шумен, 2025.
(Вътрешен академичен доклад / Доклад от конференция на НВУ)
4. Al-Salman, H., et al. Conversion of Waste PET Bottles into 3D Printing Filament: A Sustainable Approach. Journal of Sustainability & Additive Manufacturing, 2025. https://jneonatalsurg.com/index.php/jns/article/view/7253[Accessed September 2, 2026]
5. Awaja, F., & Pavel, D. Recycling of PET: Methods and products. Polymer Degradation and Stability, 87(3), 471–485, 2005. https://www.sci-hub.st/10.1016/j.polymdegradstab.2004.09.012[Accessed September 1, 2026]
6. Microbial and Chemical Recycling of Poly(ethylene terephthalate). PMC PubMed Central, 2022 / RSC Advances, 2024. https://pmc.ncbi.nlm.nih.gov/articles/PMC8945055/[Accessed Sept. 2, 2026]
7. Aktepe, et al. / ResearchGate Publications. Recycling PET Waste into Functional 3D Printing Material: Effect of Processing Temperatures. ResearchGate, 2023–2025. https://www.researchgate.net/publication/391130007_Recycling_PET_Waste_into_Functional_3D_Printing_Material_Effect_of_Printing_Temperature_on_Physio-mechanical_Properties_of_PET_Parts[Accessed September 2, 2026]
8. European Environment Agency (EEA). Plastic waste and recycling trends in Europe, EEA Report, 2022. https://www.google.com/search?q=https://www.eea.europa.eu/publications/plastic-waste-and-recycling[Accessed September 2, 2026]
9. Лазаров, Р., и Б. Банков, 3D технологии и проектиране на сложни елементи от въоръжението, Сборник доклади от Научна конференция „Актуални проблеми на сигурността", Велико Търново 2019, с. 112-116, ISSN 2367-7465
10. Ганев, В., Р. Лазаров и Б. Банков. Approach for determining the ballistic characteristics of the ammunition. В: Proceedings of International Scientific Conference "Defense Technologies" DefTech 2023. Шумен: НВУ „Васил Левски", 2023. ISSN 2815-4282.

METROLOGICAL SUPPORT FOR WEAPON SYSTEMS FOR DETERMINING THEIR TECHNICAL CONDITION

Vanko V. Ganev[1], Yana D. Dimitrova[2], Petya N. Stefanova[3]

Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria,
vvganev@gmail.com[1], dimitrovax2yana@gmail.com2, petqstefanova0202@abv.bg

***Abstract**: The operation of weapon systems is directly linked to diagnostic and metrological procedures aimed at assessing their technical characteristics throughout their lifecycle. The metrology unit is tasked with providing information on the actual values of the equipment parameters and enabling a comparative analysis of characteristics for compliance with the established limit values specified in the documentation.*

***Keywords:** metrological assurance, weapon systems, technical characteristics, the operational readiness coefficient*

МЕТРОЛОГИЧНО ОСИГУРЯВАНЕ НА ОРЪЖЕЙНИТЕ СИСТЕМИ ЗА ОПРЕДЕЛЯНЕ НА ТЕХНИЧЕСКОТО ИМ СЪСТОЯНИЕ

Ванко В. Ганев, Яна Д. Димитрова, Петя Стефанова

Въведение

Експлоатацията на оръжейните системи (ОС) е свързана пряко с диагностични и метрологични процедури имащи за цел да оценят техническите им характеристики за един жизнен цикъл.

Метрологичните изисквания към експлоатацията на оръжейните системи се дефинират в две направления:

- метрологично осигуряване на качествените характеристики на системите;
- метрологично осигуряване на средствата за измерване (СрИ).

Към първото направление се отнасят пултовата апаратурата и измервателните средства монтирани в ОС, методите и средствата за експертиза,; оценките за точност, грешките от измерване, достоверността на резултатите и надеждностните характеристики на оръжейната система.

Второто направление осигурява проследимостта, точността и достоверността на измерванията и осигуреността с метрологична информация.

Същност на изследването

Оценката на качествените характеристики на ОС се основава на техническото състояние определено от три решения: "системата е годна за бойно използване", "допуска се до работа условно" и "не се допуска до работа или негодна за бойно използване". Обосноваността на тези решения се определя от достоверността на информацията, получена от метрологичните процедури и експертизи.

Метрологичното звено има за задача да предоставя информация за действителните стойности на параметрите на ОС и да даде възможност да се направи сравнителен анализ на характеристиките за съответствие с установените гранични стойности по документация. Прилагането на такъв подход налага да се формулира решаващото правило за резултатите от измерванията W^*. На тази основа се съпоставят допустимите стойности $[W_Д, W_Г]$ и се оценяват характеристиките за достоверност на контрола във вид на заключение за годност и дефектност. В практиката се извършва обобщаване на получените резултати от метрологичните експертизи за всички ОС от един вид, както и резултатите от диагностиката. Получените статистически оценки за всички извадки се сравняват спрямо съответните характеристики на ОС в интервала $(\Delta_Д,\ \Delta_Г)$.

Следователно върху качествените характеристики на ОС влияят следните оценки:

- недостоверност на заключенията изработени в системата за контрол на ОС определени от грешки от първи и втори род свързани с недостатъчни контролни операции и грешки в измервателната процедура следствие нестабилността на определени параметри;

- неточност във входните данни на ОС преди използването им по предназначение и не отчитане на определени качествени критерии от предходни състояния;

- грешки при диагностични и регулировъчни операции, водещи до нарастване на грешката от контрола участваща при вземане на управленски решения.

В приетите практически методики параметрите на ОС се оценяват експериментално и аналитично чрез факторно–структурния анализ. Случайната функция на състоянието $S(x_1,\dots x_i,\dots n_n)$ и нейните параметри $x_1,\dots x_i,\dots x_n$ се изследват спрямо номиналните стойности $x_{10},\dots x_{i0},\dots x_{n0}$, които се оклоняват с $\pm\Delta x_1,\dots\pm\Delta x_i,\dots\pm\Delta x_n$. Вариациите на параметрите са достатъчно малки ($\Delta x << x_o$), което не позволява да се отчитат дестабилизиращите въздействия на ОС. Причината за това са вариациите на Δx и тяхното влияние върху $S(x)$, които са непрекъснати и тяхното диференциране се извършва в ред на Тейлър, а дисперсията $D[\Delta S]$ се определя от уравнението [1]:

$$\left.\begin{aligned}\hat{\Delta S} &= \frac{1}{S_0}\sum_{i=1}^{n}\nabla_{x_i}^{=}.\Delta x_i;\\ \widehat{D}_{\Delta S} &= \frac{1}{S_0^2}\sum\nabla_{x_i}^{2}.\sigma_{x_i}^{2},\end{aligned}\right\} \tag{1}$$

където $\nabla_{x_i}^{=} = [\partial S/\partial x_i]_0$ е частна производна на функцията на състоянието на параметрите, $\Delta x_i = x_i - x_{i0}$ е отклонението на $i^{\text{тия}}$ параметър, а $\sigma_{x_i}^2$ е средно квадратичното отклонение на дисперсията. Следователно относително изменение на състоянието $\nabla S(x)$ на ОС спрямо контролируемите параметри се определя от израза:

$$\nabla\hat{S}(x)_i = \frac{1}{S_0}\left[S\left(x_i^{''}\right)_0 - S\left(x_i^{'}\right)\right], \tag{2}$$

където $S_o(x_0)$ е номиналното значение на функцията на състоянието, а $S(x_i'')$ *и* $S(x_i')$ са функции на качествените параметри на ОС при приети условия на експлоатация. Този принципен подход е верен, но не достатъчно обективен при оценка на вероятността за постигане на коефициента на оперативна готовност на ОС.

За да се получи достоверна измерителна информация за състоянието на ОС е необходимо да са изпълнят две съвместими сложни събития: наличие на СрИ (събитие А) и тяхното правилно използване (събитие Б). Събитието А ще настъпи, ако ОС е напълно окомплектована със СрИ (A_1), всички СрИ са изправни (A_2). Събитие Б ще настъпи, ако ОС и СрИ са подготвени за работа ($Б_1$), операторите имат необходимата подготовка ($Б_2$), всички измервания са извършени правилно ($Б_3$), извършва се контрол на правилността на изпълнението на метрологичните работи ($Б_4$). Събития А и Б и съответстващите им вероятности характеризират работата на метрологичното звено. Колкото вероятностите на А и Б са по-близки до единица, толкова по-добре работи метрологичното звено. Затова отчитайки зависимостта на събитията А и Б произведението $P_A.P_{А/Б} = P_M$ и $P_Б.P_{А/Б} = P_М$ може да се нарече вероятност за нормална работа на метрологичното звено. От друга страна неопределените множества $А_1$ и $А_2$, $Б_1 \div Б_4$ са съвместими и независими и могат да се представят във вида:

$$\left.\begin{array}{l} P_A = P_{A_1}.P_{A_2}, \quad P_Б = P_{Б_1/A}.P_{Б_2}.P_{Б_3/Б_1.Б_2}.P_{Б_4} \\ P_M = P_{A_2.A_2}.\ P_{Б_1/A}.P_{Б_2}.P_{Б_2/Б_1.Б_3}.P_{Б_3/Б_1.Б_2}.P_{Б_4} \end{array}\right\} \quad (3)$$

Анализът на израза (3) показва, че за постигане на необходимите стойности на P_M трябва да се изпълни комплекс от съгласувани и взаимосвързани мероприятия в системата за метрологично осигуряване (СМО).

Методите за оценка на качествените характеристики на оръжейните системи се основават на проверка на съответствието на резултатите от измерването на параметрите на ОС с установените изисквания [2, 3].

За метрологичен контрол се извършва оценка на характеристиките на ОС в зависимост от граничните параметри на работоспособност на системата чрез измерваните параметри, които се явяват случайни величини на функцията за плътността на разпределение $f(x, y)$. Установяват се допустимите отклонения $\Delta x_Д$ и $\Delta x_Г$ или допуск $d = \Delta x_Д + \Delta x_Г$ и нормите за горна и долна граница $x_Г = x_o + \Delta x_Г$, $x_Д = x_o + \Delta x_Д$, където x_o е номиналното значение на параметъра, аналогично за у. Номиналното значение на параметрите се използва за определяне на априорната вероятност за техническа годност на ОС $\rho_x = P\{x \in dx\}$ и $\rho_y = P\{y \in dy\}$.

Априорната вероятност за техническа годност на ОС като цяло се определя по формулата:

$$P_{OK} = \prod_{j=1}^{m} \rho_{xj} \quad (4)$$

където: P_{OK} е вероятната техническа годност на ОС съгласно приетата стратегия за оценка; m е количеството контролируеми независими параметри, а ρ_{xj} е

априорната вероятност за техническа годност на ОС по j -я параметър. За изследваните ОС всички параметри имат еднакъв теглови коефициент, което позволява P_{OK}, ρ_x и m да се изразят чрез $\rho_x = (P_{OK})^{\frac{1}{m}}$ [4].

За определяне на апостеорните вероятности след контрол е необходимо да се използва оценката x^* на параметрите и $\rho_x^* = P\{x^* \in dx\}$ за величината P_{OK}^*. В процесът на измерване на параметрите на ОС се допуска грешка, която е случайна и независеща от параметъра величина. Тя се дефинира чрез плътността на разпределение $f_R(\varepsilon)$ и се определя от зависимостта $x^* = x + \varepsilon$, където x^* е резултатът от измерването на параметъра, x - истинското значение на параметъра и ε - грешката от измерването. Следователно математическото очакване $M[x^*] = M[x] + M[\varepsilon]$ и средно квадратично отклонение $\sigma_{\tilde{x}} = \sqrt{\sigma_x^2 + \sigma_\varepsilon^2}$ на контролируемите параметри са съпоставими по стойност с допусковото поле. Те се проверяват по условието - принадлежи или не принадлежи на допустимата норма $\left(x^* \begin{matrix}\in \\ \notin\end{matrix} dx\right)$. Това означава, че са налице два противоположни резултата "в допуск" и "не в допуск". Резултатът от условната и безусловна вероятност на двете събития се определя по зависимостите от вида [5]:

$$\left.\begin{array}{c} P_{Г/Г} = P_1\{x^* \in dx / x \in dx\}; \\ P_{ГГ} = P_2\{x^* \in dx, x \in dx\}; \\ P_{Д/Д} = P_3\{x^* \notin dx / x \notin dx\}; \\ P_{ДД} = P_4\{x^* \notin dx, x \notin dx\}; \\ \alpha_k = n_{ГД}/N_Г = P_5\{x^* \notin dx / x \in dx\}; \\ P_{ГД} = n_{ГД}/N_o = \alpha_k \rho_x = P_6\{x^* \notin dx, x \in dx\}; \\ \beta_k = n_{ДГ}/N_Д = P_7\{x^* \in dx / x \notin dx\}; \\ P_{ДГ} = n_{ДГ}/N_o = \beta_k . q_x = P_8\{x^* \in dx, x \notin dx\}; \end{array}\right\} \quad (5)$$

където: $P_{Г/Г}$ и $P_{Д/Д}$ са условни вероятности, а $P_{ГГ}$ и $P_{ДД}$ са безусловни вероятности за правилно взето решение относно истинското положение на параметъра на ОС в границите на допусковото поле; $n_{ГД}$ и $n_{ДГ}$ са количеството годни, но признати за дефектни и количеството на дефектни но признати за годни единици ОС от партия с обем N_o; $N_Г$ и $N_Д$ са количеството годни и дефектни ОС в партия с обем N_o; α_K и β_K са условни а $P_{ГД}$ и $P_{ДГ}$ са безусловни вероятности за грешно заключение за годността на контролируемите параметри на ОС, като винаги е изпълнено равенството:

$$P_{ГГ} + P_{ДД} + P_{ГД} + P_{ДГ} = 1 \quad (6)$$

За обобщен показател приемаме априорната вероятност за вземане на правилно рашение по отделен параметър на ОС $D = 1 - P_{ГД} - P_{ДГ}$ и $D^o = 1 - P_{ГД}^o - P_{ДГ}^o$ на системата като цяло, определени от уравненията:

$$\left.\begin{array}{c} P_{ГД}^O = \prod_{j=1}^m \rho_{xj} - \prod_{j=1}^m (\rho_{xj} - P_{ГДj}) = \left[1 - \prod_{j=1}^m (1 - \alpha_{kj})\right] . \prod_{j=1}^m \rho_{xj} = \alpha_k^o . P_{ok}; \\ P_{ДГ}^o = \prod_{j=1}^m \left[\rho_{xj}(1 - \alpha_{kj}) + q_{xj}\beta_{kj}\right] - \prod_{j=1}^m \rho_{xj}(1 - \alpha_{kj}) = \beta_k^o . P_{ok} \end{array}\right\} \quad (7)$$

където: α_{kj}, β_{kj} са вероятносттите за грешка от контрола по параметри, $j = 1, \ldots, m$. За изследваните ОС главно значение има обема, точността и пълнотата на контрола на техническите параметри. Показателите, които характеризират пълнотата на контрола показват каква част от пултовата апаратура и параметрите на ОС са обхванати от избрания метод за контрол на цялостното състояние $Q' = \lambda_K/\lambda_O$, където λ_K е сумарната интензивност на отказите на ОС открити с установения метод на контрол, а λ_O е сумарната интензивност на отказите на цялата система. В [6] за показател на пълнотата на контрола е използвано отношението $Q'' = (1 - P_m)(1 - P_o)^{-1}$, определено от вероятностите за безотказна работа (P_m - по контролируемите параметри и P_o - на ОС като цяло). Приеме, че всички независими параметри са равно вероятни и основната характеристика се построява от отношението на контролируемите параметри към общия им брой.

От пълнотата на контрола зависят условните и безусловните вероятности и характеристиките на ОС като цяло. Те се чувствителни към грешката от измерването на параметрите на ОС и допусковите полета. При контрол на голяма партида от ОС те позволяват да се оцени предварително каква част от фактически годните ОС ще се приеме за негодна и каква част от негодните ОС ще се приемат за годни. Тези показатели се използват при разчет на оптималната периодичност на проверката, за планиране на проверката и определяне на показателите за достоверност на контрола. Показателите $P_{ГД}$, $P_{ДГ}$ определят допустимата грешка на СрИ.

В случая, когато измерването и контрола на параметрите на ОС и нейната самопроверка не предизвикват спиране и прекъсване на работата, а проверката се изпълнява в периода на регламентните работи на съответната ОС във всеки един фиксиран момент от времето, ОС може да се намира във всяко едно от следните състояния: S_1 - използва се по назначение, намира се в работоспособно състояние; S_2 - използва се по предназначение със скрит отказ, намира се в неработоспособно състояние; S_3 - готви се за възстановяване, намира се в неработоспособно състояние; S_4 - извършва се възстановяване на неработоспособна ОС; S_5 - извършва се проверка на работоспособна ОС; S_6 - подготовка за възстановяване, намира се в работоспособно състояние; S_7 - извършва се проверка на неработоспособна ОС; S_8 - извършва се самопроверка на неработоспособна ОС; S_9 - извършва се възстановяване на работоспособна ОС; S_{10} - извършва се самопроверка на работоспособността на ОС.

От едно състояние в друго ОС може да преминават с интензивност λ_{ij} на прехода от състояние i в състояние j, $i = 1 \ldots 10$, $j = 1 \ldots 10$.

Вероятността $P_i(t)$, $i = 1,2, \ldots, 10$, не зависи от предходните процеси, а обхваща пълна група събития на моментното състояние $\sum P_i = 1$. Това дава основание преходните състояния да се обединят в матрично диференциално уравнение от вида:

$$\dot{P}(t) = A.P(t), \tag{8}$$

където: $P(t) = |P_1(t), P_2(t), \ldots, P_{10}(t)|'$ е първата производна на състоянието на ОС $\dot{P}(t) = \left|\dot{P}_1(t), \dot{P}_2(t), \ldots, \dot{P}_{10}(t)\right|'$ по съответните параметрични характеристики на А определени в матричен вид.

Решението на (8) ни дава зависимостта между вероятностите за намиране на ОС в определено състояние от параметрите на ОС и процеса на обслужване. Следователно коефициентът за оперативна готовност $K_{OГ}$ се определя от зависимостта:

$$K_{OГ} = P_1(P_1 + P_2)^{-1}. \quad (9)$$

Conclusion

Използваният модел позволява да се дефинират две алтернативни състояния на ОС – работоспособно и неработоспособно. Те са гранични и определят междупроверочните интервали на параметричните характеристики на ОС.

References

1. Крещук В. В., Метрологическое обеспечение эксплоатации сложных изделий, Стандартов, Москва, 1989
2. Лазаров, Р. Н., Полигонни изпитвания на промяната на балистичните характеристики на боеприпаси с изменена форма на проектила при движението му във въздуха и преминаването му през среди с различна плътност. Годишник на Шуменския университет „Епископ Константин Преславски“ т. XIV Е 2024: 115-120 стр., Шумен, ISSN 2815-4703.
3. Lazarov, R. N., Research on the change in ballistic characteristics of ammunition with a modified projectile shape during its movement in an air environment, https://doi.org/10.17770/etr2024vol4.8194, Proceedings of the 14th International Scientific and Practical Conference. Rezekne, Latvia, Environment. Technology. Resources 2024 Vol. 4, p. 164-168, Online ISSN 2256-070X.
4. Мусин И. А., Планирование эксперимента при моделирований погрешности средств измерений, Стандартов, Москва, 1989.
5. Манафова О., Изразяване на неопределеността на измерване при калибриране, Стандартизация, Метрология, Сертификация,. № 2 – 3, стр. 23 – 25, 1996.
6. Медич, Дж. Методы анализ данных - Москва: Финансы и статистика, 1985.

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**, Faculty of Artillery, Air Defense and Communication and Information Systems

APPLICATION OF THE SYSTEM OF TOLERANCES AND FITS IN INDUSTRY 4.0

Rosen N. Lazarov

Department "Armament and technology for design", National Military University "Vasil Levski", Shumen, Bulgaria, poceh_69@abv.bg

Abstract: *This paper investigates the transformation of the management, specification, and analysis of geometric and dimensional tolerances and fits in the context of Industry 4.0. The transition from traditional two-dimensional (2D) drawings to Model-Based Definition (MBD) establishes a single source of data throughout the entire product lifecycle. The open neutral standards STEP AP242 and QIF 3.0 are examined as key pillars for interoperability and the exchange of semantic Product and Manufacturing Information (PMI). Particular attention is given to Computer-Aided Tolerancing (CAT) methods, simulations of non-rigid (deformable) assemblies, automated tolerance synthesis using polychromatic sets, and the statistical optimization of costs in interconnected dimensional tolerance chains.*

Keywords: *Geometric Dimensions, Industry 4.0, Model-Based Definition, Computer-Aided Tolerancing*

ПРИЛОЖЕНИЕ НА СИСТЕМАТА ЗА ДОПУСКИ И СГЛОБКИ ПРИ ИНДУСТРИЯ 4.0

Росен Н. Лазаров

Катедра „Въоръжение и технологии за проектиране", Национален военен университет „Васил Левски", Шумен, България, poceh_69@abv.bg

Анотация: *Настоящият доклад изследва трансформацията в управлението, специфицирането и анализа на геометричните и размерните допуски и сглобки в контекста на Индустрия 4.0. Преходът от традиционните двуизмерни (2D) чертежи към концепцията за моделно дефиниране (Model-Based Definition - MBD) създава единен източник на данни за целия жизнен цикъл на продукта. Разгледани са отворените неутрални стандарти STEP AP 242 и QIF 3.0 като основни стълбове за оперативна съвместимост и пренос на семантична производствена информация (PMI). Специално внимание е отделено на методите за компютърно-подпомагано определяне на допуски (Computer-Aided Tolerancing - CAT), симулациите на неригидни (деформируеми) сглобки, автоматичния синтез на допуски чрез полихроматични множества и статистическата оптимизация на разходите при взаимносвързани размерни вериги.*

Ключови думи: *Геометрични размери, Индустрия 4.0, Model-Based Definition, Computer-Aided Tolerancing*

1. Въведение.

Традиционният подход при проектирането разчита на двуизмерни (2D) чертежи за комуникация между различните звена на жизнения цикъл на продукта. В ерата на Индустрия 4.0 се налага концепцията за моделно дефиниране (Model-Based Definition - MBD), при която триизмерният (3D) CAD модел служи като единствен източник на истина (one source of the truth) за всички инженерни, производствени и метрологични дейности[1].

Основни характеристики на този преход са:

1.1.Икономически ползи: Реализирането на MBD в индустрията чрез заместване на 2D чертежите може да доведе до спестяване на ресурси[1] чрез:

- По-малко инженерни часове за създаване и поддръжка на 2D чертежи. Избягва се дублиране на работа и намаляване на риска от несъответствия.
- По-малко грешки и преработка. Преминаването от 3D към 2D чертежи и обратно, извършвано от оператор или инженер води до риск от пропуснати размери, погрешно разчитане на геометрията или работа по стара ревизия. При MBD има един цифров източник на истина.
- По-бърза подготовка на производството. CAM системите могат директно да използват геометрията и част от PMI данните за програмиране на машините, вместо инженерът да прехвърля информация ръчно.
- Автоматизация на контрола на качеството. Данните за допуски и измервания могат да се предават директно към CMM и други измервателни системи.
- По-ефективна работа с доставчици. Доставчикът получава пълния цифров модел с всички производствени изисквания, което намалява техническите въпроси, забавянията и грешките при оферириане и производство.
- По-кратък time-to-market. Когато инженерингът, производството и качественият контрол използват един и същ машинно четим модел, се съкращават множество междинни стъпки в процеса.
- По-ниски разходи за управление на конфигурации и промени. Въвеждането на промяна в основния модел води до актуализиране на производните документи.

1.2.Дигитална нишка (Digital Thread): Интегрирането на MBD с отворени стандарти като STEP AP 242, QIF и платформата MtConnect генерира непрекъсната дигитална нишка между CAD моделите, механичната обработка и измервателните инструменти. Това води до 15% по-висока ефективност при обработка, 35% съкращаване на времето за програмиране и 50% по-лесна експлоатация[1].

1.3.Семантично представяне: Информацията за геометричните допуски и отклонения (GD&T) вече не е просто графичен текст или символ, а е семантично свързана с геометричните елементи (features) по начин, позволяващ автоматично разчитане и обработка от софтуерни алгоритми[1].

2. Отворени стандарти за трансфер на данни: STEP AP 242 и QIF 3.0.

За осигуряване на съвместимост в рамките на разпределеното производство се използват отворени неутрални CAD формати[1]. Двата водещи международни стандарта в тази област са:

2.1. STEP AP 242 (ISO 10303): Разработен за авиокосмическата и автомобилната индустрия, този стандарт използва езика EXPRESS за представяне на семантични PMI данни, кинематика и теселация. Втората версия на стандарта (2020 г.) се пренасочва към XML-базирана структура на данните и подобрява интеграцията на семантичната информация[1].

2.2. QIF 3.0 (Quality Information Framework): XML-базиран отворен стандарт, който заменя остарелия DMIS стандарт от 2013 г.8. QIF е силно ориентиран към метрологията и качеството. Той съдържа геометрични данни (B-reps или полигонална мрежа), топология, метрологични характеристики, пълна GD&T информация, планове за измерване, метрологични резултати и статистика. QIF позволява пълна семантична проследимост, намаляване на ръчния труд, ограничаване на грешките при трансфер на данни и проследяване на индивидуалните детайли в производството[1].

2.3. Интеграция: Разработват се методи за транслация и обмен на данни между тези два стандарта (например чрез Knowledge Graphs и езика OWL), което позволява съвместяване на проектантските изисквания в STEP с метрологичните данни от QIF[1].

3. Компютърно-подпомагано определяне и симулация на допуски (CAT).

Интеграцията на MBD в софтуерите за компютърно-подпомагано определяне на допуски (Computer-Aided Tolerancing – CAT) позволява автоматизиране на симулациите и анализа на вариациите[1].

3.1. Анализ на неригидни (деформируеми) сглобки.

Конвенционалните CAD среди приемат хипотезата за абсолютно твърди детайли. В реалността обаче детайлите се деформират под влияние на заваряване, топлинно разширение, гравитация, статични и динамични натоварвания [2].

Съвременните CAT системи комбинират CAD моделирането с изчисления по метода на крайните елементи (FEM) и математическия апарат на Торсора на малките премествания (Small Displacements Torsor – SDT). Този подход позволява симулиране на еластичните деформации и автоматично пренастройване на заложените сглобки (mating constraints) на базата на функцията на целта на сглобката (Objective Function of the Assembly – OFA) [2].

Процесът включва:

- Реконструкция на деформираните повърхнини чрез триангулация (STL) и експорт на облаци от точки.
- Актуализиране на сглобките за контакти тип Ригиден/Неригиден (R/NR) чрез алгоритми за откриване на интерференции, проекция на точки и идентифициране на оптимални контактни върхове[2].

3.2. Автоматичен синтез на допуски чрез полихроматични множества и графи.

За да се изключи субективният фактор при специфициране на допуските, се използват напреднали математически модели:

- Теория на полихроматичните множества (Polychromatic Sets Theory – PST): PST предлага формален йерархичен модел (детайли → геометрични елементи → вариационни геометрични ограничения (VGC) → типове допуски). Чрез матрици на съответствие автоматично се определят необходимите геометрични допуски (форма, съосност, разположение) и се изгражда добре ограничена мрежа от толеранси[3].

- Подход, базиран на графи: Размерните вериги и функционалните изисквания (Functional Requirements – FR / Functional Key Characteristics – FKC) се моделират като ориентирани графи, улесняващи проследяването на натрупването на отклонения и изчисляването на сглобяемостта[4][5].

4. Определяне на допуски и сглобки при Индустрия 4.0: Сравнение между стандартните методи за твърди детайли и методите за анализ на некорави детайли (FEM).

Анализът и управлението на геометричните и размерните отклонения в условията на Индустрия 4.0 претърпяват фундаментална трансформация. Въвеждането на концепцията за Моделно дефиниране (Model-Based Definition - MBD) изисква пълна интеграция на производствената и измервателната информация (PMI) в единния 3D CAD модел на изделието. В този контекст, изчисляването на функционалните изисквания на сглобките (Functional Requirements - FR) налага прецизен избор на метод за анализ на натрупването на толеранси [1].

Традиционно софтуерните инструменти приемат хипотезата за абсолютно твърди детайли (Rigid Parts). При съвременното високоточно и автоматизирано производство обаче, симулацията на реалното поведение на детайлите налага използването на методи за анализ на некорави (деформируеми) компоненти (Non-Rigid / Compliant Parts), базирани на Метода на крайните елементи (Finite Element Method - FEM) [1] [2] [9].

4.1. Сравняване на възможностите на методите е направено в Таблица 1.

4.2. Детайлен сравнителен анализ на ключовите аспекти.

4.2.1. Фундаментални допускания за физическото състояние:

- Методи за твърди детайли: При тях се приема хипотезата, че реалните части напълно запазват своята номинална форма (равнина, цилиндър, сфера). Геометричните грешки от позициониране и ориентация се изразяват чрез математическа линеаризация (напр. Торсор на малките премествания - SDT). Формата обаче е инвариантна, което изключва възможността за отразяване на локални повърхностни огъвания или структурни изкривявания [2] [9] [10] [11].

- FEM-базирани методи за некорави детайли: Тези модели признават, че реалните компоненти са гъвкави (например тънкостенни ламарини, заварени рамки, пластмасови панели) и се деформират под въздействие на външни сили. Тук

детайлът вече не е идеален заместител, а се разделя на мрежа от крайни елементи. Това позволява симулирането на локални огъвания, усуквания и промени в коравината на детайлите в сглобката [1] [2] [9] [11].

4.2.2. Математическо представяне на отклоненията

- Твърди детайли: Отклоненията се представят чрез хомогенни матрици за трансформация (HTM), кинематични вериги или вектори на малки премествания (три транслации и три ротации). При наличие на комбинирани толеранси е трудно да се разграничи количествено приносът на всяко отделно отклонение без използване на усъвършенствани регресионни анализи[1] [6] [9] [10].

- Некорави детайли (FEM): Основният модел за представяне на вариациите е мрежата от крайни елементи (FE mesh). Отклоненията от толерансите се симулират чрез прилагане на случайни или систематични отмествания директно върху възлите на мрежата (node deviations) или чрез морфиране на номиналната геометрия на мрежата. За целта се използва концепцията за Skin Model Shape (SMS), която комбинира макроскопичните геометрични отклонения с микроскопични грапавости върху триангулирани STL повърхнини[1] [2].

Таблица 1.

№	Сравнително измерение	Стандартни методи за твърди детайли (Rigid-Body)	Методи за некорави детайли, базирани на FEM
1	Основна физическа хипотеза	Компонентите са абсолютно твърди тела (производствените отклонения променят само позицията и ориентацията им, но не и формата им) [2] [9]	Компонентите са деформируеми (некорави) еластични или еластично-пластични тела[1] [2]
2	Основни математическ и модели	Векторни контури (Vector Loop / DLM) [8] [10]: -Торсор на малките премествания (SDT) [10] -Матрични трансформации (HTM) [10] -Теория на домейните и T-Map[2] [8]	Метод на крайните елементи (FEM) [1] [2]: -Метод на коефициентите на влияние (MIC) [1] -Комбиниран Якобиан-Торсор с деформации [2]
3	Представяне на толерансите в модела	Геометричните фичъри запазват номиналната си форма и се изместват като твърди тела в рамките на толерансната зона[9] [10]	Отклоненията се дефинират като премествания на отделните възли (nodes) от мрежата на крайните елементи (FE mesh) или морфиране на мрежата[1]
4	Моделиране на контактите	Опростено (кинематични връзки); контактите са фиксирани и се описват чрез локални координатни системи и свързващи матрици (Matrix Link) [1] [10]	Нелинейно; контактните точки и площи се променят динамично в зависимост от отклоненията на входящите детайли и приложените сили[1]
5	Оценяване на монтажния	Ограничено до сглобяване в номинално състояние без	Пълна симулация на етапите на сглобяване (напр. симулация в

	процес	отчитане на монтажните усилия, гравитацията или термичното разширение [2]	затегнато състояние в приспособлението и след освобождаване за отчитане на пружинирането) [1]
6	Влияние на физическите фактори	Пренебрегва се влиянието на статични/динамични натоварвания, температура, гравитация, заваръчни деформации и сили на затягане [2]	Директно интегриране на физически натоварвания, температурни полета (термично разширение), гравитационни ефекти и остатъчни напрежения от заваряване [1] [2]
7	Изчислителна сложност	Ниска; линейните или линеаризираните уравнения се решават изключително бързо чрез Монте Карло симулации или аналитично[1] [2]	Много висока; изисква решаване на множество нелинейни FEM уравнения за всяка вариация при Монте Карло симулация[1]
8	Приложими софтуерни инструменти	CETOL 6σ, SigmundWork, MECAmaster, SolidWorks TolAnalyst [1] [7]	3DCS (FE-compliant модул), RD&T, VSA, eM-TolMate [1]

4.2.3. Моделиране на контактите и монтажния процес

- Твърди детайли: Връзките между детайлите се описват чрез фиксирани уравнения на контакт в ставите или хлабините (Joints and Gaps). Използването на твърди контакти често води до математическо преограничаване на системата (over-constrained assemblies) в CAD средите, което налага изкуствено деактивиране на връзки или предефиниране на условията по приоритет на базите[1] [9].

- Некорави детайли: Сглобяването на деформируеми елементи се моделира като многоетапен процес[1].

4.2.4. Влияние на физическите фактори на средата

- Твърди детайли: Традиционният толерансен анализ е чисто геометричен. Той не е в състояние да отрази как промяната в работната среда влияе на хлабините на сглобката [2] [9] [11].

- Некорави детайли: FEM моделите позволяват директна интеграция на термо-механични натоварвания (термично разширение и дилатация), гравитационни ефекти (особено важни при големи некорави структури), монтажни напрежения от затягане на болтове или нитове и деформации, предизвикани от заваръчно свиване [2] [8] [9].

4.2.5. Изчислителна сложност и оптимизационни подходи

- Твърди детайли: Поради линеаризирания характер на моделите (напр. метода на Якобиан-Торсор), статистическият анализ (напр. Монте Карло с 10 000 до 100 000 итерации) се извършва в рамките на няколко секунди на стандартен компютър. Това улеснява бързата оптимизация на допуските чрез алгоритми като Particle Swarm Optimization (PSO) за минимизиране на разходите[1] [5] [6].

- Некорави детайли: Извършването на директна Монте Карло симулация, включваща хиляди нелинейни FEM анализи с контактни уравнения, е изключително скъпо от изчислителна гледна точка. За решаване на този проблем се

използва Методът на коефициентите на влияние (Method of Influence Coefficients - MIC). MIC изгражда линейна матрична зависимост между входящите отклонения на детайлите и крайните отклонения на сглобката, изисквайки само няколко предварителни крайноелементни симулации, което прави статистическия анализ приложим в индустриални мащаби[1].

4.3. Практическа верификация и икономически ефект

Практически казуси показват значимостта на деформационния фактор. Например при симулация на направляваща релса за задно седло на струг, стандартният толерансен анализ (без деформации) показва, че хлабините в сглобката са напълно в допустимите граници. Когато обаче се приложи FEM анализ, отчитащ теглото на задното седло и еластичното огъване на релсата, се оказва, че хлабините падат под критичния минимум за определени конфигурации на отклоненията. Това налага затягане на критичните толеранси, което би било напълно пропуснато при стандартния анализ на твърди тела [2][8].

Внедряването на Closed-Loop PMI среди позволява измервателните данни от реално произведени детайли (във формат QIF 3.0) да се заложат обратно в софтуера за анализ на некорави детайли. По този начин Монте Карло симулациите се извършват не с теоретични разпределения, а с реалните деформационни форми на детайлите, затваряйки цикъла на качеството при Индустрия 4.0 [1][8].

MBD средите и по-конкретно стандартът QIF 3.0 позволяват затваряне на цикъла на качеството (Closed Loop PMI)[1][8]. Метрологичните данни от измервателните машини (CMM) се записват обратно в семантичния модел. Тези реални разпределения на отклоненията заменят теоретичните предположения (нормални разпределения) в CAT софтуерите, повишавайки точността на Монте Карло симулациите за оценка на брака[1] [2].7

5. Статистическа оптимизация на разходите при взаимносвързани вериги.

Едно от най-големите предизвикателства пред Индустрия 4.0 е балансирането на разходите за производство и функционалното качество на сглобките чрез оптимално разпределяне на допуските[5][6].

5.1. Взаимносвързани размерни вериги

Когато няколко размера на един детайл се обработват при едно установяване на една и съща машина (например чела на стъпаловиден вал), техните точности са технологично свързани. Модифицирането на един допуск влияе директно върху останалите вериги и променя производствената цена[5].

5.2. Оптимизационни алгоритми и икономически ефект

- Particle Swarm Optimization (PSO): Метаевристичният алгоритъм PSO се използва за минимизиране на общата функция на производствените разходи при нелинейни ограничения за допустим брак (например поддържане на ниво на качеството от 63 дефекта на милион / 4σ закон на разпределение). За определяне на математическата връзка се използват моделите разходи-допуски на Chase и Spotts[5].

- Модифициран модел на Якобиан-Торсор: Използва се за триизмерен статистически толерансен анализ. Чрез изчисляване на чувствителността на

функционалния параметър (FR) спрямо отделните детайли, софтуерът идентифицира критичните и некритичните допуски. Затягането на критичните и разхлабването на некритичните допуски подобрява сглобяемостта без увеличаване на производствената цена[6][7].

- Икономическа верификация: Прилагането на тези оптимизации в реални производствени сглобки (например коаксиалност на лагерни гнезда в редуктори или морски предавателни кутии) води до намаляване на процента на дефектните детайли и директно спестяване на около 7.63% от производствените разходи за сглобката[8].

6. Предизвикателства пред индустрията.

Въпреки очевидните предимства, пълното внедряване на системите за допуски при Индустрия 4.0 се сблъсква с:

6.1. Инерция на системата: Преходът от десетилетия утвърдени 2D практики към изцяло дигитално 3D MBD управление изисква значителни инвестиции и преобучение на инженерния състав[1].

6.2. Проблеми при транслацията на данни: Преводът на комплексни геометрични толеранси, модификатори за максимум материал (MMC) и приоритет на базите (datum precedence) в чисти математически отклонения на възлите при крайноелементните мрежи остава сложна и невинаги напълно автоматизирана задача[1].

7. Заключение.

Работата със системата за допуски и сглобки при Индустрия 4.0 извежда проектирането извън рамките на субективната преценка на конструктора. Чрез стандарти като STEP AP 242 и QIF 3.0, автоматизиран анализ с метода на крайните елементи за деформируеми детайли и математически алгоритми за статистическа оптимизация на разходите (PSO, Якобиан-Торсор), съвременните предприятия постигат драстично съкращаване на времето за подготовка на производството и минимизират загубите от брак.

References

1. Aderiania, A. R., Warmefjorda K., Soderberga R., Model-based definition in computer aided tolerance analyses, ScienceDirect, Procedia CIRP 114 (2022) 112–116 1-s2.
2. Korbia A., Tlijaa M., Louhichib B., BenAmaraa A., A CAD Model for Tolerance Analysis of non-rigid Planar partsassemblies, 28th CIRP Design Conference, May 2018, Nantes, France, *ScienceDirect Procedia CIRP 70 (2018) 126–131*
3. Yi Zhang, Zongbin Li, Lida Xu, Jikong Wang, A new method for automatic synthesis of tolerances for complex assemblies based on polychromatic sets, *Enterprise Information Systems*, DOI: 10.1080/17517575.2011.593004, Vol. 5, No. 3, August 2011, 337–358

4. Avila Rondón R. L., Pérez Rodríguez R., Cordovés García A., Avila Alfaro R.P., Mendoza Núñez Z., Seañez De Villa J. M., Estévez Parra E., Rodríguez Ramírez Y., Tolerances Modeling in Assemblies: an Approach Based on Graphs, *Advanced Materials Research* Vol 902 (2014) pp 378-384 (2014) Trans Tech Publications, doi:10.4028/www.scientific.net/AMR.902.378
5. Helinga B., Aschenbrennera A., Walterb M. S. J., Wartzacka S., On Connected Tolerances in Statistical Tolerance-Cost-Optimization of Assemblies with Interrelated Dimension Chains, 14th CIRP Conference on Computer Aided Tolerancing (CAT), *ScienceDirect*,Procedia CIRP 43 (2016) 262 – 267.
6. Hua Chen, Xin Li, Sun Jin, A statistical method of distinguishing and quantifying tolerances in assemblies, *Computers & Industrial Engineering* 156 (2021) 107259
7. Hassani A., Aifaoui N., BenAmara A., Computer aided tolerancing based on analysis and synthetizes of tolerances method, International Conference on Advances in Mechanical Engineering and Mechanics, 2008, Tunisia
8. Renzi C., Ceruti A., Leali F., Integrated geometrical and dimensional tolerances stack-up analysis for the design of mechanical assemblies: an application on marine engineering, *Computer-Aided Design and Applications*, 2018, DOI:10.1080/16864360.2018.1441229
9. Louhichi B., Tlija M., BenAmaraa A., Tahanc A., An algorithm for CAD tolerancing integration: Generation of assembly configurations according to dimensional and geometrical tolerances, Computer-Aided Design 62 (2015) 259–274
10. Serrano-Mira, J.; Rosado-Castellano, P.; Romero-Subirón, F.; Bruscas-Bellido, G.M.; Abellán-Nebot, J.V., Incorporation of form deviations into the matrix transformation method for tolerance analysis in assemblies, *ScienceDirect*, Procedia Manufacturing 41 (2019) 547–554.
11. Tlija M., Louhichi B. and BenAmara A., Evaluating the effect of tolerances on the functional requirements of assemblies, *Mechanics & Industry* 14, 191–206 (2013), DOI: 10.1051/meca/2013054

COMPUTATIONAL ANALYSIS OF SINGLE-PIECE AND SEGMENTED FRANGIBLE CORE DESIGNS FOR PROJECTILE IMPACT ON STEEL ARMOUR

Mirel Nană[1], Constantin Enache[1], Florin-Marian Dîrloman[1], Adrian-Nicolae Rotariu[1], Octavian-Gabriel Chiriac[1]

[1]Military Technical Academy "Ferdinand I" 39-49 Av. George Coșbuc, Bucharest, Romania
mirelnana01@gmail.com, constantin.enache@mta.ro, florin.dirloman@mta.ro,
adrian.rotariu@mta.ro

***Abstract**: This paper presents a computational study of a frangible projectile design and evaluates how the geometry of its tungsten core governs terminal performance against steel armour. Two core configurations are compared under identical impact conditions: a monolithic single-piece core and a segmented core assembled from five identical elements, both housed within a steel body and ogive. The analysis is carried out using ANSYS-based explicit dynamics simulations and focuses on target perforation, core fragmentation, spatial dispersion of the resulting fragments, and the evolution of projectile velocity throughout the penetration process. The numerical results show that core geometry has a decisive influence on the fragmentation response and on the post-impact dispersion pattern. Relative to the single-piece design, the segmented five-element configuration produces a higher number of fragments within a comparable dispersion area, indicating improved fragmentation efficiency. The segmented configuration also presents advantages from a manufacturing standpoint, as the identical elements can be produced and assembled with reduced tooling complexity. Overall, the study identifies the five-element segmented core as the more effective design for the proposed frangible projectile.*

***Keywords**: frangible projectile, tungsten core, segmented core design, numerical simulation, fragmentation efficiency, terminal ballistics.*

1. Introduction

The design of aircraft automatic-cannon ammunition has always been driven by the demand for a favourable compromise between terminal effect on the target, safe handling on board, and the smallest possible risk of ricochet against platforms or infrastructure. In the specific field of small-calibre air-to-air and air-to-ground engagements, the frangible projectile concept has progressively emerged as one of the most effective solutions for defeating lightly armoured targets, precisely because it combines a robust airframe with an internal core that disintegrates in a controlled manner upon impact [1, 2].

Unlike conventional armour-piercing rounds, the frangible projectile carries a dense internal core, which it is a most frequently a tungsten-based heavy alloy, that fragments after the ogive breaks against the target surface. The resulting fragment ensemble of high-density particulates produces a combined axial and radial terminal effect: incident kinetic energy is delivered on a broader footprint behind the armour, while the residual velocity of the individual particles remains sufficient to inflict damage on internal components [2, 3]. This behaviour is particularly advantageous when the target contains distributed sub-systems (fuel lines, avionics bays, hydraulic circuits) rather than a single

hardened element, since the perforation of the outer plate is only the first stage of the intended damage sequence.

Currently, frangible ammunition is available for the most widespread automatic-cannon calibres in service on modern platforms: 20 × 102 mm (M61 Vulcan), 25 × 137 mm and 27 × 145 mm, with reference rounds such as: PGU-33/U TPF-T, PEB 327 (DM103) and the SAPHEI configuration PGU-28/B. These constructive solutions rely on the same operating principle, but differ in the internal configuration of the core, in the choice of the ogive material, and in the arrangement of the fragmenting element with respect to the impact axis [1, 4]. The comparative analysis of the constructive solutions clearly shows that the geometry of the frangible element, rather than its mass alone, is the parameter that governs the fragmentation pattern and, consequently, the terminal effect.

Establishing this functional dependence experimentally is expensive and, in most cases, only partially conclusive: high-speed diagnostic methods capture the fragment ensemble only after it exits the plate, while the internal evolution of the fragmentation process cannot be resolved experimentally. The finite element method, in its explicit dynamics implementation, has therefore become the standard investigation tool for terminal ballistics studies, providing the time-resolved kinematic and damage fields that experimental testing cannot resolve directly [5-8].

The present work follows this methodological line and reports a computational study performed with ANSYS Explicit Dynamics (AUTODYN module) on a 20 × 102 mm frangible projectile. The objective of the present article is to establish, by means of explicit dynamics simulations, how the internal segmentation of the tungsten core influences the terminal effect of the round against a steel armour plate, and to identify the constructive configuration that offers the most favourable balance between penetration and fragmentation. Two configurations of the tungsten core are therefore compared under identical impact conditions on a Steel 1006 armour plate: a monolithic single-piece core and a segmented core assembled from five identical cylindrical elements. The comparison is based on four descriptors that are directly relevant for terminal effectiveness: the perforation of the armour plate, the fragmentation morphology of the tungsten core, the spatial dispersion of the resulting fragments behind the plate and the time history of the axial velocity during the penetration process.

2. Numerical model

The numerical investigation is carried out with ANSYS 16.2, using the Workbench environment and, more specifically, the Explicit Dynamics/AUTODYN module dedicated to high strain-rate phenomena. This solver is well suited for the coupled problem of ogive collapse, core fragmentation and plate perforation, since it allows the simultaneous use of Lagrangian meshes for structured components and Smoothed Particle Hydrodynamics (SPH) discretization for the parts that undergo severe distortion and material separation [5, 6]. The simulation is set up as a two-dimensional axisymmetric problem: the axis of revolution coincides with the projectile axis, which is aligned with the plate normal at the moment of impact. The 2D axisymmetric formulation preserves the essential physics of a normal-incidence impact while considerably reducing the computational cost when compared with a full 3D model of

equivalent mesh density, and it remains the standard choice for the preliminary phase of a frangible projectile design [7].

2.1 Materials and constitutive models

Three materials are involved in the simulation: a shock-resistant tool steel (Steel S-7) for the projectile body and ogive, a low-carbon steel (Steel 1006) for the armour plate, and a tungsten heavy alloy for the frangible core, with reference densities of 7.75, 7.89 and 19.22 g/cm³ respectively (see Table 1). Steel S-7 was retained for the body and ogive because its high impact toughness and shock resistance closely reproduce the mechanical response of the alloys typically used in production frangible rounds, while Steel 1006, a low-carbon ferritic grade, was chosen as a reference armour material representative of thin protective panels found on light armoured targets and structural components of tactical aircraft [4].

The tungsten heavy alloy is a standard choice for the frangible element because its high density concentrates the kinetic energy of the projectile on a small volume, and its brittle failure mode under high strain rates favours the formation of a dense fragment ensemble rather than a monolithic residual penetrator.

Table 1. Materials and reference densities assigned in the AUTODYN model

Component	Material	Reference density (g/cm³)	Discretization
Projectile body	Steel S-7	7.75	Lagrange
Ogive	Steel S-7	7.75	Lagrange
Frangible core	Tungsten heavy alloy	19.22	SPH
Target plate	Steel 1006	7.89	Lagrange

The mechanical response of each material is captured through the built-in constitutive models available in the AUTODYN material library. A Johnson-Cook strength model combined with a linear equation of state was used for the two steels, so that the pressure-dependent flow stress and the thermal softening are consistently accounted for in the impact regime. The tungsten heavy alloy is described with the corresponding Johnson-Cook parameters together with an equivalent tensile-stress failure criterion, which triggers material separation and the formation of discrete fragments as the effective plastic strain approaches its critical value [6-8]. A geometric strain-based erosion criterion is imposed on every deformable body, with the erosion strain threshold set to 1.1. Erosion is a numerical technique that removes elements once they exceed a prescribed distortion, thereby preventing the well-known mesh entanglement and time-step collapse that would otherwise halt the simulation as soon as the ogive begins to plastically deform upon the plate. The erosion threshold was chosen to be moderately high, so that the removed elements do not artificially deplete the kinetic energy of the impactor before the fragmentation process is fully developed. Its value is consistent with the range reported in recent studies on high-velocity impact of small-calibre projectiles against thin steel plates [7, 9].

2.2 Geometry and constructive configuration

The projectile geometry retains the general external profile of a 20 × 102 mm round, with a cylindrical steel body, a pointed steel ogive and a coaxial tungsten core housed inside the body cavity. The projectile body is defined in three sub-parts: main cylindrical section, base and an auxiliary transition part connecting the cylinder to the base, which are then merged into a single deformable body through the AUTODYN "Joins" option (see Figure 1).

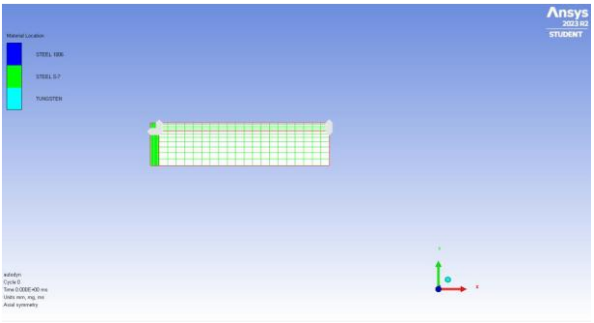


Figure 1. Projectile body assembled from three sub-parts (cylindrical section, base and transition element) merged through the AUTODYN "Joins" option

This subdivision is a purely numerical device: it allows a uniform structured mesh to be applied to each sub-part while preserving the mechanical continuity of the assembled body. The ogive is generated with the dedicated "Ogive" primitive available in the Parts menu (see Figure 2), using the geometric parameters obtained from the constructive design phase of the projectile.

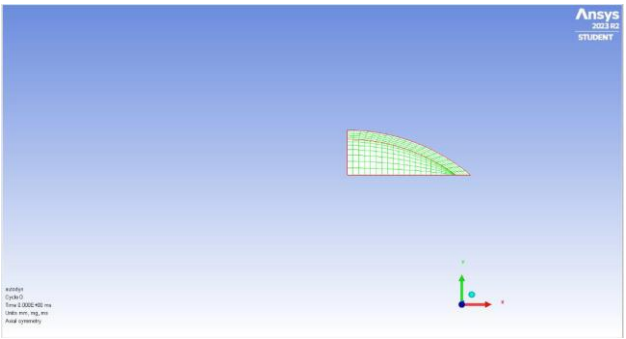


Figure 2. Steel ogive generated with the dedicated AUTODYN "Ogive" primitive and meshed with a structured Lagrangian grid

The armour plate is generated as a separate Lagrangian part (see Figure 3) and its boundary is fully restrained through the Boundary/velocity condition available in the pre-processor, as detailed in Section 2.4.

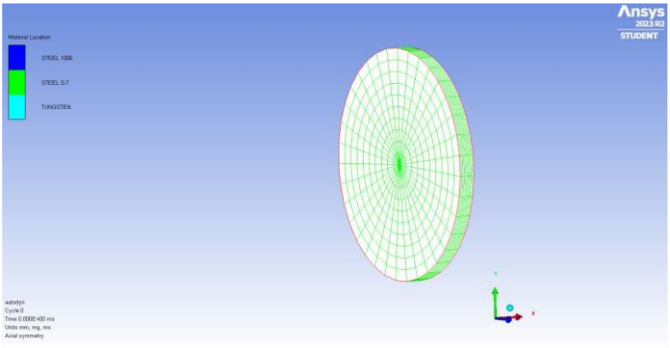


Figure 3. Steel 1006 armour plate discretized with a Lagrangian mesh, coloured according to the material legend (dark blue)

Two configurations of the frangible core are examined in this work. In configuration I, the core is a single tungsten cylinder whose length and diameter fill the internal cavity of the projectile body (see Figure 4), which represents the reference, closest to the constructive solution found in the majority of frangible ammunition currently in service. In configuration II, five identical cylindrical tungsten segments are stacked coaxially inside the same cavity (see Figure 5), so that the total mass of tungsten and the external envelope of the core are preserved. The segments are simply joined in contact, without a bonding layer, so that the interfaces between them act as pre-existing separation surfaces during impact.

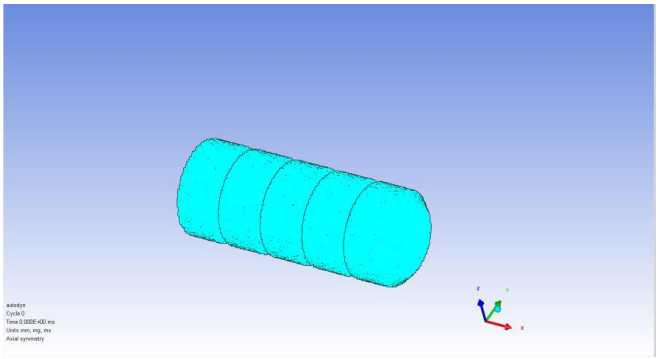


Figure 4. Configuration I - monolithic tungsten core discretized with SPH particles

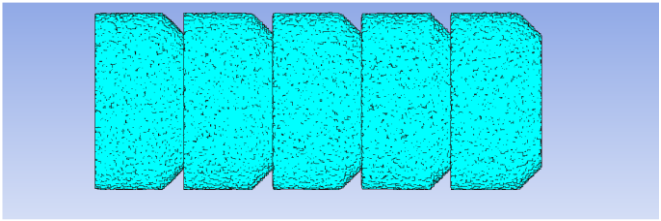


Figure 5. Configuration II - segmented tungsten core assembled from five identical SPH segments

Both configurations share the same body geometry, the same ogive, the same total core mass and the same overall length. The comparison is therefore driven exclusively by the internal architecture of the frangible element, which is the design parameter under investigation.

2.3 Discretization and interactions

A hybrid Lagrange/SPH discretization is used throughout the model. The projectile body, the ogive and the armour plate are meshed with a structured Lagrangian grid, which offers a clean representation of the shock wave propagation in the steel components and accurately resolves the geometric definition of the ogive tip during the initial phase of the impact. The tungsten frangible core, in either of its two configurations, is discretized through Smoothed Particle Hydrodynamics. The SPH formulation, being mesh-free, is not affected by the element distortion issues that would otherwise impact the fragmentation stage, and it naturally accommodates the progressive separation of the tungsten material into discrete fragments as the failure criterion is met [6, 10].

The generation of the SPH domain for the frangible core is defined iteratively by prescribing the coordinates of a set of boundary reference points that match the real dimensions of the core cavity. For the segmented configuration, five sets of coordinates are generated so that each tungsten segment is represented by an individual SPH sub-domain in direct contact with its adjacent segments. The contact between the projectile body and the ogive, both Lagrangian, is imposed through the Lagrange/Lagrange interaction. The interaction between the SPH particles of the frangible core and the surrounding Lagrangian parts is enforced automatically by the solver through the integrated SPH/Lagrange coupling. Prior running the simulation, the geometrical integrity of the assembly is verified through the Interaction/Lagrange/Lagrange consistency check offered by the pre-processor, in order to eliminate the residual gaps or interpenetrations that would otherwise introduce spurious contact events at the very first cycles of the analysis.

2.4 Initial and boundary conditions

The impact scenario is representative of the operational conditions of the projectile. The projectile is assigned an initial translational velocity of 760 m/s along the axis of symmetry, corresponding to the residual velocity of the round after 400 m of flight from the muzzle of the automatic cannon, as obtained from the external ballistics computation performed in the design phase. The armour plate is fully restrained: a null velocity

condition is imposed on the plate boundary, which reproduces the effect of a rigid mounting frame and isolates the perforation problem from the plate's rigid-body response. The complete initial configurations used for the two configurations are depicted in Figures 6 and 7.

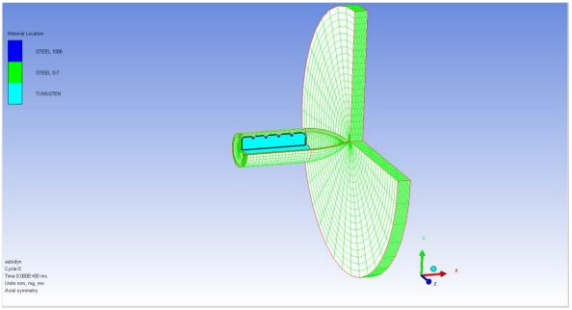


Figure 6. Initial configuration of the impact simulation - configuration I (monolithic tungsten core)

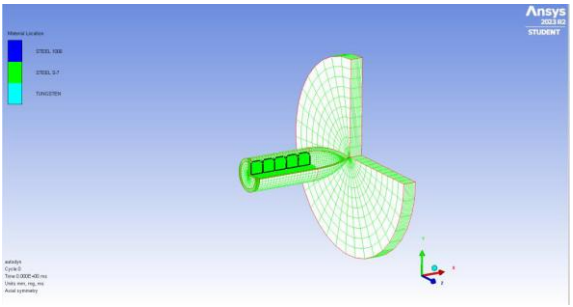


Figure 7. Initial configuration of the impact simulation - configuration II (segmented five-element tungsten core)

A parametric study of the plate thickness in the range 10 - 30 mm was carried out during the design phase in order to identify a target that is representative for the class of light armoured targets addressed by the projectile. The comparison of the two frangible core configurations is reported here for a 15 mm Steel 1006 plate, which corresponds to the intermediate value of the range and, at the impact velocity considered, produces a clearly resolved perforation in both configurations. This choice ensures that the differences observed between the two configurations are attributable to the internal architecture of the core rather than to the terminal effect being either quenched (over-armoured target) or trivially amplified (under-armoured target).

The simulation is controlled by prescribing the Start Cycle, End Cycle and Increment parameters in the Output section of the solver, together with the Cycle Limit, Time Limit and Energy Limit values in the Controls section. The simulation end conditions are set so

that the analysis covers the whole penetration process, from the first contact of the ogive with the plate to the free-flight phase of the fragment ensemble on the rear side of the plate

3. Results and discussion

The two constructive configurations of the frangible core are compared through a set of qualitative and quantitative descriptors extracted from the simulations: sequence of images describing the initial, intermediate and final phases of the penetration event; number of fragments and their spatial dispersion pattern behind the plate; and the time history of the residual axial velocity of the leading part of the projectile. The residual velocity is a particularly informative descriptor because, for a given impact velocity and a given target, it summarizes in a single scalar the overall energy dissipation during the penetration process, since the amount of kinetic energy consumed in plastic deformation, fragmentation and heating of the plate is equal to the difference between the impact and the residual kinetic energies of the projectile.

3.1 Configuration I - monolithic tungsten core

The evolution of the impact event for the reference configuration follows the classical sequence associated with kinetic-energy penetrators against a moderately thick steel plate. The steel ogive is the first component to interact with the target: it deforms plastically, loses its pointed profile within the first tens of microseconds, and progressively transfers the incident load to the underlying tungsten core (see Figure 8). Projectile steel body begins to peel radially outward, as expected from a slender projectile impacting a rigid target, while the tungsten core advances axially into the penetration cavity in the plate.

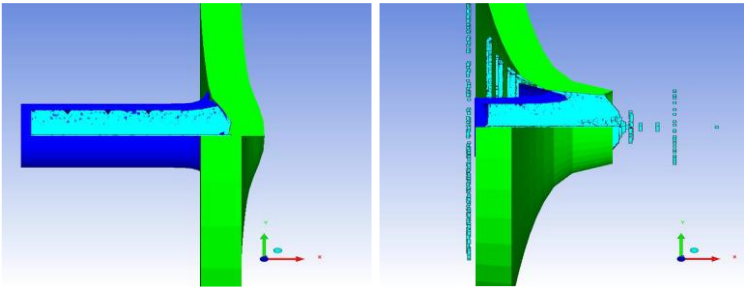


Figure 8. Penetration phase for the monolithic core: axial engagement of the tungsten cylinder with the Steel 1006 plate and progressive plastic deformation of the steel ogive and body

Once the tungsten cylinder is engaged in the plate, the fragmentation process starts from the leading face of the core, where the axial compressive stress reaches the highest value, and propagates rearwards along the axis of the cylinder. The failure surfaces develop essentially by shear localization at the periphery of the core and by tensile fracture on its axis, in agreement with the fragmentation mechanism reported for tungsten heavy alloys at the strain rates typical of this impact regime [9, 10]. As a consequence,

the number of fragments generated by the monolithic core increases progressively during the penetration, but at any given time the front of the fragment cloud is dominated by a small number of relatively large, plate-like fragments issued from the leading face of the cylinder.

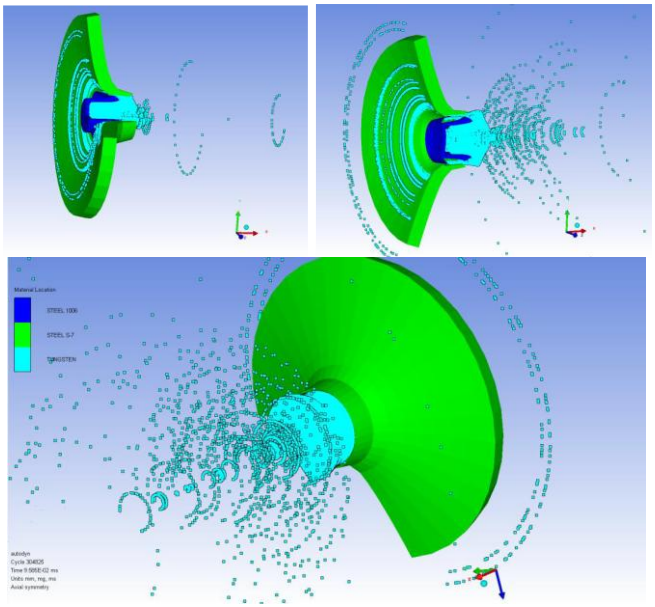


Figure 9. Final fragment distribution behind the plate for configuration I - dispersion pattern issued from the monolithic tungsten core after perforation of the 15 mm Steel 1006 plate

The fragment distribution behind the plate is axially elongated and radially narrow (see Figure 9). The lateral dispersion, however, is generated primarily by the expulsion of large sub-fragments from the leading face and by the peel-off of the outer material of the cylinder. The overall pattern is therefore concentrated on a limited number of comparatively massive fragments, which is characteristic of the terminal effect of a monolithic penetrator and is broadly consistent with the observations reported for equivalent tungsten cores in the literature [3, 10]. The axial velocity time history of the leading fragment shows a monotonically decreasing profile, with the highest slope corresponding to the phase in which the tungsten core is fully engaged in the plate, followed by an almost constant residual velocity once the plate has been perforated (see Figure 10). The pronounced slope on the interval 0.05-0.07 ms corresponds to the phase in which the tungsten cylinder is fully engaged in the Steel 1006 plate.

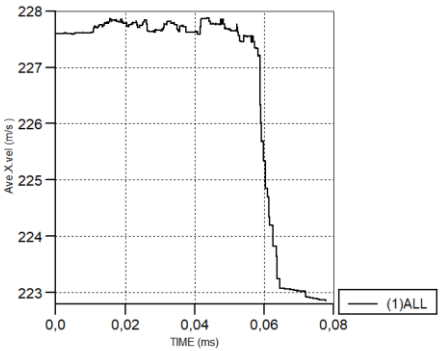


Figure 10. Time history of the residual axial velocity of the leading fragment for configuration I

3.2 Configuration II - segmented five-element tungsten core

The response of the segmented core is qualitatively different from the very first stages of the impact. The leading tungsten segment is loaded axially in the same way as the monolithic core, but instead of transmitting a compressive stress wave through a continuous cylinder, the axial loading is redistributed at each internal interface between adjacent segments (see Figure 11). Because these interfaces act as pre-existing surfaces of separation, they release the compressive wave much more efficiently and generate an early transverse dispersion of the segments as soon as the plate offers a lateral confinement to the leading element.

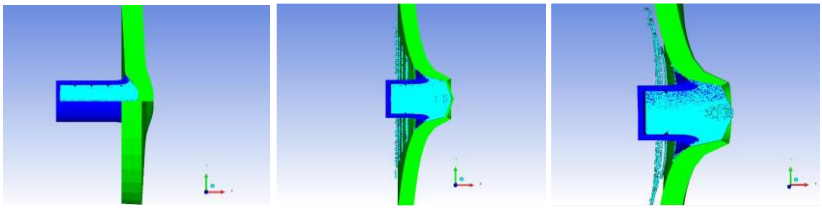


Figure 11. Penetration phase for the segmented five-element core: parallel engagement of the individual tungsten segments and immediate redistribution of the axial loading at the internal interfaces

Even in the early stages of the perforation process, the fragment ensemble generated by the segmented core exhibits a smaller radial extent than the one obtained for the monolithic core at an equivalent penetration depth (see Figure 12). This behaviour is a direct consequence of the redistribution of the axial load at the segment interfaces, which prevents the outer material of the tungsten cylinder from being ejected radially with the high velocity that characterises the monolithic case. Compared with the monolithic core at the same instant, the fragments issued from the segmented core are contained on a smaller radius around the impact axis.

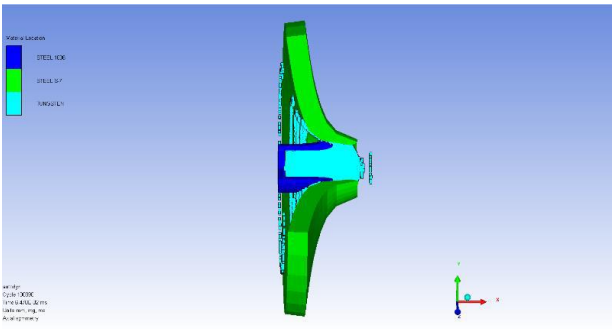


Figure 12. Initial stage of the fragment dispersion for configuration II

As the penetration continues, the fragmentation process proceeds simultaneously on multiple leading faces, one for each segment that is progressively engaged with the plate, rather than only on the front face of a single cylinder. This parallel fragmentation is the key mechanism responsible for the increased number of fragments observed in the final configuration. The intermediate stage of the perforation event (see Figure 13) shows the multiplication of the fragment population as successive segments cross the plate: each segment contributes an individual fragment cloud whose morphology is representative of a much shorter penetrator, and the resulting fragments are smaller, more numerous, and axially more compact than in the monolithic case.

The final phase of the simulation confirms these observations. At the end of the perforation event, the dispersion pattern behind the plate (see Figure 14) is denser than for the monolithic core and, at the same time, exhibits a smaller lateral extent, i.e. the fragments are concentrated on a smaller radius around the axis of impact.

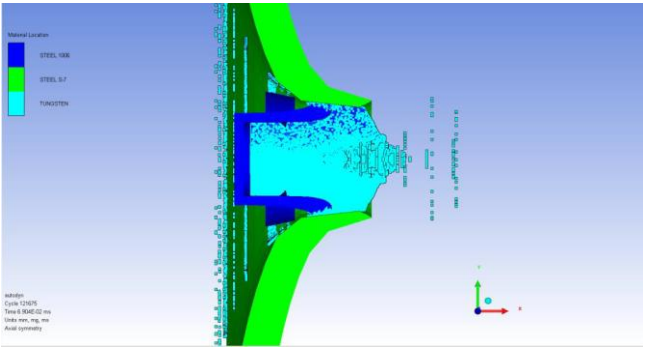


Figure 13. Intermediate stage of the perforation event for configuration II

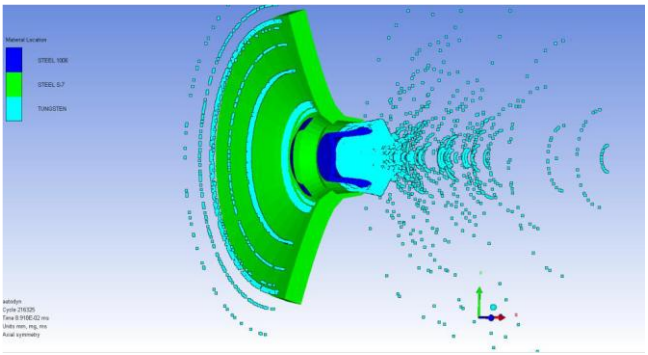


Figure 14. Final fragment dispersion behind the plate for configuration II

This behaviour is highly favourable from the point of view of the terminal effect: a higher number of fragments delivered on a smaller surface increases the probability of encountering a critical sub-system of the target, which is exactly the design intent of a frangible projectile. The residual velocity of the leading fragment (see Figure 15) is comparable with the one obtained for the monolithic core, indicating that the improvement of the fragmentation pattern is not achieved at the expense of penetration capability. Compared with Figure 9, the fragments are more numerous, of smaller individual size, and concentrated on a smaller radius around the axis of impact. The velocity drop follows the same time window as in Figure 10, confirming that the penetration capability is preserved by the segmentation of the core.

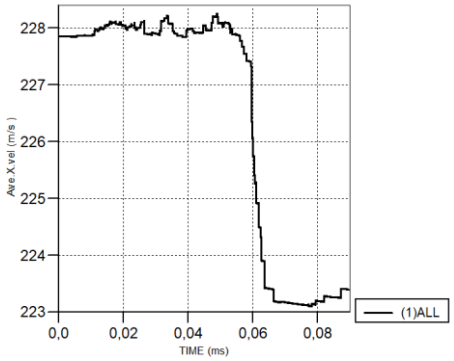


Figure 15. Time history of the residual axial velocity of the leading fragment for configuration II

3.3 Comparative analysis

The side-by-side comparison of the two configurations, summarized qualitatively in Table 2, brings out three main observations that are relevant for the design of the

projectile. First, the perforation capability of the round is not modified by the segmentation of the core. Both configurations perforate a 15 mm Steel 1006 plate at 760 m/s and both leave the plate with a residual velocity that is comparable in magnitude. In other words, the two configurations belong to the same class from the point of view of penetration performance, which was one of the constraints imposed on the design.

Second, the segmentation of the core produces a measurable improvement of the fragmentation pattern. The higher number of fragments generated by the segmented configuration, combined with the smaller lateral dispersion, results in a higher fragment density on the dispersion area behind the plate. Under the standard assumptions used in terminal ballistics analyses, uniformly distributed critical points on the target volume, this translates directly into a higher probability of engaging a critical sub-system per impact, which is the operational figure of merit for a frangible round. The parallel fragmentation of the five segments also delivers a more compact fragment dispersion in the axial direction, which reduces the "time-of-arrival" distribution of the individual fragments on the target and further concentrates their damage effect.

Third, the constructive simplification associated with the segmented configuration should not be underestimated. Five identical tungsten cylinders can be produced by turning on a single set of tools and inspected using a single measurement protocol, whereas a monolithic tungsten cylinder of the same total length imposes tighter machining tolerances along its full length and does not allow the manufacturer to compensate for local defects by selecting the best elements from a production batch. From an industrialization point of view, the segmented configuration is therefore also the more attractive solution.

Table 2. Qualitative comparison of the two configurations studied

Descriptor	**Configuration I Monolithic core**	**Configuration II Segmented (5 elements)**
Perforation of the 15 mm Steel 1006 plate	Achieved	Achieved
Number of fragments behind the plate	Lower	Higher
Radial dispersion of the fragment cloud	Larger	Smaller (more concentrated)
Axial spread of the fragment cloud	Elongated	Compact
Fragment density on the dispersion area	Lower	Higher
Residual velocity of the leading fragment	Reference	Comparable
Constructive/manufacturing complexity	Higher (single machined block)	Lower (identical, repeatable elements)

It should be mentioned that the present analysis is based on a two-dimensional axisymmetric model with an idealized normal-incidence impact and does not include the effect of angular incidence, projectile yaw, plate spacing or multi-layered targets. These aspects are known to modify quantitatively the fragmentation pattern and will be

addressed in the next stage of the study. Nevertheless, the trend identified here, a favourable influence of the internal segmentation of the core on the fragmentation efficiency, is expected to be preserved in more general impact configurations, since it originates from a mechanism that is intrinsic to the segmented architecture of the core.

4. Conclusions and perspectives

A computational investigation of the terminal effect of a 20 × 102 mm frangible projectile against a Steel 1006 armour plate has been carried out with ANSYS Explicit Dynamics, using a hybrid Lagrange/SPH discretization strategy. The tungsten frangible core, integrated in a steel body with a steel ogive, was considered in two constructive configurations: a monolithic single-piece core and a segmented core assembled from five identical cylindrical elements, and both were tested at an impact velocity of 760 m/s on a 15 mm plate.

Both configurations achieve full perforation of the plate and exhibit a comparable residual velocity of the leading fragment, i.e. the segmentation of the core does not degrade the penetration capability of the projectile. The internal fragmentation mechanism, however, is markedly different. The monolithic core fragments essentially through the propagation of failure surfaces starting from its leading face, and produces a fragment distribution dominated by a small number of relatively large sub-fragments spread over a wide radial and axial envelope. The segmented core fragments in parallel on multiple leading faces, one per segment, as soon as each element is engaged with the plate, and produces a denser, more compact fragment cloud on a smaller dispersion area. From the point of view of the terminal effect, the higher fragment density on the same dispersion area increases the probability of engaging critical sub-systems of the target, which is the intended design objective of a frangible round. In addition, the segmented configuration offers clear advantages from a manufacturing standpoint, since the identical elements can be produced with reduced tooling complexity and inspected on a common protocol.

On the basis of these results, the five-element segmented core is identified as the more effective solution for the proposed frangible projectile. The perspectives of the work include the extension of the numerical model to a full three-dimensional configuration, in order to capture the effect of angular incidence and projectile yaw; the analysis of the sensitivity of the fragmentation pattern to the number and to the length ratio of the segments; the introduction of realistic aircraft-representative target arrangements (spaced, multi-layered, sub-system-populated); and, most importantly, the experimental validation of the numerical predictions by means of high-velocity impact tests instrumented with ultra-high-speed imaging and residual-velocity diagnostics. These developments will complete the design cycle of the projectile and will consolidate the numerical model as a predictive design tool for the next generations of frangible ammunition.

Acknowledgments

The authors gratefully acknowledge the support of the Military Technical Academy "Ferdinand I" of Bucharest for making available the software and the computational resources used in this study.

References

1. General Dynamics Ordnance and Tactical Systems, PGU-33/U TPF-T 25 mm Frangible Training Round, Technical datasheet, 2019.
2. R. E. Brown, M. Held, "Terminal ballistics of small-calibre kinetic energy projectiles," Propellants, Explosives, Pyrotechnics, vol. 24, no. 4, pp. 195-205, 1999.
3. M. Held, "Fragmentation of naturally fragmenting projectiles," Propellants, Explosives, Pyrotechnics, vol. 15, no. 6, pp. 254-260, 1990.
4. NATO Standardization Office, STANAG 4569 - Protection Levels for Occupants of Armoured Vehicles, Ed. 2, 2012.
5. ANSYS Inc., ANSYS Explicit Dynamics / AUTODYN User's Manual, Release 16.2, Canonsburg, PA, USA, 2015.
6. Century Dynamics Inc., AUTODYN - Explicit Software for Non-linear Dynamics, Theory Manual, Version 11.0, 2007.
7. D. J. Chapman, D. D. Radford, S. M. Walley, "Numerical simulation of high velocity impact of small-calibre projectiles on thin steel plates," International Journal of Impact Engineering, vol. 35, no. 12, pp. 1522-1533, 2008.
8. G. R. Johnson, W. H. Cook, "A constitutive model and data for metals subjected to large strains, high strain rates and high temperatures," Proceedings of the 7th International Symposium on Ballistics, The Hague, Netherlands, pp. 541-547, 1983.
9. A. Rusinek, R. Zaera, J. R. Klepaczko, "Constitutive relations in 3-D for a wide range of strain rates and temperatures - Application to mild steels," International Journal of Solids and Structures, vol. 44, no. 17, pp. 5611-5634, 2007.
10. L. B. Lucy, "A numerical approach to the testing of the fission hypothesis," The Astronomical Journal, vol. 82, pp. 1013-1024, 1977.

EXPERIMENTAL STUDY ON THE BALLISTIC IMPACT PERFORMANCE OF MULTILAYER SIDE BODY ARMOR

Alexandru-G. Vintilă[1], Florina Bucur[2]*, Adrian-N. Rotariu[3], Savu-E. Dima[4], Andrada-M. Sandu[5]

[1,2,3,5] Military Technical Academy "Ferdinand I"
[4] S.C. Tactical Life S.R.L.
**Corresponding author: florina.bucur@mta.ro*

***Abstract**: Personal ballistic protection has become increasingly important due to the development of high-energy small-arms ammunition and the need for lightweight and effective protective systems.*

This paper presents an experimental investigation of a multilayer ceramic–Kevlar side armor plate subjected to .308 Winchester ammunition. The impact process was recorded using a high-speed camera, while video analysis and post-impact examination were used to evaluate ceramic fragmentation and Kevlar deformation. The results showed complete fragmentation of the ceramic strike face, while the Kevlar backing absorbed the residual energy and prevented complete perforation. These results demonstrate the effectiveness of ceramic–aramid configurations against high-energy ballistic threats.

***Keywords:** Ballistic impact, Ceramic armor, Kevlar, High-speed imaging*

Introduction

The continuous evolution of ballistic threats has led to the development of increasingly efficient personal protection systems capable of stopping high-energy projectiles while maintaining an acceptable balance between protection level, weight and user mobility. Modern body armor therefore commonly relies on multilayer configurations combining materials with complementary mechanical properties [1–3].

Among the materials employed in ballistic protection, advanced ceramics and aramid fibers are widely used due to their complementary mechanical behaviour. Ceramic materials exhibit high hardness and compressive strength, promoting projectile erosion and fragmentation upon impact. In contrast, aramid fiber composites possess high tensile strength and energy absorption capability, allowing them to retain projectile fragments and limit the deformation transmitted behind the armor [2, 4–7].

The ballistic performance of ceramic–aramid configurations depends not only on the individual properties of the constituent materials but also on the interaction mechanisms developed during impact, including stress-wave propagation, ceramic cracking, projectile fragmentation, energy dissipation and deformation of the backing layer. Understanding these mechanisms is important for the development and optimization of lightweight ballistic protection systems [2, 4, 5, 8, 9].

The present study investigates the ballistic response of a multilayer ceramic–Kevlar side armor plate, with particular emphasis on the interaction between the ceramic strike face and the Kevlar backing and the associated damage mechanisms during projectile impact.

High-speed imaging provides valuable information on projectile behaviour, damage evolution and the dynamic response of multilayer structures during ballistic impact. Combined with post-impact examination, it enables an effective evaluation of ballistic response.

1. Materials and Methods

1.1 Experimental Setup

The experimental study was conducted at the "Anatolie Sălceanu" firing range under controlled conditions [10]. The complete configuration used is presented in Figure 1.

The experimental setup comprised the equipment required to perform the ballistic testing and evaluate the ballistic performance of the proposed multilayer ballistic configuration. It included a firearm, secured on a shooting bench, a rigid test stand equipped with a target-holding fixture, a witness panel used to indicate perforation, and a high-speed camera used to capture the projectile trajectory and impact.

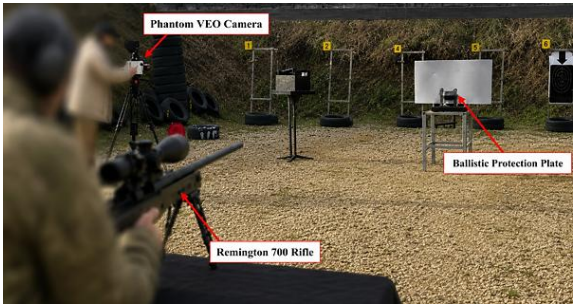


Figure 1: Experimental set-up

A Remington 700 MDT precision rifle chambered in .308 Winchester was used due to its high accuracy and repeatability, ensuring consistent projectile impact conditions during the ballistic test (Figure 2) [11].

Commercial .308 Winchester full metal jacket (FMJ) ammunition with a projectile mass of 9.55 g, a nominal muzzle velocity of 850 m/s and a kinetic energy of approximately 3450 J was used for the ballistic study (Figure 3) [12].



Figure 2: Remington 700 MDT precision rifle



Figure 3: .308 Winchester FMJ ammunition

The projectile–target interaction was monitored using a Phantom VEO high-speed camera equipped with a CMOS global shutter sensor, capable of recording images at a maximum resolution of 1,280 × 960 pixels and frame rates up to 10,860 fps (Figure 4) [13]. The recorded image sequences were subsequently processed using Phantom Cine Analyzer software.



Figure 4: Phantom VEO camera: (a) front-side view; (b) rear-side view

1.2 Ballistic Specimen

The investigated specimen was a Level IV side body armor plate manufactured by a local producer, designed for personal ballistic protection against high-energy threats [14]. The specimen consisted of a multilayer configuration comprising an alumina (Al_2O_3) ceramic strike face and a Kevlar backing layer (Figure 5).

The ceramic front layer, with a thickness of 9 mm, was intended to erode and fragment the projectile upon impact, thereby dissipating a significant portion of its kinetic energy. The Kevlar backing, with a thickness of 4.5 mm, was intended to absorb the residual impact energy, retain projectile and ceramic fragments, and limit the deformation transmitted to the rear face of the armor.



Figure 5: Ballistic protection plate: front view and cross-sectional configuration

The complete side armor plate had overall dimensions of 200 × 150 mm, a total thickness of 20 mm and a mass of approximately 2 kg. According to the manufacturer, the plate complies with NIJ Standard 0101.06 Level IV requirements and the Romanian Military Standard SMT 40202 (Protection Level SR8) [14, 15].

1.3 Experimental Procedure

Prior to testing, the armor plate was rigidly mounted on the support frame in order to eliminate undesired movements during impact (Figure 6). The test was performed at a firing distance of 10 m, with the projectile impacting the target at normal incidence (0°).

Following impact, the specimen was visually inspected and the damage morphology of both the ceramic strike face and the Kevlar backing was documented. Particular attention was paid to projectile fragmentation, ceramic cracking, residual deformation of the backing layer and the occurrence of complete or partial perforation.



Figure 6: Ballistic protection plate secured for testing

The high-speed image sequences recorded during the ballistic test were analyzed using Phantom Cine Analyzer software. Frame-by-frame examination enabled the identification of the main stages of the impact event, including projectile contact, ceramic fragmentation, deformation of the Kevlar backing and the final response of the multilayer armor plate. These observations were correlated with the post-impact examination in order to assess the ballistic performance of the investigated configuration.

2. Results and Discussion

2.1 Ballistic Response of the Ceramic–Kevlar Armor Plate

The ballistic performance of the investigated side armor plate was evaluated through post-impact examination and high-speed image analysis.

Following impact by the .308 Winchester projectile, extensive damage was observed in the ceramic strike face (Figure 7). The impact generated localized crushing and rapid propagation of radial cracks throughout the ceramic layer. This fracture pattern is characteristic of brittle armor ceramics and contributes to dissipating impact energy while reducing the integrity and penetration capability of the projectile [4, 5].

A detailed examination of the separated ceramic layer (Figure 8) confirmed complete fragmentation within the impact region. This behaviour is characteristic for ballistic ceramics, which act as sacrificial materials by absorbing impact energy through brittle fracture and projectile erosion. Consequently, the residual kinetic energy is transferred to the backing layer [4, 5].



Figure 7: Ballistic protection plate post-ballistic testing

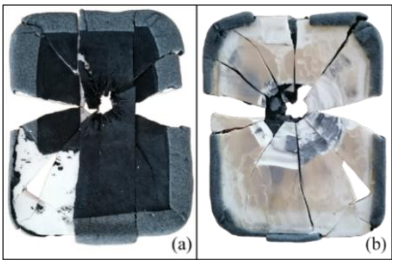


Figure 8: Ceramic layer: (a) front view; (b) rear view

The Kevlar backing exhibited a significantly different mechanical response (Figure 9). Instead of brittle fracture, the aramid laminate underwent progressive tensile deformation accompanied by energy absorption through fiber stretching and load redistribution within the multilayer structure. No complete perforation of the backing was observed, indicating that the aramid layer effectively contributed to absorbing and dissipating the residual impact energy.

Post-impact measurements on the rear face of the plate revealed a maximum back-face deformation (BFD) of approximately 10.35 mm and a deformation diameter of approximately 85.5 mm (Figure 10). Although permanent deformation occurred, the structural continuity of the Kevlar laminate was preserved, demonstrating its capability to distribute the impact load over a large area while maintaining the integrity of the protection plate.

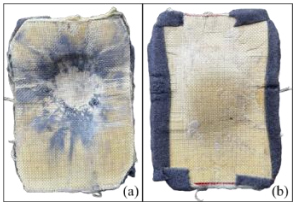


Figure 9: Kevlar backing layer: (a) front view; (b) rear view

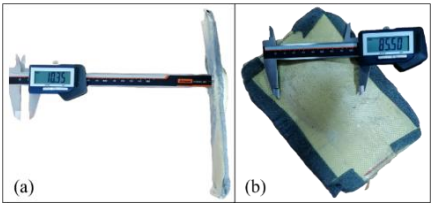


Figure 10: Measurements of the Kevlar backing layer after testing: (a) thickness measurement; (b) back-face deformation measurement

Overall, the observed response confirms the complementary action of the ceramic strike face and the Kevlar backing in dissipating the projectile kinetic energy and preventing complete perforation.

2.2 High-Speed Image Analysis

High-speed recordings processed with Phantom Cine Analyzer software enabled frame-by-frame examination of the dynamic response of the multilayer armor plate during projectile impact (Figure 11).

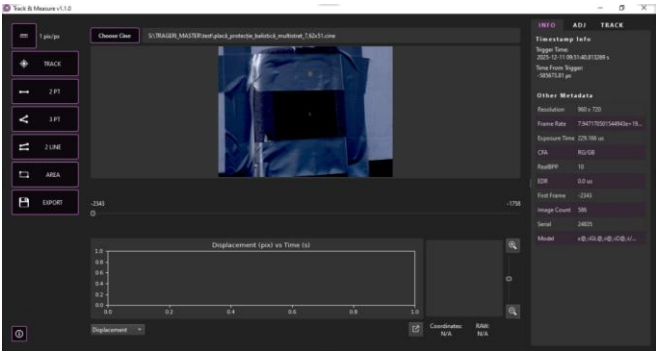


Figure 11: Phantom Cine Analyzer software interface

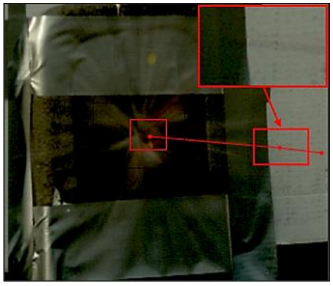


Figure 12: Bullet trajectory before impact

Immediately after impact, the projectile contacted the ceramic strike face, producing localized compressive failure within the impact zone. During the following frames, stress waves propagated throughout the ceramic layer, initiating crack nucleation and rapid radial crack growth. As fragmentation progressed, the projectile gradually lost its structural integrity while ceramic fragments were ejected from the impact region.

Subsequently, the remaining projectile fragments interacted with the Kevlar backing, producing progressive out-of-plane deformation of the laminate. The deformation increased until reaching its maximum value, after which the backing gradually recovered part of its elastic deformation while retaining the fragmented projectile and ceramic debris. Throughout the entire impact sequence, no complete perforation of the armor plate was observed.

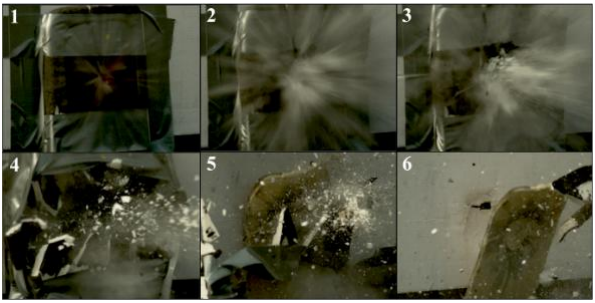


Figure 13: Sequential analysis of the ballistic impact: (1) initial impact; (2–3) impact wave propagation and ceramic fragmentation; (4) load transfer to the Kevlar backing; (5) maximum back-face deformation; (6) final post-impact state

The final frames of the recorded sequence (Figure 13) confirm the cooperative behaviour of the multilayer configuration. Although the ceramic strike face was completely fragmented, the Kevlar backing maintained its structural continuity and successfully stopped the remaining projectile fragments. These observations are consistent with the post-impact examination and demonstrate that the investigated ceramic–Kevlar configuration effectively dissipates the projectile kinetic energy through successive fragmentation and energy absorption mechanisms.

2.3 Discussion

The experimental results demonstrate that the ballistic performance of the investigated armor configuration is governed by the complementary mechanical behaviour of its constituent materials. The observed impact sequence is consistent with the failure mechanisms commonly reported for ceramic–aramid ballistic configurations. Upon impact, the ceramic strike face acts as a sacrificial layer, dissipating a significant portion of the projectile kinetic energy through localized crushing, crack propagation and fragmentation. As the projectile loses its integrity, the residual fragments are stopped by the Kevlar backing, where the remaining energy is absorbed through tensile deformation and load redistribution within the aramid laminate. The experimental observations obtained from both post-impact examination and high-speed recordings confirm this cooperative behaviour, demonstrating that the ballistic performance of the investigated armor plate results from the effective interaction between the ceramic strike face and the composite backing rather than from the individual contribution of each material.

The combination of post-impact observations and high-speed image analysis proved particularly valuable for understanding the sequence of events occurring during ballistic impact. Whereas conventional post-test observation only reveals the final damage state, high-speed recordings enable direct observation of projectile fragmentation, crack propagation and deformation evolution throughout the impact event. This combined experimental approach provides a comprehensive assessment of the ballistic response of

multilayer armor systems and a useful experimental basis for future numerical validation and extended ballistic investigations.

Conclusion

The ballistic response of a multilayer ceramic–Kevlar side armor plate subjected to .308 Winchester (7.62 × 51 mm) ammunition was experimentally investigated using high-speed imaging and post-impact examination.

The experimental results demonstrated that the ballistic performance of the armor plate is achieved through the complementary action of its constituent layers. The alumina ceramic strike face acted as the primary energy-dissipation component by fragmenting and destabilizing the projectile, whereas the Kevlar backing absorbed the residual kinetic energy and successfully prevented complete perforation while maintaining the structural integrity of the armor configuration.

High-speed image analysis enabled visualization of projectile fragmentation, crack propagation within the ceramic layer and deformation of the Kevlar backing, providing information complementary to the post-impact observations.

Overall, the investigated multilayer ceramic–Kevlar configuration exhibited an effective ballistic response against .308 Winchester ammunition, demonstrating the advantages of combining brittle ceramic materials with high-performance aramid composites in personal ballistic protection systems.

Future work will focus on extending the experimental investigation to different impact velocities, projectile types and impact angles, as well as integrating the experimental observations with numerical simulations to improve the understanding and optimization of multilayer ballistic protection systems.

Acknowledgments: This paper has been supported by S.C. Tactical Life S.R.L.

References

1. Crouch, I. G. (2019). Body armour: Engineering design. Woodhead Publishing.
2. Hazell, P. J. (2022). Armour: Materials, theory and design. CRC Press.
3. Cunniff, P. M. (1999). Dimensionless parameters for optimization of textile-based body armor systems. Proceedings of the 18th International Symposium on Ballistics.
4. Medvedovski, E. (2010). Ballistic performance of armour ceramics: Influence of design and structure. Part 1. Ceramics International, 36(7), 2103–2115.
5. Medvedovski, E. (2010). Ballistic performance of armour ceramics: Influence of design and structure. Part 2. Ceramics International, 36(7), 2117–2127.
6. Morye, S. S., Hine, P. J., Duckett, R. A., Carr, D. J., & Ward, I. M. (2000). Modelling of the energy absorption by polymer composites upon ballistic impact. Composites Science and Technology, 60(14), 2631–2642.
7. Phoenix, S. L., & Porwal, P. K. (2003). A new membrane model for ballistic impact into woven fabrics. International Journal of Solids and Structures, 40(24), 6723–6765.

8. Wilkins, M. L. (1978). Mechanics of penetration and perforation. International Journal of Engineering Science, 16(11), 793–807.
9. Hurmuzache, A., Bucur, F., Puică, C., & Rotariu, A.-N. (2026). Numerical study on the performance of a ceramic/Kevlar 29 fiber ballistic package against small-caliber kinetic threats. Macromolecular Symposia, 430, e70423.
10. Vintilă, A.-G. (2026). Evaluarea fenomenelor de impact dintre pachetele balistice multistrat și muniția de calibru mic (Master's thesis). Military Technical Academy "Ferdinand I", Bucharest, Romania.
11. Remington Arms Company. (n.d.). Model 700 bolt-action rifle: Owner's manual & technical specifications.
12. Sellier & Bellot. (n.d.). .308 Winchester FMJ: Product specifications.
13. Vision Research. (n.d.). Phantom VEO camera: User manual.
14. STIMPEX S.A. (n.d.). Ballistic protective plates. Retrieved August 7, 2026, from https://stimpex.ro/ro/products/defense-products/ballistic-protection-equipment/body-armor-and-plates/ballistic-protective-plates/
15. National Institute of Justice. (2008). Ballistic resistance of body armor (NIJ Standard 0101.06). U.S. Department of Justice.

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

RESEARCH ON THE RELIABILITY AND SERVICE LIFE OF SPECIAL MECHANICAL SYSTEMS

Andrada-M. Sandu, Pamfil Șomoiag, Liviu-C. Matache, Alina Pleșca, Alexandru-G. Vintilă

Faculty of Integrated Armament Systems, Military Engineering and Mechatronics, Military Technical Academy „Ferdinand I", Bucharest, ROMANIA,
**Corresponding author: maria.sandu@mta.ro*

Abstract: *This paper evaluates the reliability and service life of the 100 mm model 1977 anti-tank gun using the two-parameter Weibull distribution and data from 15 guns. The recoil system is identified as the reliability-limiting component under the non-repairable assumption, whereas the barrel governs the partially repairable system service life. The influence of projectile-related ballistic parameters on barrel service life is also assessed.*

Keywords: *Reliability analysis, Weibull distribution, Mean Time to Failure, Weapon system, Gun barrel service life*

Introduction

The reliability assessment of a weapon system represents a predictive process based on the application of reliability models, failure mode and failure mechanism analyses, and other related methods.

The reliability assessment process should employ up-to-date data obtained from verification and operational activities, in accordance with the requirements of the applicable technical documentation. Furthermore, reliability assurance activities should be integrated with the other components of the design–development–manufacturing–operation cycle [1].

The required data are obtained through the analysis of the reliability of components, materials, and processes, testing of weapon systems during the manufacturing stage and the collection of specific information (physical, chemical, thermodynamic, etc.) that enables the investigation of particular failure mechanisms.

1. Configuration and reliability model of the reference system

The present study aims to perform a statistical reliability analysis of a system, taking into account the influence of its main component subsystems and the manner in which they are interconnected [2]. The methodology is based on the application of theoretical reliability models combined with statistical estimation methods, with the objective of quantitatively assessing system performance.

To conduct the analysis, the 100 mm model 1977 anti-tank gun, presented in Figure 1, was selected as the reference system.



Figure 1: 100 mm model 1977 anti-tank gun

The reliability analysis of the system is conducted at the level of three main components, namely the *barrel*, the *breech mechanism*, and the *recoil system*. These components are considered critical to the proper functioning of the overall assembly. The reliability of the system is determined based on the reliability of these components, taking into account their functional roles and the loads and stresses to which they are subjected.

From the standpoint of reliability theory, the 100 mm model 1977 anti-tank gun, adopted as the reference system, can be mathematically represented as a ***series-configured*** system, since its functional capability depends on the successful operation of all three components.

2. Reliability assessment of the 100 mm model 1977 anti-tank gun – a case study

For the statistical reliability analysis of the 100 mm model 1977 anti-tank gun, the Weibull distribution was adopted because of its suitability for modeling mechanical systems subjected to progressive degradation, wear, and fatigue processes.

The two-parameter Weibull distribution, with parameters β and θ, has the probability density function given by the following equation [3]:

$$f(t) = \frac{\beta}{\theta}\left(\frac{t}{\theta}\right)^{\beta-1} e^{\left[-\left(\frac{t}{\theta}\right)^{\beta}\right]} \quad (1)$$

where β represents the shape parameter, θ denotes the scale parameter, and t is the *operating variable*, expressed in the present study as the number of *rounds fired*.

In the present analysis, the Weibull parameters β and θ were estimated for each component from the corresponding experimental failure data using the maximum likelihood method, providing the basis for the subsequent determination of the reliability functions [2].

The reliability model is based on three fundamental assumptions: the weapon is represented as a series system, the initial model is considered non-repairable, and system failure is defined by the occurrence of the first component failure, irrespective of the component in which it occurs.

Operational data concerning component failures were collected from the service and maintenance records of a sample of 15 anti-tank guns [2].

Based on these data, the principal reliability parameters were determined, and the reliability behavior of the analyzed components was evaluated as a function of the number of rounds fired, with the aim of identifying the influence of failures on system operation and estimating its service life.

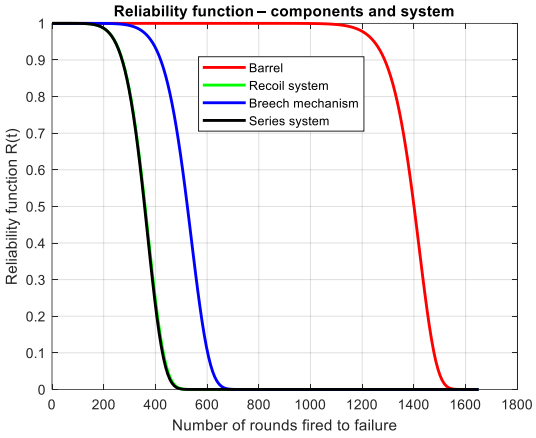


Figure 2: Reliability function plot for the reference system and its components

The reliability functions presented in (Figure 2) show that the barrel exhibits the highest reliability over the investigated operating range, whereas the recoil system exhibits the lowest reliability and therefore represents the most vulnerable component.

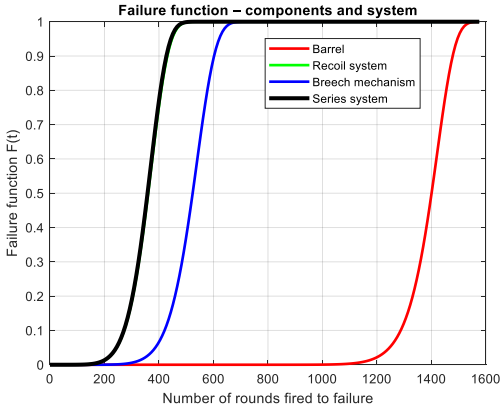


Figure 3: Failure distribution function of the reference system and its components

The plot of the failure distribution function (Figure 3) for the series system determined on the basis of the Weibull distribution under the assumption of a non-repairable system and considering exclusively the occurrence of the first failure, demonstrates that the behavior of the overall assembly is governed by the component exhibiting the steepest increase in the probability of failure. The results indicate that the recoil system is the critical component, exhibiting the fastest increase in failure probability, followed by the breech mechanism, whereas the barrel exhibits a considerably later increase in failure probability.

Figure 4 presents the Weibull probability density function *f(t)* for the system components and the series system. The function *f(t)* describes the probability distribution of failure occurrence as a function of the number of rounds fired and indicates the interval in which failures are most likely to occur.

The recoil system reaches its maximum failure probability density at approximately 350–400 rounds, indicating the earliest concentration of failures. The breech mechanism peaks at 500–600 rounds, while the barrel reaches its maximum at approximately 1,350–1,450 rounds. The close correspondence between the probability density curves of the series system and the recoil system further confirms that the overall failure behavior is predominantly governed by the recoil system.

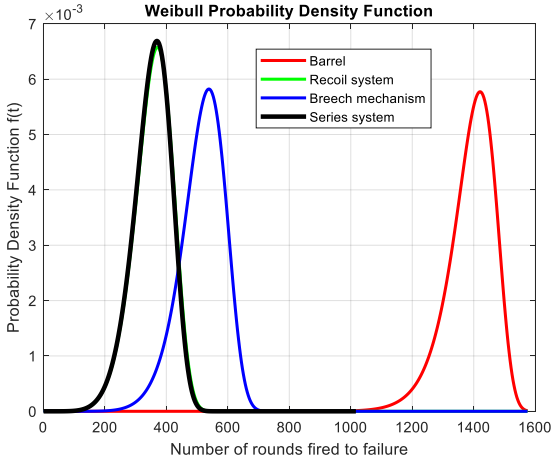


Figure 4: Probability density function plot using the Weibull distribution for the reference system and its components

The plot presented in Figure 5 illustrates the Mean Time to Failure values for the analyzed components and the non-repairable series system, expressed as the mean number of rounds fired until the first failure. The barrel exhibits the highest MTTF, approximately 1,389 rounds, reflecting its comparatively gradual degradation. The breech mechanism shows an intermediate value of approximately 516 rounds, while the

recoil system records the lowest MTTF, approximately 355 rounds, identifying it as the most vulnerable component of the system.

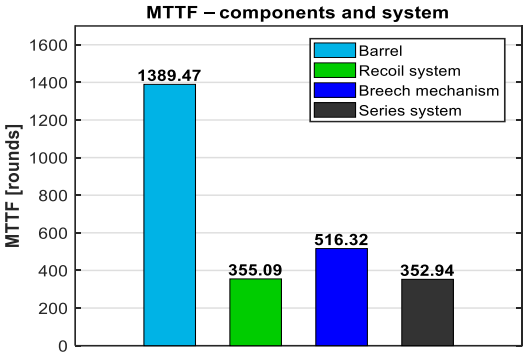


Figure 5: MTTF values based on the Weibull distribution for the reference system and its components

The series system exhibits an MTTF of approximately 353 rounds, closely corresponding to that of the recoil system. This indicates that, under the series-system assumption, the reliability behavior of the complete system is strongly influenced by the component with the lowest MTTF.

Although the initial analysis considered the system as non-repairable, the recoil system and breech mechanism can be repaired or replaced during operation. Their failure therefore results in only a temporary loss of system functionality.

In contrast, the barrel is considered non-repairable, as advanced wear and internal erosion cannot be effectively reversed through conventional maintenance. Within the model adopted in the present study, the barrel is treated as the non-repairable and life-limiting component.

Progressive internal wear and erosion eventually cause the barrel to reach the limiting conditions specified by the applicable technical documentation. Reaching this limit is therefore considered the terminal condition of the service-life model. Under this assumption, the service life of the system is no longer determined by the first failure of any component. Instead, operation may continue after replacement of the repairable components until the barrel reaches its limiting condition.

To assess the reliability behavior of the partially repairable system, the approximate number of replacements of the repairable components before barrel failure was estimated using the following formulas:

$$N_{recoil\ system} = \frac{MTTF_{barrel}}{MTTF_{\ recoil\ system}} \tag{2}$$

$$N_{breech\ mechanism} = \frac{MTTF_{barrel}}{MTTF_{\ breech\ mechanism}} \tag{3}$$

The estimates indicate that, before the barrel reaches its limiting service-life condition, approximately three recoil-system replacements and two breech-mechanism replacements may be required. These values should be interpreted as approximate estimates based on the mean failure behavior of the components rather than as deterministic replacement intervals.

The comparison between the two models (Figure 6) highlights the influence of component repairability on system service life. Under the non-repairable assumption, the first component failure limits the system MTTF to approximately 353 rounds, whereas, under the partially repairable assumption, operation can continue until the barrel reaches its limiting condition, corresponding to an expected service life of approximately 1,389 rounds.

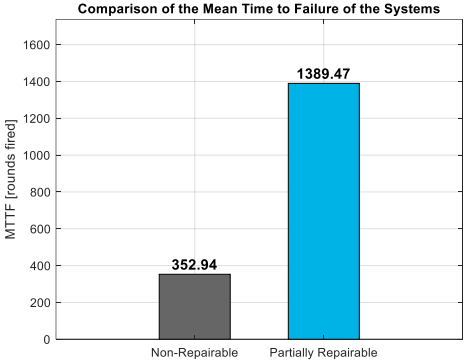


Figure 6: Comparison of system service life under the non-repairable and partially repairable assumptions

Since the partially repairable system analysis identifies the barrel as the ultimate service-life-limiting component, the subsequent analysis focuses on the factors affecting barrel durability and, in particular, on the influence of projectile-related ballistic parameters.

3. Influence of projectile type on barrel service life

Barrel service life is defined as the operating period during which the barrel maintains its ballistic performance within the limits specified by the technical documentation, namely accuracy, projectile muzzle velocity, and range [4].

Barrel service life is primarily influenced by its design characteristics, including caliber, wall thickness, rifling configuration, steel properties, and manufacturing technology. Projectile and propellant characteristics also contribute significantly through driving-band properties, projectile stability, manufacturing accuracy, and the pressure and temperature generated during combustion. Maintaining service life and performance

requires proper bore cleaning, ammunition preparation, compliance with the prescribed firing rate, post-firing preservation, and periodic maintenance [4].

The analytical quantification of the combined influence of all factors governing barrel wear is highly complex; therefore, empirical equations are employed for the approximate estimation of barrel service life [4]. Given the differing assessments of the relative significance of these factors, several empirical formulations have been developed. One such equation is presented below [4]:

$$N = 240 \cdot \frac{d}{\omega} \cdot \left[\frac{\sigma_e}{2250} - 4 \cdot \left(\frac{P_{max}}{2250} - 1\right)\right] \cdot \frac{0{,}25}{l_b} \quad (4)$$

where the terms represent: d - caliber; ω - propellant charge mass; P_{max} - maximum gas pressure; σ_e - yield strength of the barrel material; l_b - the driving band width.

Thus, by applying Equation (4), and assuming that the artillery gun performs firings with the same type of projectile, an estimate of the service life of the barrel of the 100 mm model 1977 anti-tank gun was determined for firing with low charge high-explosive, armor-piercing tracer, low-spin shaped-charge projectile, and sub-caliber projectiles with discarding sabot, respectively, as shown in Figure 7.

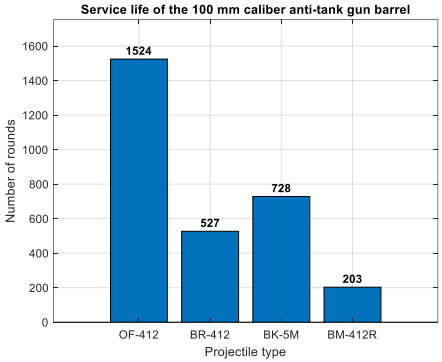


Figure 7: Service life of the 100 mm model 1977 anti-tank gun barrel for each projectile type

The results obtained and presented in Figure 7 show that the highest service life is associated with the case in which the gun fires the low-charge high-explosive projectile, whereas the minimum barrel service life corresponds to the case in which the system fires the sub-caliber projectile with discarding sabot.

The lower barrel life associated with the sub-caliber projectile with discarding sabot is primarily attributed to its higher maximum pressure (3075 kgf/cm² compared with 2000 kgf/cm² for the low charge high-explosive projectile). According to Equation (4), higher maximum pressure and propellant charge, as well as increased driving-band width, reduce barrel service life by increasing thermomechanical and frictional loading.

Thus, projectile type significantly influences barrel service life through its ballistic and design parameters.

Conclusion

Under the non-repairable system assumption, reliability is determined by the first component failure. The recoil system represents the reliability-limiting component, with the lowest MTTF of approximately 355 rounds, closely corresponding to the series-system MTTF of 353 rounds.

Under the partially repairable model, the recoil and breech mechanisms can be replaced during operation, while the barrel is considered non-repairable. Within the partially repairable model adopted in this study, the barrel represents the terminal, non-repairable component. The expected system service life is therefore governed by the barrel and is estimated at approximately 1,389 rounds.

Projectile type significantly affects barrel wear through differences in propellant charge, barrel pressure, and projectile–bore contact characteristics, which determine the resulting thermomechanical stresses.

References

1. Ghiță, A. (1996). *Reliability Calculation Methods: Definition and Evaluation of Reliability*. Bucharest: Military Technical Academy Publisher.
2. Sandu, A.-M. (2026), Cercetări privind fiabilitatea și durata de viață a sistemelor mecanice speciale (Master's thesis). Bucharest, Military Technical Academy "Ferdinand I".
3. Burlacu, G. (2005). *Reliability, Maintainability and Availability of Technical Systems: Reliability Theory*. Bucharest: Matrix Rom.
4. Constantin, Gh. (1996). *Fundamentals of Weapon Systems Reliability: Reliability of the Elements Comprising Weapon Systems and the Influence of Environmental Factors on Reliability*. Bucharest: Military Technical Academy Publisher.

THE SYSTEM OF SISTEMS CONCEPT IN MULTIDOMAIN ENVIRONMENT

Valentin S. Vasilev

Faculty of Navigtion, Nikola Vaptsarov Naval Academy, Varna, Republic of Bulgaria,
valentin-vasilev@naval-acad.bg

***Abstract**: Modern multi-domain operations require military forces to adapt to an increasingly complex, nonlinear battlespace where traditional, centralized assets face significant challenges. The proposed paper analizes contemporary theory developments of the transition to a "system of systems" (SoS) force architecture using a systems-theoretic approach and hypernetwork modeling within the C4ISTAR framework. By replacing rigid binary connections and concentrated platforms with decentralized, highly adaptive networks of differnent sensors, decision-making, and strike units, the SoS model optimizes the OODA-loop and prevents critical information loss. The structural and functional resilience across micro, meso, and macro operational levels are described, in order to propose possible theoretical approach to control internal system`s entropy and enabling dynamic resource allocation under intense opposition. Moreover, adopting an SoS concept provides a feasible basis for maintaining command and control stability, operational-level superiority, and synchronized targeting within uncertain multidimensional environments.*

***Keywords:** Command and Control, Multidomain battle space, System of systems.*

Introduction

The increasing complexity of the security environment leads to a transformation of the battlespace. Military doctrines describe multi-domain operations conducted across the entire continuum of operations - at strategic, operational, and tactical levels - inherently characterized by joint operations. The evolution of military technologies and the increasing complexity of their employment necessitate designing processes within a multidimensional space. Applying the systems approach enables the representation of military forces and the organization of the battlespace as a "system of systems." A direct outcome of implementing the systems approach is enhanced situational awareness regarding environmental conditions - factors, processes, patterns, risks, and threats - ultimately leading to reduced uncertainty (Nielsen et al., 2015).

A pressing issue that has continuously attracted interest in one form or another is the predictability of events. In the 1980s, the concept of "security" emerged, driven by evolution and the corresponding need for predicting random events. Schematically examining a joint effects-based operations, it can be tentatively assumed that it is conducted in several domains simultaneously to achieve a common effect and synergy through the utilization of generated forces and developed military capabilities.

1. The evolution of complex systems in multidomain operations

Using the systems approach, let us view the organization of a military system as a collection of smaller subordinate military systems interacting by exchanging energy, information, or other material and non-material resources. Each interconnected system, in turn, possesses its own functionality, structural organization, and characteristics. They

are figuratively "immersed" in a surrounding environment. This environment contains the zone of military operations, which can be described as a specific area within the multi-domain battlespace.

1.1. New organization of the battle field

When tasks are addressed in a multidimensional space, the management of the system's state depends on operational factors. Operational factors determine the situational conditions that affect the entities present within the given spatial region. Under these conditions, a real-life military system interacts with the external environment. A defining characteristic of military systems is that, to enhance combat resilience, they are largely isolated from their surrounding environment. Although they inherently display features of closed complex systems, they maintain resource connectivity with the external environment. This connectivity is typically informational, energetic or material. For example, while executing assigned tasks, a military system collects information from the environment, conducts electronic warfare against targets, delivers firepower, or sustains battle damage. As shown in these basic examples, there is a high probability that the system will be subject to adverse impacts with significant potential to increase its internal entropy, shifting the bifurcation point substantially to the right - thereby exacerbating state uncertainty.

The increasing complexity of battlespace organization is a continuous process that accompanies the evolution of security and defense requirements. Achieving a state of superiority requires constructing something fundamentally different from the existing reality in space, reflecting current needs and technological advancement. A distinct, innovative approach to battlespace organization makes it possible to achieve operational-level military superiority through adaptive resource transformation of deployed forces and capabilities and timely maneuvering, so that neither combat units, nor their numbers, are decisive at any given moment. Gaining superiority has always depended on the ability to maneuver forces and transform available resources from a surplus type into a lacking type that is critical for achieving superiority over opposing forces. This is particularly valuable under conditions of qualitative and quantitative force constraints and systemic resource shortages.

1.2. Forces made of complex systems

Creating a "system of systems" type organization enhances freedom in leveraging operational factors and their combinations, provided there is sufficiency in the operational factor of "information," thereby achieving an operational-level advantage (Nielsen et al., 2015). Utilizing advantages within the context of the operational factors of "time," "space," and "forces" acquires different dimensions when systems are built from integrated, highly adaptive, and sometimes nearly self-sufficient subsystems. These subsystems are managed sustainably over time regardless of external conditions, despite uncertainty and unpredictable adverse impacts. In fact, command resilience is critical to achieving military superiority in the described battlespace environment. Therefore, command and control capabilities normally are the primary targets of the opponent's adverse actions.

The organization of command and control systems is based on principles of continuity, redundancy, concealment, etc., specifically to increase combat resilience - that is, the ability of forces or weapon systems to withstand adverse opponent actions. Combat resilience, in turn, is directly linked to the combat effectiveness of forces and weapon systems. Combat effectiveness should be understood as the capacity of forces and weapon systems to affect the adversary. When organizing the battlespace as a "system of systems," it must be taken into account that the security environment phenomena are interconnected. This is accounted as connectivity among operational factors, interrelationships across different operational domains, and the integration of resource and information flows. Furthermore, it should be noted that these connections are resource-based in nature - primarily informational and energetic, and to a lesser extent material, financial, and economic.

The battlespace has changed its organization. Concentrated centers of power where resources are gathered are losing their relevance. The existence of massive command posts saturated with critical communication infrastructure, huge logistics hubs, and mega-factories producing critical defense components is becoming obsolete. Concentrating systemic resources in a single, limited space carries the risk of destruction in a single strike or, more abstractly, being compromised by a single adverse impact - be it of great power, high intensity, broad scale, or long duration. This is not entirely new. The occurrence of a single random event in such cases has the potential to dramatically affect the entire system by striking critical subsystems, command nodes, vital connectivity, and key infrastructure. Advances in surveillance systems, communications, and the implementation of radically new high technologies - driven by ambitions for influence, total control, and even dominance in a specific domain - have led to the emergence and refinement of powerful new-generation weaponry. Narrowing the focus to the military domain, examples of such weapons possessing high destructive potential and target hit probability include maneuvering ballistic and hypersonic missiles. Their characteristics allow for surprise and high-power strikes at long engagement ranges (exceeding 2,000 km) and high flight speeds (up to Mach 10–12 in certain weapon systems). The conclusion is clear: in practice, the safety of no physical object located within the operational zone can be continuously guaranteed over time. These altered battlespace conditions demand a radically updated response.

Forces operating in multidimensional space face the challenges of dynamic reconfiguration and maintaining combat resilience in a highly confrontational environment, ensuring effectiveness against opposing complex systems. Naturally, military systems are driven by requirements for self-organization and resilience amidst significant and abrupt external changes. Introducing the "system of systems" construct allows forces to be projected across multidimensional space on three levels: micro, meso, and macro (Duan, 2026). Such an organization enables tailored interaction between combat units at every level, yielding required emergent system properties upon subsequent reorganizations. Force resilience, particularly at the micro level, directly depends on preserving the quality and quantity of connectivity and establishing an appropriate organizational structure to overcome information loss. At the meso level, a fractal transition occurs from the micro to the macro level. The organization becomes

more complex, and combat elements arrange themselves into combat clusters capable of group-level reorganization. At the macro level, adaptation to environmental changes is organized using entirely system of systems principles, linked into a unified hypernetwork that accounts for impacts in real time. Executed simulations demonstrate that organizing forces as an aggregate of high-order systems exhibits robust resilience against random and targeted attacks compared to traditional networks (Duan, 2026). The system of systems framework provides a foundation for designing adaptive, highly resilient target engagement networks composed of intelligent combat systems.

2. Why SoS?

In the multidimensional battlespace, single engagements between individual platforms fractally transform into complex confrontations between systems of systems across various domains. In multidimensional space, a combat system of systems is defined as an organized whole of heterogeneous combat units from different operational domains, unified by common integrated systems within the C4ISTAR architectural framework - Command, Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition, and Reconnaissance - to execute the full spectrum of possible missions at strategic, operational, and tactical levels.

2.1. The requirments of composition and connectivity

Changes in the battlespace fundamentally alter the conditions for achieving superiority in a conflict situation. The center of gravity shifts from the protection and combat survivability of individual platforms to the system's ability to maintain structural and functional resilience as a system of systems, regardless of the severity and scale of adverse impacts (Nielsen et al., 2015). Modern local conflicts demonstrate that concepts of intelligent defense through network-centric and effects-based operations aim for states of asymmetry and decentralization. In this model, complex, expensive, multi-role platforms are replaced by swarming, affordable, low-cost, and highly specialized unmanned systems capable of real-time assembly and attacking within dynamically adaptive target-engagement networks against opposing military systems.

Combat systems are quintessential nonlinear complex systems. In a complex environment, the complexity of hypernetworks presents an elevated risk of cascading failures, total lockups, and the actual breakdown of the system of systems. System fragmentation and reliance on binary links between adjacent nodes introduce significant potential for information loss in complex environments (Malizia, F. *et al.* 2024). Force organization in the complex conditions of multidimensional space is inherently challenging. Multidimensional combat missions require real-time, multi-faceted coordination among numerous subsystems across command posts, sensors, and effectors deployed on strike platforms across various domains.

A viable solution lies in applying tools from hypernetwork theory. A hypernetwork is a network where an edge or a hyper-edge can connect an arbitrary number of vertices (Millan, *et al.*, 2025). In contrast, a standard network in three-dimensional space connects exactly two vertices per edge, which in a multidimensional setting creates

conditions for information loss. A hyperedge can thus accurately model multi-party collaboration without loss of information (Malizia *et al.*, 2024).

A system of systems can be modeled as a hypernetwork H = {V, E},where:

$V = \{v_1, v_2, ..., v_n\}$ is the set of nodes (for example combat platforms),

$E = \{e_1, e_2, ..., e_m\}$ is the set of hyperedges representing joint missions in multidimensional space (Duan, 2026).

Functionally, a military system of systems executes the OODA combat loop (Observe, Orient, Decide, Act), structured around the C4ISTAR architectural framework. Structurally, elements of a military system of systems are categorized into three main functional classes (Duan, 2026):

- *Decision-making and control units:* Command centers and posts that analyze intelligence data, plan operations, and assign tasks to strike platforms.
- *Sensors:* Platforms with intelligence, radar tracking, and battle damage assessment capabilities designed to gather environmental data.
- *Effectors:* Platforms equipped with physical or software target engagement capabilities.

Connectivity among combat units in a military system of systems facilitates information exchange divided into three distinct flows: an intelligence flow between sensor, decision-making, and strike units; a command flow (between decision-making units and all other units); and a mutual support and feedback flow. These connections are dynamic and normally are concealed within the noise of a multidimensional battlespace.

2.2. The adequate adapted answer

What does a possible response look like through the lens of multidimensional space, where complex systems exchange systemic resources via networked or network-centric interconnections, and less frequently via strict hierarchies? The technological surge in the theater of operations manifests in the emergence of advanced, new-generation complex combat platforms. These platforms embody substantial combat potential as systemic elements within multi-domain space. Local armed conflicts demonstrate that physical units alone - such as communication technologies, advanced artillery systems, guided cruise missiles, electronic warfare systems, radars, and their carrying platforms - are insufficient to guarantee superiority. The reality of multidimensional space necessitates building a resilient, efficient defense system composed of multiple distinct "systems of systems." Each adaptive integrated subsystem is organizationally built from physical system elements dispersed and distributed across the battlespace, comprising command and control nodes along with corresponding sensors and effectors.

Forces executing missions in multidimensional space face complex impacts and a diversification of physical threat sources. The nature of threat manifestation is shifting: traditional threats are complemented by conceptually novel forms of attack, complicating the operational employment of forces. In response to this environmental unpredictability, the solution involves integrating heterogeneous defense technologies connected functionally - capable of delivering reliable, real-time countermeasures against a wide spectrum of threats across multiple domains.

Conceptual architectural frameworks are being developed in which weapon systems in multidimensional space, as integral components of force structure, face requirements exceeding standard force interoperability. These next-generation systems must function in a resilient and coordinated manner across the battlespace. They must feature an adaptive organizational structure integrating: command and control systems; decision-support communication and information systems; complex sensors to perceive multidimensional battlespace dynamics; and multiple effectors capable of synchronized target engagement across multiple domains.

To illustrate the concept of "system of systems" force design, consider an example of a layered air defense architecture with early warning capabilities. A target is initially detected and classified by long-range technical systems. Subsequently, tracking and identification may be handed over to a low Earth orbit (LEO) space-based system. Information is securely exchanged through encrypted C4I networks, reaching an intelligent C2 decision-support system in real time, synchronizing the system of systems with bounded signal latency and high data transmission resilience. The next phase may involve transferring target tracking to ground-, air-, or sea-based radar and electro-optical stations, or unmanned platforms. Following data processing, targeting data is routed to effector control systems. Risk and threat assessments are conducted by real-time algorithms to ensure kinetic or non-kinetic interception along designated segments of the munition's trajectory. Throughout detection, classification, and engagement, the C2 system maintains a unified, multi-layered operational-tactical picture, harmonizing individual system functions within multi-domain operations.

Conclusion

Structuring military forces on the "system of systems" principle enables dynamic adaptation to multidimensional battlespace conditions through flexible, real-time allocation of systemic resources across domains. Weapon systems evolve to achieve higher combat resilience, resulting in increased combat effectiveness. Building combat systems as a "system of systems" represents an adapted, natural response to the systemic complexity characteristic of multidimensional space. A critical challenge arises here: ensuring command resilience across diverse environmental conditions, particularly amidst non-linearity and heightened process dynamics within the battlespace. Contemporary multi-domain operations require military forces to adapt to an increasingly complex, nonlinear battlespace where traditional, centralized assets face significant challenges. New battlespace reality requires military forces organization to be transformed to "system of systems" force architecture within the C4ISTAR framework.

References

1. Duan, Y., et al. (2026) Resilience Modeling Method for Combat System-of-systems Based on Hypernetwork and Game Theory. Journal of System Simulation. 38(7): 1870-1886. Available at: https://dc-china-simulation.researchcommons.org/journal/ vol38/iss7/6

2. Malizia, F. et al. (2024) Reconstructing higher-order interactions in coupled dynamical systems. Nat Commun 15, 5184. Retrieved from https://doi.org/10.1038/ s41467- 024-49278-x
3. Millan, A. et al. (2025) Topology shapes dynamics of higher-order networks. Nat. Phys. 21, 353–361. Retrieved from https://doi.org/10.1038/s41567-024-02757-w
4. Nielsen, Cl. et al. (2015). Systems of Systems Engineering: Basic Concepts, Model-Based Techniques, and Research Directions. ACM Computing Surveys. 48. 1-41. Retrieved from https://doi.org/10.1145/2794381

A MULTI-CRITERIA MODEL FOR ASSESSING THE RESILIENCE OF COMMUNICATION SYSTEMS UNDER NUCLEAR, CHEMICAL AND BIOLOGICAL THREATS

Nikolay Iliyanov Padarev

Faculty of Logistics and Technologies, Vasil Levski National Military University, Veliko Tarnovo, Republic of Bulgaria, nipadarev@nvu.bg

***Abstract**: Maintaining reliable information exchange under nuclear, chemical and biological threats is a prerequisite for continuity of government, interagency coordination and timely public warning. This paper proposes a multi-criteria model integrating technical protection, redundancy and autonomy, information resilience, operational interoperability and warning capability. Scenario-specific weights account for the different characteristics of nuclear, chemical and biological threats. The model is applied to publicly documented capabilities in the United States, the United Kingdom, France and Israel. Based on the identified dependencies, guidelines are formulated for applying the model to assess communication resilience within the national disaster protection system.*

***Keywords:** communication resilience, CBRN threats, crisis management, multi-criteria assessment, interoperability, critical infrastructure, public warning.*

Introduction

Crisis-management capability depends not only on the availability of personnel, resources and pre-established plans, but also on whether information reaches the structures responsible for assessing it and taking the necessary action in a timely manner. When communication is disrupted, decisions are made on the basis of an incomplete or outdated operational picture.

The problem becomes particularly significant under nuclear, chemical and biological threats. The consequences may include physical destruction, power outages, restricted access to contaminated areas, congestion of public networks and the need for prolonged operations in hazardous environments. In a nuclear scenario, the electromagnetic pulse may additionally affect unprotected electronic equipment and communication infrastructure [1].

Resilient civil communication systems are among NATO's baseline requirements for national resilience [2]. Existing approaches define resilience as the capacity to prepare, adapt, withstand impacts and recover [3, 4]. However, there is no sufficiently structured model that simultaneously accounts for technical, information-related and organisational characteristics across different CBRN scenarios.

The aim of this study is to develop and pilot a multi-criteria model for assessing communication resilience and to analyse its potential application within the national disaster protection system. The hypothesis is that communication resilience is determined not by the reliability of an individual asset, but by the combined influence of technical protection, redundancy and autonomy, information resilience, operational interoperability and timely warning capability.

The proposed model is piloted through a scenario-based comparative assessment of publicly documented communication capabilities in the United States, the United Kingdom, France and Israel. The pilot application tests the applicability of the criteria structure, the feasibility of scenario-specific weighting and the sensitivity of the results; it does not constitute a definitive empirical validation of national capabilities.

1 Specific Requirements under CBRN Threats

Communication resilience is the ability of interconnected assets, networks, personnel and procedures to maintain the minimum required information exchange, switch to backup operation and restore critical functions within defined time limits. It is broader than technical reliability: a resilient system tolerates failures but prevents them from resulting in a loss of command and control.

Assessing communication resilience requires consideration not only of the availability of backup assets, but also of their functional independence. The use of shared infrastructure components, such as base stations, power supplies, transmission lines or identity-management systems, may cause simultaneous failure of the primary and backup channels. Actual redundancy is therefore determined by the ability to preserve information exchange when a shared infrastructure component fails.

In a nuclear scenario, the determining factors are physical protection, resistance to electromagnetic effects, dispersal, autonomous power supply and independent backup channels. In a chemical incident, rapid warning, transmission of field measurements and interoperability among response units, laboratories and command authorities are paramount [5].

A biological threat may initially remain undetected and develop over an extended period. Critical factors include information exchange among medical, laboratory and administrative structures, the protection of restricted information and personal data, and the timely provision of reliable information to the public. The World Health Organization identifies risk communication as a core function in public-health emergencies [6]. The criteria may therefore be common, but their relative weights should vary according to the threat.

2 Research Methodology

The model comprises five groups of criteria (Table 1). Their selection follows the logic of the functional chain and accounts for both the technical condition and the organisational capacity to use communications in a disrupted environment.

Table 1: Model criteria

Criterion	**Key indicators**
C1 Technical protection	Physical protection; EMP resistance; dispersal
C2 Redundancy and autonomy	Independent channels; autonomous power supply; recovery
C3 Information resilience	Cybersecurity; data protection; information reliability
C4 Operational interoperability	Interagency exchange; procedures; exercises
C5 Warning capability	Multi-channel delivery; priority access; risk communication

The indicators are rated on a scale from 0 to 4: 0 denotes no publicly available data; 1, a capability stated in regulations or policy; 2, a partially established capability; 3, an institutionally supported capability; and 4, an established, redundant and practically tested capability. A score of zero does not demonstrate the absence of a capability, but rather the absence of sufficient open-source information.

$$C_i = (1 / m_i) \Sigma_j x_{ij} \quad (1)$$

where x_{ij} is the indicator score and m_i is the number of indicators in the respective group.

Scenario-specific weights are assigned to account for differences among the effects considered (Table 2).

Table 2: *Scenario-specific weighting coefficients*

Criterion	Nuclear	Chemical	Biological
C1	0.30	0.15	0.10
C2	0.30	0.20	0.20
C3	0.15	0.20	0.25
C4	0.15	0.25	0.20
C5	0.10	0.20	0.25

The scenario-specific weighting coefficients were assigned by the author on the basis of a comparative analysis of the characteristic effects and communication requirements associated with nuclear, chemical and biological threats. They are preliminary and subject to subsequent expert validation.

$$R_s = 25 \Sigma_i w_{is} C_i \quad (2)$$

where R_s is the resilience index for scenario s and w_{is} is the weight of the respective criterion. The result is expressed on a scale from 0 to 100. The methods applied include systems and comparative analysis, scenario analysis and multi-criteria assessment. Sensitivity is tested by varying each weight by ±10% and renormalising the remaining weights.

3 Comparative Pilot Application

The model is applied to publicly documented capabilities in the United States, the United Kingdom, France and Israel. The US system combines national planning, priority services, backup channels and multi-channel warning [7, 8]. In the United Kingdom, ResilienceDirect supports secure interagency information exchange, while the Emergency Services Network integrates voice, video and data services for emergency responders [9, 10].

France is developing the Réseau Radio du Futur as a common secure and priority communication environment, complemented by FR-Alert [11]. In Israel, the National Emergency Management Authority and Home Front Command provide coordination and geographically targeted warning used during actual threats [12, 13].

The aggregate criterion scores presented in Table 3 were derived from the technical, information-related and organisational capabilities identified in public sources. Each score was assigned by comparing the available evidence with the adopted 0–4 scale. The scores reflect the extent to which a given capability is publicly documented, rather than the full scope of the national communication systems.

Table 3: Aggregate scores by criterion

Country	**C1**	**C2**	**C3**	**C4**	**C5**
United States	4	3	4	4	4
United Kingdom	3	3	3	4	3
France	3	3	3	3	4
Israel	3	3	3	4	4

The resulting profiles reveal differences among the systems examined. For the United States, public sources support high scores for technical protection, information resilience, operational interoperability and warning capability. The score for redundancy and autonomy is lower because open sources do not permit the functional independence of all backup components to be established. The United Kingdom scores higher for operational interoperability, France for warning capability, while Israel demonstrates high scores for operational interoperability and warning mechanisms used in practice.

Table 4: Composite scores by scenario

Country	**Nuclear**	**Chemical**	**Biological**
United States	92.50	95.00	95.00
United Kingdom	78.75	81.25	80.00
France	77.50	80.00	81.25
Israel	81.25	86.25	86.25

$$R^{N}(USA) = 25(0.30\times4 + 0.30\times3 + 0.15\times4 + 0.15\times4 + 0.10\times4) = 92.50 \quad (3)$$

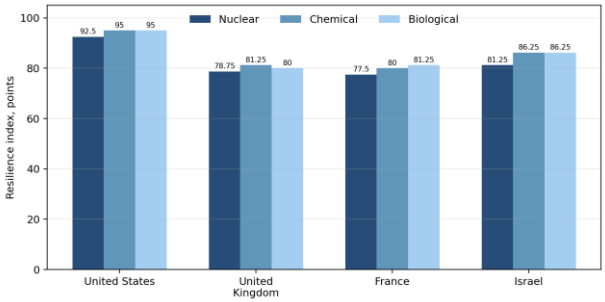


Figure 1: Comparative values of the resilience index by scenario

The higher values for the United States are explained by publicly documented capabilities across all assessed groups, including backup communication channels, autonomous support and multi-channel warning. Israel's results reflect well-developed timely warning mechanisms and the practical experience gained through their use. The close scores of the United Kingdom and France indicate a similar overall level of resilience achieved through different combinations of technical and organisational capabilities.

The sensitivity analysis indicates that varying the weighting coefficients within the adopted limits does not alter the overall ranking in the nuclear scenario. In the chemical and biological scenarios, the close values for the United Kingdom and France confirm that the composite index should not be interpreted in isolation, but together with the individual criterion scores and the available evidence for the respective capabilities.

4 Applicability of the Model Within the National Disaster Protection System

The proposed model can be used to assess the communication resilience of the structures participating in Bulgaria's Unified Rescue System under nuclear, chemical and biological threats. Its application is intended to determine their capacity to maintain critical information exchange during power disruption, congestion of public networks, physical damage to infrastructure or restricted access to affected areas [14, 15].

The assessment is conducted for a specific scenario, level of command and communication function. This makes it possible to account for differences in information-exchange requirements during a nuclear, chemical or biological incident. A communication capability sufficient for a local chemical incident may prove inadequate in cases of large-scale radiological contamination, prolonged power disruption or a slowly developing biological threat.

Practical application of the model involves defining the functions to be assessed, collecting evidence for the indicators, assigning criterion scores, applying the scenario-specific weights and calculating the composite index. The resulting value should be considered together with the profile of the individual criteria, because identical composite scores may conceal different technical and organisational weaknesses.

Particular attention should be paid to analysing dependencies between primary and backup assets. Two communication channels do not provide genuine redundancy when they share a power supply, base station, transmission line, data centre or identity-management system. The assessment should therefore consider the functional independence of the channels, rather than merely their number.

The results can support the prioritisation of technical modernisation, autonomous power supply, data protection, personnel training and joint exercises. Periodic application of the model makes it possible to track changes in resilience and assess the effects of implemented measures.

For the model to be used as a national instrument, its criteria, indicators and scenario-specific weights must be validated through a structured expert assessment and tested in command-post or field exercises. Until such validation is completed, the model should be regarded as a tool for comparative assessment and decision support, rather than a substitute for the operational judgement of the competent authorities.

The comparative pilot application shows that close composite scores do not imply an identical structure of communication resilience. Similar results may be achieved through different combinations of technical protection, redundancy and autonomy, information resilience, operational interoperability and warning capabilities. The composite index should therefore be considered together with the profile of the individual criterion scores.

The results show that an additional communication channel does not automatically ensure greater resilience. When the primary and backup channels share a power supply, transmission medium, data centre or identity-management system, a common point of failure arises. Functional independence is therefore a more meaningful indicator than the nominal number of communication assets.

Scenario-specific weighting enables the model to account for the different nature of nuclear, chemical and biological threats. The sensitivity analysis indicates that the results are relatively robust; nevertheless, the close scores of some countries confirm that the ranking depends on the selected weighting coefficients.

The principal limitation of the study is its reliance on publicly available information, which does not disclose all national capabilities and protected communication solutions. A further limitation arises from the author-defined criteria, initial scores and weighting coefficients. The next stage of the research should include expert validation and model testing through a scenario-based or command-post exercise.

Conclusion

Communication resilience under nuclear, chemical and biological threats results from the interaction of technical assets, power supply, information systems, procedures and personnel preparedness. A backup channel does not guarantee resilience when it depends on the same physical or information resource as the primary channel.

The developed model integrates heterogeneous characteristics into a common assessment framework and accounts for their varying significance across scenarios. The comparative pilot application shows that higher scores are achieved by systems combining independent channels, autonomous support, secure interagency information exchange and warning mechanisms tested in practice.

The proposed model can be applied to assess the ability of the structures within Bulgaria's Unified Rescue System to maintain the required information exchange under different CBRN scenarios. The research hypothesis is supported at the level of documentary and scenario-based pilot application; the next stage is expert and practical validation of the model.

References

1. Federal Emergency Management Agency. (2022). Planning guidance for response to a nuclear detonation (3rd ed.). https://www.fema.gov/sites/default/files/documents/fema_nuc-detonation-planning-guide.pdf
2. North Atlantic Treaty Organization. (2024). Resilience, civil preparedness. Article 3.

3. National Institute of Standards and Technology. (2015). Community resilience planning guide for buildings and infrastructure systems (NIST Special Publication 1190). https://doi.org/10.6028/NIST.SP.1190v1
4. Cybersecurity and Infrastructure Security Agency. (n.d.). Emergency communications. U.S. Department of Homeland Security. https://www.cisa.gov/topics/emergency-communications
5. Federal Emergency Management Agency. (2020). Hazardous materials incidents: Guidance for state, local, tribal, territorial, and private sector partners.
6. World Health Organization. (2017). Communicating risk in public health emergencies: A WHO guideline for emergency risk communication policy and practice. https://iris.who.int/handle/10665/259807
7. Cybersecurity and Infrastructure Security Agency. (n.d.). National emergency communications plan. U.S. Department of Homeland Security.
8. Federal Emergency Management Agency. (2023). Emergency Alert System and Integrated Public Alert and Warning System.
9. Cabinet Office. (2025). Resilient communications. GOV.UK. https://www.gov.uk/guidance/resilient-communications
10. UK Home Office. (2025). Emergency Services Network: Overview.
11. Agence des communications mobiles opérationnelles de sécurité et de secours. (n.d.). Le Réseau Radio du Futur.
12. Israel Ministry of Defense. (n.d.). National Emergency Management Authority.
13. Israel Home Front Command. (n.d.). Emergency warning services and guidelines.
14. Republic of Bulgaria. (2006). Disaster Protection Act. State Gazette No. 102 of 19 December 2006, as subsequently amended and supplemented.
15. Fire Safety and Civil Protection Directorate General. (n.d.). National Early Warning and Notification System and BG-ALERT.

AUTOMATED QUALITY CONTROL SYSTEMS FOR WATER HEATING APPLIANCES

Aleksandra P. Docheva[1], Daniel R. Denev[2]

Faculty of Technical Sciences, Department of Communication and Computer Engineering and Security Technologies, Konstantin Preslavsky University of Shumen, Shumen, Bulgaria, [1]alexa_do4ka@abv.bg, [2]d.denev@shu.bg

***Abstract**: Automated quality control systems play an important role in the modern production of water heaters. They ensure reliability, safety and high quality of the final products through the use of sensors, programmable controllers and specialized software for monitoring and analysis. This report examines the principles of operation of automated quality control systems, the main methods for testing water heaters, the technologies used and the advantages of their implementation in the production process.*

***Keywords**: Quality control, Automation, Industry*

АВТОМАТИЗИРАНИ СИСТЕМИ ЗА КОНТРОЛ НА КАЧЕСТВОТО НА ВОДОНАГРЕВАТЕЛНИ УРЕДИ

Александра П. Дочева[1], Даниел Р. Денев[2]

Факултет по технически науки, катедра „Комуникационна и компютърна техника и технологии за сигурност“, Шуменски университет „Епископ Константин Преславски“, гр. Шумен, България, [1]alexa_do4ka@abv.bg, [2]d.denev@shu.bg

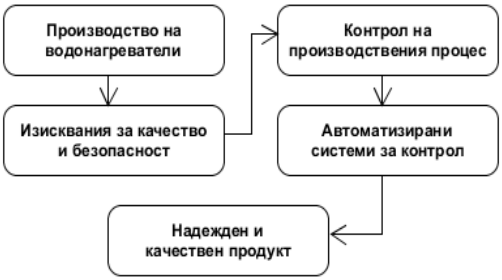
***Резюме**: Автоматизираните системи за контрол на качеството играят важна роля в съвременното производство на водонагревателни уреди. Те осигуряват надеждност, безопасност и високо качество на крайните продукти чрез използване на сензори, програмируеми контролери и специализиран софтуер за мониторинг и анализ. В настоящия доклад са разгледани принципите на работа на автоматизираните системи за контрол на качеството, основните методи за изпитване на водонагревателни уреди, използваните технологии и предимствата от тяхното внедряване в производствения процес.*

***Ключови думи**: Контрол на качеството, Автоматизация, Индустрия*

Въведение

Контролът на качеството е съществен елемент от производството на електрически и топлотехнически уреди. Водонагревателните уреди работят едновременно с електричество и вода, поради което към тях се поставят високи изисквания за безопасност, енергийна ефективност и надеждност [9]. С развитието на индустриалната автоматизация ръчният контрол постепенно се заменя от автоматизирани системи, които осигуряват по-висока точност, бърза обработка на данните и по-малко човешки грешки. Те извършват множество измервания, откриват отклонения още в ранните етапи и позволяват своевременни коригиращи

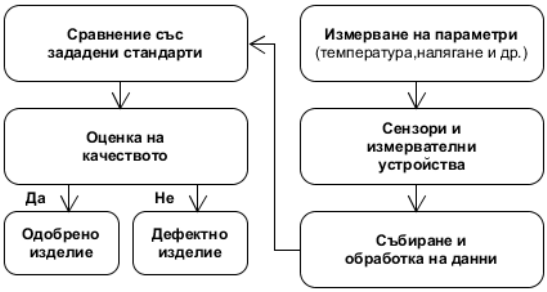
действия [8]. Непрекъснатото наблюдение гарантира съответствие със стандартите и повишава конкурентоспособността на предприятията. На фиг. 1 е показана ролята на автоматизацията в производството [4].



Фиг. 1: Роля на автоматизацията в производството

Същност на автоматизираните системи за контрол на качеството

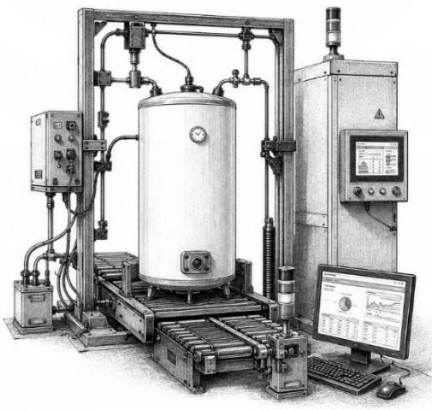
Автоматизираните системи за контрол на качеството представляват комплекс от хардуерни и софтуерни средства, предназначени за наблюдение, измерване и оценка на характеристиките на произвежданите изделия. При производството на водонагревателни уреди тези системи следят различни параметри като температура, налягане, електрическа изолация и херметичност. Получените данни се обработват автоматично, което позволява бързо откриване на отклонения и дефекти. Автоматизираните системи за контрол на качеството функционират на принципа на непрекъснатото събиране и анализ на информация от производствения процес. Те сравняват измерените стойности с предварително зададени стандарти и автоматично сигнализират при наличие на отклонения. По този начин се гарантира, че всяко изделие отговаря на техническите изисквания преди да бъде пуснато на пазара. Съвременните системи могат да извършват контрол както по време на производството, така и след завършването на изделието. Това позволява ранно откриване на дефекти и предотвратява натрупването на производствени грешки. В резултат се подобрява качеството на продукцията и се намаляват разходите за последващи ремонти и корекции. Автоматизираният контрол също така осигурява висока степен на обективност при оценяването на качеството. За разлика от ръчните проверки, които могат да бъдат повлияни от човешкия фактор, автоматизираните системи работят по едни и същи критерии при всяко измерване. На фиг. 2 е показан принципът на работа. [1]



Фиг. 2: Принцип на работа

Основни компоненти на системите

Ефективността на автоматизирания контрол зависи от използваните технически средства. Основните компоненти включват измервателни сензори, програмируеми логически контролери (PLC), комуникационни модули и специализиран софтуер. Сензорите измерват температурата, налягането и други физически параметри, а контролерите обработват получените данни и вземат решения в реално време [10]. Софтуерът визуализира резултатите и съхранява информация за качеството на всяко изделие. Комуникационните модули осигуряват обмен на данни между устройствата и централната система за управление. Чрез баркодове или RFID технологии се осигурява проследимост на изделията през целия производствен цикъл [2]. На фиг. 3 е показана автоматизирана изпитвателна станция за контрол на качеството на водонагревателни уреди.



Фиг. 3: Автоматизирана изпитвателна станция за контрол на качеството на водонагревателни уреди

Методи за изпитване на водонагревателни уреди

Контролът на качеството включва различни видове изпитвания. Сред най-често използваните са тестове за електрическа безопасност, проверка на изолационното съпротивление, изпитване на нагревателните елементи и тестове за устойчивост на налягане. Автоматизираните стендове извършват тези проверки без необходимост от постоянна човешка намеса, като резултатите се записват и анализират автоматично. Освен стандартните електрически тестове, водонагревателните уреди преминават и изпитвания за енергийна ефективност. При тях се измерва количеството електроенергия, необходимо за загряване на определен обем вода. Резултатите са важни както за производителя, така и за крайните потребители. Друг важен метод е проверката на работата на термостатите и защитните устройства. Тези компоненти трябва да реагират коректно при достигане на зададените температурни граници. Автоматизираните тестови станции симулират различни експлоатационни условия и проверяват тяхната надеждност. Използват се и тестове за дълготрайност, при които уредите се подлагат на многократни цикли на нагряване и охлаждане. Целта е да се оцени устойчивостта на материалите и компонентите при продължителна експлоатация. Таблица 1 и таблица 2 показват методи и параметри. [3]

Таблица 1: Основни методи за изпитване на водонагревателни уреди

Метод на изпитване	Контролиран параметър	Цел на изпитването	Очакван резултат
Тест за херметичност	Течове на вода	Проверка на плътността на съда и връзките	Липса на течове
Тест за налягане	Работно налягане	Проверка на устойчивостта на водосъдържателя	Без деформации и повреди
Тест за електрическа безопасност	Изолационно съпротивление	Защита от токов удар	Стойности в допустимите граници
Проверка на нагревателния елемент	Мощност и консумация	Контрол на ефективността на нагряване	Номинална мощност
Проверка на термостата	Температура на изключване	Осигуряване на правилен температурен режим	Коректно сработване
Тест на защитните устройства	Аварийно изключване	Защита при прегряване	Надеждно прекъсване на захранването
Изпитване на енергийна ефективност	Разход на електроенергия	Оценка на икономичността	Съответствие със стандарта
Визуална инспекция	Външен вид и монтаж	Откриване на механични дефекти	Без видими дефекти

Предимства на автоматизацията в производството

Внедряването на автоматизирани системи за контрол на качеството води до значително повишаване на производителността. Намалява се вероятността от човешки грешки и се подобрява точността на измерванията. Освен това се съкращава времето за инспекция на продуктите и се намаляват разходите, свързани с бракуване и рекламации. Автоматизацията също така позволява проследимост на производствения процес и съхранение на информация за всеки произведен уред. Автоматизацията допринася за по-добро използване на производствените ресурси. Чрез постоянно наблюдение на процесите се намаляват престоят на машините и времето за диагностика на възникнали неизправности. Това води до по-висока производителност и по-добра организация на работата. Друго съществено предимство е възможността за работа в непрекъснат режим. Автоматизираните системи могат да извършват контролни операции денонощно без намаляване на точността и качеството на измерванията. Това е особено важно при големи производствени обеми. Събраната информация позволява извършването на статистически анализи на качеството [7]. Производителите могат да идентифицират най-често срещаните дефекти и да предприемат мерки за тяхното отстраняване още в началните етапи на производството. [6]

Таблица 2: Параметри измервани от автоматизираната система за контрол

Измерван параметър	Използван сензор	Допустим диапазон	Вид контрол
Температура на водата	Температурен датчик	$50 - 75\ °C$	Автоматичен
Налягане в резервоара	Сензор за налягане	$0.6 - 1.0\ MPa$	Автоматичен
Изолационно съпротивление	Измервателен модул	$>\ 2\ M\Omega$	Автоматичен
Консумирана мощност	Електроизмервателен модул	$\pm 5\%$ от номиналната	Автоматичен
Време за загряване	Софтуерен таймер	Според техническата спецификация	Автоматичен
Наличие на течове	Датчик за течове	0 течове	Автоматичен
Работа на термостата	Температурен контролер	Сработване при зададена температура	Автоматичен

Бъдещи тенденции и развитие

Развитието на технологиите води до все по-широко използване на изкуствен интелект, машинно обучение и Интернет на нещата (IoT) в системите за контрол на качеството. Чрез анализ на големи обеми данни могат да се предвиждат потенциални повреди и да се оптимизира производственият процес. Очаква се бъдещите системи да бъдат още по-интелигентни, автономни и способни да извършват самодиагностика и автоматична корекция на откритите отклонения. Все по-голямо приложение намират облачните технологии, които позволяват съхранение и анализ на данни от различни производствени обекти в единна информационна среда. Това улеснява управлението на качеството в предприятия с

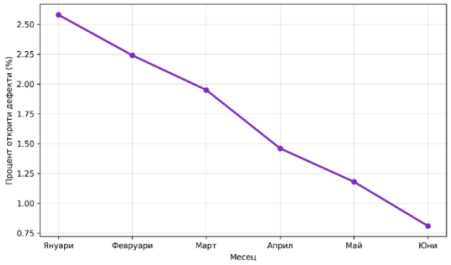
множество производствени линии или заводи. Развитието на цифровите двойници (Digital Twin) също предлага нови възможности. Чрез създаване на виртуален модел на водонагревателния уред производителите могат да симулират различни режими на работа и да откриват потенциални проблеми още преди реалното производство.

Внедряване на интелигентна система за контрол

В производствена линия за водонагреватели TESY е внедрена интелигентна система за контрол на качеството, използваща машинно зрение и алгоритми за анализ на данни. В продължение на шест месеца се проследява броят на дефектите, открити преди напускане на производството (таблица 3 и фиг. 5). Една от най-перспективните тенденции в развитието на автоматизираните системи за контрол на качеството е внедряването на предиктивна поддръжка. Този подход използва данни от сензори и интелигентни алгоритми за анализ на състоянието на оборудването, което позволява ранно откриване на потенциални неизправности и предотвратяване на непланирани спирания на производството. За да се оцени ефективността на внедрената предиктивна поддръжка, е извършен анализ на производствена линия за водонагревателни уреди. Проследени са непланираните спирания на оборудването в рамките на една година след внедряването на интелигентна система за наблюдение и диагностика. Получените резултати са представени в таблица 4 и на фиг. 6 и фиг. 7.

Таблица 3: Резултати от внедряване на интелигентна система

Месец	Проверени уреди	Открити дефекти	Процент открити дефекти (%)
Януари	1200	31	2.58
Февруари	1250	28	2.24
Март	1180	23	1.95
Април	1300	19	1.46
Май	1270	15	1.18
Юни	1350	11	0.81

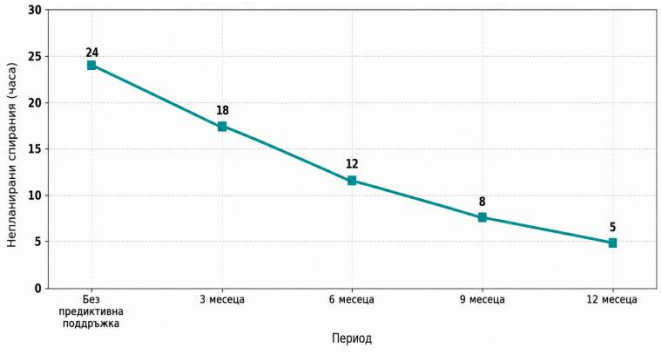


Фиг. 5: Намаляване на дефектите след внедряване на интелигентна система

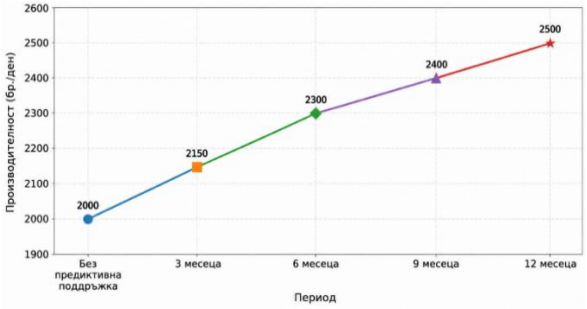
Получените резултати показват ясно и последователно намаляване на непланираните спирания след внедряването на системата за предиктивна поддръжка. В началния етап на изследването общото време на престой възлиза на 24 часа, докато след дванадесет месеца то намалява до едва 5 часа. Това представлява редукция с приблизително 79%, което е показател за високата ефективност на използваните алгоритми за прогнозиране и ранно откриване на неизправности.

Таблица 4: Резултати от внедряване на предиктивната поддръжка

Период	Непланирани спирания (часа)	Производителност (бр./ден)
Без предиктивна поддръжка	24	2000
След 3 месеца	18	2150
След 6 месеца	12	2300
След 9 месеца	8	2400
След 12 месеца	5	2500



Фиг. 6: Намаляване на непланираните спирания след внедряване на предиктивна поддръжка



Фиг. 7: Увеличение на производителноста след внедряване на предиктивна поддръжка

Съществото намаляване на престоите оказва пряко и значително влияние върху производителността на производствената линия. В началото производителността е около 2000 броя на ден, като след внедряването на предиктивната поддръжка се наблюдава устойчив ръст, достигащ до 2500 броя на ден след дванадесетия месец. Това представлява увеличение от приблизително 25%, което потвърждава пряката зависимост между намаляването на престои и повишаването на производствения капацитет. Подобрението се дължи на възможността за своевременно идентифициране на потенциални повреди и планиране на ремонтни дейности в подходящ момент, без да се нарушава производственият процес. По този начин се избягват аварийни спирания, оптимизира се използването на оборудването и се намаляват разходите, свързани с поддръжката и загубите от непродуктивно време. В заключение, получените резултати потвърждават, че предиктивната поддръжка представлява ключов фактор за повишаване на ефективността и надеждността на съвременните производствени системи. [5]

Заключение

Автоматизираните системи за контрол на качеството са неразделна част от съвременното производство на водонагревателни уреди. Те осигуряват висока точност, надеждност и безопасност на крайните продукти, като същевременно повишават ефективността на производствения процес. Благодарение на развитието на автоматизацията и цифровите технологии предприятията могат да поддържат високи стандарти за качество и да отговарят на нарастващите изисквания на потребителите. В бъдеще интегрирането на интелигентни технологии ще направи тези системи още по-ефективни и ще допринесе за по-висока конкурентоспособност на производителите. Използването на автоматизирани системи за контрол на качеството позволява значително намаляване на производствените рискове и повишаване на надеждността на водонагревателните уреди. Благодарение на непрекъснатото наблюдение и анализ на технологичните процеси се осигурява високо ниво на контрол върху всеки етап от производството [11]. Това води до по-малък процент дефектни изделия и по-високо доверие от страна на потребителите. Автоматизацията създава възможност за по-ефективно използване на човешките и материалните ресурси.

Литература

1. Yu, J., Fu, J., Guo, F., & Xie, Y. (2018). Automatic testing system to evaluate the energy efficiency of electric storage water heaters. Measurement and Control, 51(7–8), 223–234.
2. Semitela, Â., Ferreira, A., Completo, A., Lau, N., & Santos, J. P. (2026). Detecting and classifying defects on the surface of water heaters: Development of an automated system. Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture, 240(2), 1859–1869.

3. Tušek, J., Bajcer, B., & Kampuš, Z. (2004). On line leak testing of welded water heaters. Journal of Materials Processing Technology, 155–156, 1164–1170.
4. Healy, W. M. (2017). The dependence of water heater energy factor on deviations from nominal test conditions. ASHRAE Transactions, 123(2).
5. Peres, R. S., Jia, X., Lee, J., Sun, K., & Colombo, A. W. (2020). Industrial artificial intelligence in Industry 4.0: Systematic review, challenges and outlook. IEEE Access, 8, 220121–220139.
6. Sekar, R., Hsieh, S. J., & Wu, Z. (2013). Remote diagnosis design for a PLC-based automated system: Evaluation of factors affecting remote diagnosis performance. International Journal of Advanced Manufacturing Technology, 65(5–8), 1091–1109.
7. Тодорова-Лазарова, В. П. (2025). Dynamic arrays in MS Excel for data processing and analysis in information systems. Proceedings of the International Scientific Conference UNITECH 2025, Gabrovo, 1–6. ISSN 1313-230X.
8. Arabadzhieva-Kalcheva, N., & Tsankov, Ts. (2022). Failure Modes and Effects Analysis – FMEA. Proceedings of the Scientific Conference with International Participation MATTEH 2022, 2, Shumen, 58–62. ISSN 1314-3921.
9. Arabadzhieva-Kalcheva, N., Tsankov, Ts., & Todorova, M. (2024). Cause-consequence analysis as a risk management method. Annual of Konstantin Preslavsky University of Shumen, XIV E, Faculty of Technical Sciences, 184–188. ISSN 1314-8818. https://doi.org/10.46687/YT24NEL
10. Ahmedov, I., Chirakov, D., & Tsankov, Ts. (2018). Inspection of automotive controllers for stability via communication systems with specialized diagnostic software. Journal of Physics and Technology, Plovdiv: Plovdiv University Press "Paisii Hilendarski", 52–55. ISSN 2535-0536.
11. Simeonova, I., & Metodieva, Ts. (2024). Model for administrative security management in a municipality. Journal Scientific and Applied Research, 26(1). Shumen: Konstantin Preslavsky University Press. ISSN 1314-6289.

A METHOD FOR OPTIMIZING COMBINED USE OF UNMANNED AERIAL SYSTEMS AND ARTILLERY FORMATIONS TO ENGAGE TARGETS IN CONTEMPORARY ARMED CONFLICTS

Ivelin G. Katsev

Faculty of Artillery, Air Defense and Communication and Information Systems, National Military University, Shumen, Bulgaria, katsev.i@abv.bg

***Abstract**: Contemporary military and armed conflicts reveal the significant use of unmanned aerial vehicles to perform combat tasks by military units, which raises the need to analyze the combined use of unmanned aerial systems and artillery weapons to ensure higher efficiency in performing tasks during the process of fire destruction of enemy target in limited resources conditions.*

***Keywords**: Operations research (OR), unmanned aerial systems (UAS), artillery, optimization, efficiency.*

Introduction

Contemporary armed conflicts in Europe and Middle East can be characterized by significant and dynamic changes in the way combat operations and tactical actions are conducted, predetermining the role of technological superiority, making it a key factor in achieving military objectives, in which the use of high-tech means of remote impact prevails over direct physical confrontation between opposing forces.

The development of information technologies, unmanned aerial systems, high-precision weapons, electronic warfare means, space systems and artificial intelligence change operational domains and confirm the leading position of high-tech means used by military formations in performing tasks in all operational areas for conducting armed conflicts.

Of particular importance is the reduction of the time between the detection of targets for impact and their destruction. Modern intelligence means allow information to be obtained practically in real time, while digital communication systems ensure its rapid transmission to command posts and firepower units.

Unmanned aerial systems occupy a central place in this so-called digital transformation of the battlefield, they perform a wide range of tasks - reconnaissance, surveillance, target designation, fire correction and assessment of the results of the impact. Along with them, the development of loitering munitions and FPV strike unmanned systems creates new opportunities for influencing the enemy at a relatively low cost and limited risk to personnel. This leads to a change in the ratio of the use of traditional weapon systems and new technological means.

This study examines the technological transformation of modern military conflicts, with the emphasis placed on the role of unmanned aerial systems, information superiority and their interaction with traditional artillery firepower. The main goal is to investigate how the integration of modern technologies into a single reconnaissance and strike

system affects the effectiveness of military operations and how different options for using available resources can be assessed through mathematical models.

- **Fundamentals of the use of autonomous systems in the military sphere**

The progress in the development of artificial intelligence (AI) and its comprehensive implementation in the military sphere, both in the development of new weapons and in the further development and improvement of existing ones, is increasingly influencing the way military operations are conducted and particularly the combat operations within them. With the increasing capabilities of artificial intelligence, through the use of machine learning, deep learning, neural networks, reinforcement learning and others, AI is becoming established as a powerful instrument for increasing the capabilities for collecting, processing, storing and analyzing all types of data to support the decision-making process, by providing high quality and precision when processing a significant amount of information (big data).

The applications of artificial intelligence in the military sphere can be summarized in the following areas:

- Autonomous weapons systems;
- Intelligence and surveillance;
- Cybersecurity;
- Logistics;
- Training and simulations.

Taking advantage of the benefits of implementing artificial intelligence in armed forces, it is guaranteed to increase the capabilities of military formations, having a significant positive impact on the imperatives of capabilities (doctrines - organizational structure - training - material resources - personnel - leadership - infrastructure - interoperability) to ensure the achievement of joint functions of components in the joint forces.

The development of artificial intelligence and its implementation in unmanned vehicles provides greater intensity in the performance of tasks and the ability to act in any tactical situation without the need for additional communication with ground station or operator of unmanned system. Such platforms belong to autonomous weapon systems. Their capabilities for combat use affect the area for conducting armed conflict in a stochastic and non-entropic manner, creating a high level of uncertainty through the threat of use and the presence of a high risk to personnel and combat equipment due to the low ability to prevent the use of autonomous weapon systems, both for reconnaissance and for strike purposes.

- **Basics of operations research in the military sphere.**

Operations Research (OR) is a scientific approach to supporting decision-making through the use of mathematical models, statistical methods, optimization, simulation, analysis of various alternatives and other methods.

The main idea is to represent the real system through a mathematical model that allows its behavior to be studied without the need to carry out the real process.

The processes of modeling, simulations, wargaming and analysis of alternatives in NATO are defined as tools for Operations Research and Analysis.

Basic elements of OR:

- objective function – what we want to maximize or minimize;
- controllable variables – the decisions we can make;
- constraints – the available resources and physical/operational limitations;
- parameters – characteristics of the system;
- uncertainty – random or unknown factors;
- evaluation criteria – by which we compare solutions.

In a military context, the objective function can be related to:

- maximizing efficiency;
- minimizing resource consumption;
- minimizing time;
- minimizing risk;
- maximizing the probability of completing the task.

➢ **Optimization method for distributing targets between artillery units and unmanned aerial systems units.**

The method is based on optimization to achieve maximum efficiency of the remote impact group on the one hand, and on the other hand, to use a minimum number of resources to achieve effective destruction of all targets in the group.

The targets to be destroyed are grouped into four groups and are presented in Table No. 1, while the ammunition consumption for the different types of targets is presented in Table No. 2. In addition, the available amount of ammunition for the artillery systems and the resource of barrage ammunition, as well as their relative values, are presented in Table No. 3. Also, the relative probability of striking is presented in Table No. 4. The artillery formations are represented by the designation A, B, C and D, while the unmanned aerial systems formation is designated E.

Table 1. Distribution of targets by groups.

Target group	№1 area targets with high fortification	№2 area targets with low fortification	№3 unitary targets with low mobility	№4 unitary targets with high mobility
amount	10	50	30	20

Table 2. Number of shells and loitering ammunition by target groups to be destroyed, number

	target group №1	target group №2	target group №3	target group №4
unit A	40	120	40	80
unit B	50	150	50	100
unit C	30	100	30	60
unit D	20	40	40	40
unit E (UAS)	30	20	2	3

Table 3. Allocated quantity of shells for the fire units and loitering ammunition for the UAS formation.

	target group №1	target group №2	target group №3	target group №4
amount	1200	1800	1000	2400
cost	500	600	1300	2500

Table 4. Relative probability of striking targets within groups by artillery formations and UAS formations.

	target group №1	target group №2	target group №3	target group №4
unit A	20%	25%	25%	10%
unit B	15%	30%	10%	5%
unit C	30%	25%	20%	10%
unit D	10%	30%	10%	5%
unit E (UAS)	10%	15%	80%	60%

To solve the optimization tasks, the use integer linear optimization without time constraints is needed by following formulas:

1. In order to achieve maximum relative effectiveness in striking targets:

1. $max\,\psi = max \sum_{i=1}^{n} \sum_{j=1}^{m} e_{ij} x_{ij}$, under:

2. $\sum_{i=1}^{n} x_{ij} \le R_j$

where:

ψ – objective function for finding the maximum effectiveness in hitting the targets for impact;

e_{ij} – effectiveness of the impact of the formations on the target groups, reflected by the probability of hitting;

x_{ij} – number of tasks from group j, assigned to performer i;

R_j – maximum number of available resources.

2. To minimized the consumption of resources used when strike all targets:

3. $min\,\chi = min \sum_{i=1}^{n} \sum_{j=1}^{m} r_{ij} x_{ij}$, under:

4. $\sum_{j=1}^{m} r_{ij} x_{ij} = D_j$,

where:

χ – objective function for finding the minimum consumption of resources used to strike all targets;

r_{ij} –amount of ammunition or loitering ammunition to hit one target;

D_j –total number of targets for impact;

The constraints that are introduced in task are as follows:

5. $r_{11}x_1+r_{12}x_2+r_{13}x_3+r_{14}x_4 \le b_1=1200;$
6. $r_{21}x_1+r_{22}x_2+r_{23}x_3+r_{24}x_4 \le b_2=1800;$
7. $r_{31}x_1+r_{32}x_2+r_{33}x_3+r_{34}x_4 \le b_3=1000;$
8. $r_{41}x_1+r_{42}x_2+r_{43}x_3+r_{44}x_4 \le b_4=2400;$
9. $r_{51}x_1+r_{52}x_2+r_{53}x_3+r_{54}x_4 \le b_5=100;$
10. $e_{11}x_1+e_{21}x_1+e_{31}x_1+e_{41}x_1+e_{51}x_1 \le d_1=10;$
11. $e_{12}x_2+e_{22}x_2+e_{32}x_2+e_{42}x_2+e_{52}x_2 \le d_2=50$
12. $e_{13}x_3+e_{23}x_3+e_{33}x_3+e_{43}x_3+e_{53}x_3 \le d_3=30;$
13. $e_{14}x_4+e_{24}x_4+e_{34}x_4+e_{44}x_4+e_{54}x_4 \le d_4=20;$
14. $e_{i,j},\ r_{i,j},\ x_n \ge 0,$

where:

$r_{1\text{-}5'1\text{-}5'}$ – consumption of shells and loitering ammunition for formations to strike the target groups;

$e_{1\text{-}5'1\text{-}5'}$ – Probability of hitting the target groups by the artillery formations and the UAV formation;

$b_{1\text{-}5}$ – availability of shells in artillery formations and loitering ammunition;

$d_{1\text{-}4}$ – total number of targets to strike;

$x_{1\text{-}4}$ – number of hit targets from group No. 1, 2, 3 and 4.

To solve the tasks, the "Optimization Toolbox" function of the "MATLAB" software product was used. The results for achieving maximum effectiveness $(max\psi)$ are presented in tables № 5 and, 6, while the results for efficiency in performing all tasks and the minimum consumption resources $(min\chi)$ are presented in tables № 7 and 8.

I. The determination of maximum relative effectiveness for striking targets is as follows:

15. $max\psi = max\sum_{i=1}^{n}\sum_{j=1}^{m} e_{ij}x_i = e_{11}x_1+e_{21}x_1+e_{31}x_1+e_{41}x_1+e_{51}x_1+e_{12}x_2+e_{22}x_2+e_{32}x_2+e_{42}x_2+e_{52}x_2+e_{13}x_3+e_{23}x_3+e_{33}x_3+e_{43}x_3+e_{53}x_3+e_{14}x_4+e_{24}x_4+e_{34}x_4+e_{44}x_4+e_{54}x_4 = 7*0.1+12*0.3+10*0.3+38*0.3+30*0.8+13*0.6 = 50.5$

Determining the resources spent to achieve maximum effectiveness in striking groups of targets.

16. $\chi = \sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}x_{ij} = 280000+1080000+390000+3800000+445500 = 5\ 995\ 500$

Table 5. Weapon- target distribution to achieve maximum effectiveness.

	target group №1	target group №2	target group №3	target group №4	Total tasks per unit
unit A	-	-	-	7	7
unit B	-	12	-	-	12
unit C	10	-	-	-	10
unit D	-	38	-	-	38
unit E (UAS)	-	-	30	13	43
Total	20	50	30	20	110

Table 5 reveals that the distribution of targets for maximum effectiveness in destruction leads to the mass use of formations whose effectiveness is of greater value for different types of targets. Here we can distinguish that all formations, except for formation A, perform tasks on targets that have the highest probability of striking.

Table 6. Amount of artillery shells and loitering munitions used to achieve the highest efficiency.

	unit A	unit B	unit C	unit D	unit E (UAS)
target group №1	-	-	300	-	-
target group №2	-	1800	-	1520	-
target group №3	-	-	-	-	60
target group №4	560	-	-	-	39
Total Consumption of resources, n	560	1800	300	1520	99
Consumption of resources, %	47%	100%	30%	63%	99%
Total cost of consumed resources	280000	1080000	390000	3800000	450000
Remainder of resources, n	640	0	700	880	1
Remainder of resources, %	53%	0%	70%	37%	1%

Table No. 6 reveals that out of 6500 allocated resources, 4279 were spent, which is about 66% of the resources spent to destroy 110 targets. Also, the value of the resources spent is 5,995,500 out of a maximum of 9,430,000, which is 64%. In addition, almost all of the resources of formations B and E were spent, which can be used to determine the need to allocate larger amounts of ammunition and loitering ammunition to these formations.

II. Determining the efficiency in performing all tasks and the minimum value of the number of resources used $(min\,\chi)$ is performed as follows:

17. $$\psi = \sum_{i=1}^{n}\sum_{j=1}^{m} e_{ij}x_{ij} = 10*0.25+12*0.3+10*0.3+10*0,2+28*0.3+20*0.8+20*0.6 = 47.5$$

Determining the resources spent to achieve maximum effectiveness in striking groups of targets.

18. $$min\,\chi = min\sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}x_{ij} = 600000+1080000+780000+2800000+450000 = 5710000$$

Table 7. Weapon-target distribution.

	target group №1	target group №2	target group №3	target group №4	Total tasks per unit
unit A	-	10	-	-	10
unit B	-	12	-	-	12
unit C	10	-	10	-	20
unit D	-	28	-	-	28
unit E (UAS)	-	-	20	20	40
Total	20	50	30	20	110

From Table No. 7 it can be summarized that Formation E (UAS) is mainly used to engage targets from groups No. 3 and 4, while Formations A, B and D are only used to engage targets from group No. 2. In this case, Formation B is used most flexibly.

Table 8. Amount consumed artillery shells and loitering munitions.

	unit A	unit B	unit C	unit D	unit E (UAS)
target group №1	-	-	300	-	-
target group №2	1200	1800	-	1120	-
target group №3	-	-	300	-	40
target group №4		-	-	-	60
Total Consumption of resources, n	1200	1800	600	1120	100
Consumption of resources, %	100%	100%	60%	47%	100%
Total cost of consumed resources	600000	1080000	780000	2800000	445500
Remainder of resources, n	0	0	400	1280	0
Remainder of resources, %	0%	0%	40%	53%	0%

Table 8 reveals that out of 6500 allocated resources, 4820 were spent, which is about 74% of the resources spent to strike 110 targets. Also, the value of the resources spent is 5,710,000 out of a maximum of 9,430,000, which is 61%. In addition, all resources of

formations A, B and E were spent, which can be used to determine the need to allocate larger amounts of ammunition and loitering munitions to these formations.

Analysis of the results of the analytical study shows that with the test data set in this way, combined use of artillery formations and UAV formations is obtained for striking targets, and in both cases of optimization, the use of almost entire resource of the UAV formation is observed, combined with a diverse use of artillery formations depending on whether we aim to achieve maximum effectiveness in destruction or a minimum value of the amount of ammunition consumed. There is also a clear distinction between the use of UAV formations for striking only unitary targets, where they are most effective, while artillery formations remain most effective for destruction of area targets.

The comparative analysis of the two optimization tasks – to achieve maximum efficiency in hitting the targets for impact and to determine the minimum value of the amount of resources used for striking the targets, with the test data set in this way, leads to the conclusion that in the first case about 66% of the number of available resources are used, which in value corresponds to 64% of the total value of the allocated resources, while in the second case about 74% of the number of available resources are used, which in value corresponds to 61% of the total value of the allocated resources, or we have the use of 8% more resources, which are 3% lower in value.

When determining the conditional efficiency of destruction in the first case we have 50.5 relative effectiveness, while in the second 47.5, which is about 6% lower effectiveness when using 8% more resources with only 3% lower value.

The study reveals the relationship between mathematical models and the planning and conduct of modern military operations, revealing that by using optimization of the distribution of targets for impact, resources and weapon systems, the effectiveness is increased when using separately mainly remote fire impact means, creating a synergistic effect when using them together to hit targets after optimization of the distribution of targets by executors taking into account the commander's intention and the limitations in the operational environment.

The combination of the analyses shows that the armed forces of the countries have moved from using unmanned systems as supporting intelligence assets to using them as the core of a networked, data-driven concept of multi-domain operations. This so-called "transformation" provides one of the clearest contemporary examples of how the principles of military research – optimization, decision analysis, resource allocation and operational effectiveness assessment – can be applied in real combat conditions to generate disproportionate strategic advantages.

Conclusion

By synthesizing the analyses of the most famous world organizations that analyze military conflicts, it can be formulated that final findings relative to the establishment of unmanned systems as a major part of the architecture of the future battlespace, and not only as its complement, but as evidenced by the unprecedented in its scale and duration empirical testing in conditions of intense conflicts, both in Ukraine and in the Middle East.

These platforms are not just a complement to existing combat systems — they are a catalyst for a qualitative change in the way multi-domain operations are planned and conducted. The ability of UAS to operate simultaneously on land, sea, air, cyber, space and the electromagnetic spectrum make them an integrating element of the multi-domain concept for conducting modern operations.

It can be summarized that technological innovations in unmanned systems follow three common development vectors:

- increasing autonomy (from remotely controlled to semi-autonomous and autonomous platforms);
- modularity and scalability (from specialized expensive systems to universal low-cost platforms with interchangeable payloads);
- network integration (from isolated platforms to interconnected ecosystems with a common, recognizable picture of the battlespace).

States and their armed forces that have managed to integrate all three categories into a networked, multi-domain system with a short innovation cycle and sufficient production scale will have a decisive operational advantage in military and armed conflicts in the 21st century.

References:

1. Ahuja R., Kumar A., Jha K., Orlin, J., Exact and Heuristic algorithms for the Weapon-Target assignment problem, Operations research, Vol. 55, No. 6, 2007, ISSN: 0030-364X. https://doi.org/10.1287/opre.1070.0511.
2. Bozov, I., Order of performance tasks by unmanned aircraft systems to artillery formations, International Scientific Conference ―Defense Technologies‖ "DefTech" 2024, 2024, pp 167-172, ISSN 2367-7902.
3. Ding, Y., Kuang, M., Shi, H., Gao, J., Multi-UAV Cooperative Target Assignment Method Based on Reinforcement Learning, Drones, 2024, volume 8, issue 10, ISSN: 2504-446X. https://doi.org/10.3390/drones8100562.
4. Guangsheng, J., et al, A Survey of Intelligent Optimization Algorithms for Weapon Target Assignment (WTA) Problem, Management Science Informatization and Economic Innovation Development Conference (MSIEID), 2020, pp50-54, ISBN:978-1-6654-1541-5. DOI: 10.1109/MSIEID52046.2020.00017.
5. https://www.csis.org/analysis/combined-arms-warfare-and-unmanned-aircraft-systems.
6. https://www.csis.org/analysis/seven-contemporary-insights-state-ukraine-war
7. https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-conventional-warfighting-russias-invasion-ukraine-february-july-2022.
8. https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-ukraines-offensive-operations-2022-23.
9. https://www.rusi.org/explore-our-research/publications/insights-papers/emergent-approaches-combined-arms-manoeuvre-ukraine.

10. Iliev, K., Vladov, I., Criteria for classification of objects for destruction in Counterbattery fight, International Scientific Conference ―Defense Technologies‖ "DefTech" 2025, 2025, pp 579-583, ISSN 2815-4282
11. Jiangyi Y., et al, A multi-type target collaborative allocation method with temporal constraints, *Intelligent Systems with Applications*, Volume 30, 2026, Article 200665, ISSN:2667-3053. https://doi.org/10.1016/j.iswa.2026.200665.
12. Jinrui L., Guohua W., Ling W., A comprehensive survey of weapon target assignment problem: Model, algorithm, and application, Engineering Applications of Artificial Intelligence, Volume 137, Part B, 2024, Article 109212, ISSN: 0952-1976.
13. https://doi.org/10.1016/j.engappai.2024.109212

FIELD ARTILLERY SYSTEMS AND TECHNOLOGIES:ASSESSMENT OF CAPABILITIES AND TECHNOLOGICAL DEVELOPMENT

Ivan K. Vladov, Yavor Y. Valkov, Yuliadi P. Keranov

NMU "Vasil Levski" Faculty "Artillery , Air Defence, Communication and Information systems", Shumen, Shumen region, Bulgaria,
Ivankvladov@abv.bg; yavor.valkov@gmail.com; keranovuli@gmail.com

Abstract: *This paper presents weapons, technologies and logistics in Bulgarian field artillery, with a short comparison with German artillery. The purpose is not to provide a detailed technical study, but to discuss the main differences in equipment, technology and support. Bulgarian artillery still includes systems that originate from an older generation, while Germany operates modern 155 mm systems such as the Panzer howitzer 2000 and is developing newer artillery capabilities. Bulgaria has nevertheless begun to improve its reconnaissance and support capabilities, including the introduction of the ARTHUR Mod C counter-battery radar. The discussion suggests that the main difference is not only the age of individual weapons, but also the level of integration between weapons, reconnaissance, communications, ammunition and logistics.*

Keywords*: Bulgarian field artillery, German artillery, Panzer howitzer 2000, 2S1 Gvozdika, Arthur Mod C, Logistics.*

Introduction

Field artillery remains an important part of land forces because it provides long range fire support. However, modern artillery is no longer only a question of how powerful a gun's impact is. A useful artillery system also needs reconnaissance, communication, ammunition, transport, maintenance and trained personnel. This makes it reasonable to discuss Bulgarian artillery as a complete system and not only as a list of weapons.

When Bulgarian and German artillery are compared, one clear difference can be seen in the age and generation of the main weapon systems. Bulgaria continues to operate or support several Soviet-designed systems such as the 2S1 Gvozdika, D-20 and BM-21 Grad. Public Bulgarian documentation also shows that the 2S1 requires formal repair and technical support. At the same time, Bulgaria has started introducing newer reconnaissance technology. In December 2024, the 4th Artillery Regiment in Asenovgrad received an ARTHUR Mod C radar, described by the Land Forces as a new capability and as an initial step toward modernization.

Germany provides a useful comparison because the Bundeswehr's principal self-propelled artillery system is the 155 mm Panzer howitzer 2000. Official Bundeswehr information describes it as a standard artillery system and gives it a standard range of about 30 km, with longer ranges possible with extended-range ammunition. German artillery also places strong emphasis on observation, fire support teams, training and information exchange.

This comparison should not be understood as a claim that Bulgarian artillery has no useful capabilities. Older systems can remain operational when they are maintained and supplied with ammunition. The more important point is that they do not represent the

newest generation of field artillery when compared with systems such as the PzH 2000. The Bulgaria's modernization process is therefore better described as gradual rather than complete.

1. Weapons: bulgarian systems and the comparison with german self-propelled artillery

One of the most recognizable Bulgarian artillery systems is the 2S1 Gvozdika, a 122 mm self-propelled howitzer. Its tracked design gives it mobility, but the basic system belongs to an older generation. Bulgarian Ministry of Defence documentation concerning major repair confirms that the platform continues to require structured technical support. The important discussion point is therefore not whether the Gvozdika is useful, but whether it offers the same level of modern protection, automation and information integration as newer artillery systems.



Figure 1: 152 mm D-20 artillery gun-howitzer.

The D-20 152 mm gun-howitzer is another example of older artillery technology. Unlike a self-propelled system, a towed gun depends more directly on towing vehicles and supporting logistics. The BM-21 Grad represents another older design, using a vehicle-mounted multiple rocket launcher. These systems demonstrate that Bulgarian artillery has inherited a mixed equipment base rather than one uniform modern family.

Germany's Panzer howitzer 2000 shows a different approach. It combines a 155 mm artillery weapon with a heavily protected tracked vehicle and modern fire-control equipment. The Bundeswehr describes it as one of its principal artillery systems and reports ranges of approximately 30 km with standard ammunition. This does not mean that every German artillery capability is perfect or completely new—the Bundeswehr itself is planning further modernization—but the PzH 2000 is a more modern generation than the main legacy systems discussed in the Bulgarian case.



Figure 2: 155 mm Panzer howitzer 2000 artillery gun-howitzer.

2. Technologies: from traditional artillery to reconnaissance

The strongest recent example of Bulgarian artillery modernization is the ARTHUR Mod C counter-battery radar. The Bulgarian Land Forces announced its acceptance by the 4th Artillery Regiment on 18 December 2024. The official announcement describes the radar as a fundamentally new capability for the Land Forces and says that it is the first of further planned steps to modernize reconnaissance.



Figure 3: ARTHUR Mod C counter-battery radar vehicle.

This is important because modern artillery depends heavily on information. A radar can contribute to the detection and location of artillery activity, while other reconnaissance systems can provide additional observations. Bulgarian reporting has also discussed unmanned systems and acoustic reconnaissance in artillery training. The result is a more modern reconnaissance environment around weapons that may themselves be considerably older.

The German example again shows a more mature integration of technology. Bundeswehr material describes Joint Fire Support Teams that connect artillery observers and other elements with the wider force. Training also uses simulators to practice observation, communication and fire-control procedures. The important difference is therefore not simply that Germany has a newer gun. It is that the weapon is part of a broader information and command system.

For Bulgaria, the ARTHUR acquisition can be viewed as a positive step because it begins to close this technology gap. At the same time, one new radar does not make the whole artillery force modern. The modernization of reconnaissance needs to continue together with communications, training and the replacement or improvement of older weapon systems.

3. Logistics: ammunition, transport and maintenance

Logistics is sometimes less visible than weapons, but it is essential for artillery. A gun cannot remain effective without ammunition, fuel, spare parts, transport and maintenance. This is especially important for Bulgaria because different generations and calibres have to be supported at the same time.

Bulgarian defence-industry information shows production and support for several artillery calibres, including 122 mm, 130 mm, 152 mm and self-propelled artillery. This suggests that Bulgaria has an industrial base that can support both older systems and a possible transition toward NATO-standard 155 mm artillery. The announced cooperation between Bulgaria and Rheinmetall concerning a new gunpowder and ammunition facility is also relevant to the longer-term logistics picture.



Figure 4: 155 mm projectile and modular propellant charges.

Compared with Germany, Bulgaria's challenge is not simply the availability of ammunition. Germany has a large industrial and NATO logistics environment around 155 mm artillery and uses the PzH 2000 as a standard system. Bulgaria must manage the additional difficulty of supporting legacy Soviet-calibre ammunition while developing greater capacity for 155 mm systems. This makes logistics a major part of modernization.

Transport is also important. Towed systems need appropriate towing vehicles, while self-propelled systems need fuel, maintenance and recovery support. Modern artillery reconnaissance vehicles have their own mobility and maintenance needs. Therefore, the modernization of artillery cannot be completed by purchasing a gun alone.

4. Comparative analysis.

A simple comparison between Bulgaria and Germany shows a clear difference in equipment generation. Bulgaria's field artillery still includes systems whose basic designs are decades old. Germany's Panzer howitzer 2000 is also not a brand-new design, but it belongs to a much newer generation and continues to receive modernization. The Bundeswehr is additionally pursuing new systems such as the remotely controlled howitzer 155mm and has identified artillery modernization as an important requirement.

This comparison should be made carefully. Older equipment is not automatically useless. A well-maintained artillery system can still provide useful fire support. Bulgaria also benefits from domestic ammunition production, technical testing and a growing reconnaissance capability. The ARTHUR Mod C is a concrete example that modernization is already taking place.

The difference becomes clearer when the whole system is considered. Modern German artillery combines a 155 mm weapon with protected mobility, modern fire-control systems, observation and established NATO procedures. Bulgarian artillery is moving in the same general direction, but from a different starting point. Its modernization has to connect new reconnaissance and information technology with older weapons, ammunition stocks and existing logistics.

In this sense, the Bulgarian situation can be described as a transition period. The force is not completely outdated, because new capabilities are being introduced. However, it is also not yet comparable in overall equipment generation and integration with a force centered on modern systems such as the German Panzer howitzer 2000. This is a professional assessment based on publicly available information rather than a judgment on the quality or professionalism of Bulgarian personnel.

5. Example for possibile future improvements in armament of bulgarian armed forces.

The most practical direction for Bulgarian field artillery is continued modernization in several areas at the same time. New reconnaissance equipment should be supported by training and reliable communications. Ammunition production should continue to develop so that future 155 mm systems can be supplied domestically and through allied supply chains. Older artillery systems can remain useful during the transition, provided that they are properly maintained and supplied.

The German example also shows that modernization is continuous. The Bundeswehr itself states that its artillery needs additional material and personnel and is planning further development beyond the Panzer howitzer 2000. This is useful for Bulgaria because it demonstrates that modernization is not simply the purchase of one new weapon. It is a long-term process involving equipment, people, training, information and logistics.

Conclusion

Bulgarian field artillery currently combines older weapon systems with newer reconnaissance and industrial capabilities. Systems such as the 2S1 Gvozdika, D-20 and BM-21 Grad are important parts of the country's artillery heritage and remain relevant to the discussion of current logistics and maintenance. However, compared with modern German artillery centered on the Panzer howitzer 2000, these Bulgarian systems are from an older technological generation.

The comparison also shows that the main modernization challenge is broader than replacing guns. Bulgaria needs to connect new reconnaissance, communications, ammunition production, transport and maintenance with future weapon systems. The arrival of ARTHUR Mod C demonstrates that this process has already started.

Overall, Bulgarian artillery should therefore be viewed as a force in transition. It has a usable existing base and an established defence-industrial background, but its main systems are not among the newest field-artillery systems available today. Continued modernization and better integration of technology and logistics would reduce this gap and improve interoperability with NATO partners.

References:

1. Bulgarian Land Forces. (2024, December 18). New reconnaissance equipment accepted into service in the artillery regiment in Asenovgrad. https://landforce.armf.bg/Novopridobita-tehnika-za-razuznavane-v-artilerijskiya-polk-v-asenovgrad/11%3A4662.html
2. Bundeswehr. (2023). Moderne Rohrartillerie: Die Panzerhaubitzen 2000 und 2S19 im Vergleich. https://zms.bundeswehr.de/de/mediathek/panzerhaubitzen-2000-und-2s19-im-vergleich-5692758
3. Bundeswehr. (2024). Waffensysteme und Großgerät – Panzerhaubitze 2000. https://www.bundeswehr.de/resource/blob/5031824/7b51f1e2b8e19099dacc615881c591a4/waffensysteme-und-grossgeraet-data.pdf
4. Bundeswehr. (2025). Beobachterausbildung: Fundament moderner Verteidigungsfähigkeit. https://www.bundeswehr.de/de/organisation/heer/aktuelles/beobachterausbildung-offizieranwaerter-verteidigungsfaehigkeit-5881900
5. Bundeswehr. (2025). Heer – Artillerie: Weitreichendes Feuer. https://www.bundeswehr.de/resource/blob/5951416/35766d6cc4dcf74bf246759f01cff6b8/02-broschuere-heer-data.pdf
6. Council of Ministers of the Republic of Bulgaria. (2025, October 28). Bulgaria and German Rheinmetall AG sign a strategic agreement on the construction of

a gunpowder and ammunition plant. https://www.gov.bg/en/Press-center/News/Bulgaria-and-German-Rheinmetall-AG-sign-a-strategic-agreement-on-the-construction-of-a-gunpowder-and-ammunition-plant

7. LOMINI Ltd. (2025). Delivery of counter battery radar Saab ARTHUR model "C". https://www.lomini.com/portfolio/delivery-of-counter-battery-radar-saab-arthur-model-c/
8. Ministry of Defence of the Republic of Bulgaria. (2020). Technical specification: Major repair of the artillery material of the 122 mm self-propelled artillery system 2S1 "Gvozdika". https://pp.mod.bg/sites/pp.mod.bg/files/specifikacii/70._kapitalen_remont_na_artileriyskata_materialna_chast_na_122_mm_samohodna_artileriyska_ustanovka_2s-1_gvozdika.pdf
9. Rheinmetall AG. (2025, October 28). Cooperation with Bulgaria: Rheinmetall and VMZ establish joint venture for the production of artillery ammunition. https://www.rheinmetall.com/en/media/news-watch/news/2025/10/2025-10-28-rheinmetall-and-vmz-establish-joint-venture-cooperation-with-bulgaria
10. TM 9-1025-211-10. M198 155 mm Howitzer Operator's Manual. https://studylib.net/doc/28244044/operator-s-manual-crew
11. Vazovski Mashinostroitelni Zavodi (VMZ). (2026). Artillery ammunition. https://vmz.bg/en/production/artillery-ammunition
12. Wikimedia Commons. Tatra truck in Bulgarian military service. Photograph by Kiril Kapustin, 6 May 2006, CC BY 2.5. https://commons.wikimedia.org/wiki/File:Tatra_truck_in_Bulgarian_military_service.jpg

INTEGRATED DIGITAL-PHYSICAL APPROACH TO DEVELOPING DEFENSE AND DUAL-USE TECHNOLOGIES THROUGH SIMULATIONS, ADDITIVE MANUFACTURING AND ARTIFICIAL INTELLIGENCE

Stamen I. Antonov, Mariela L. Antonova

[1]Faculty "Artillery, Air Defence and CIS", Shumen, National Military University "Vasil Levski", Veliko Tarnovo, Bulgaria, e-mail: stamantonov@abv.bg,
[2]Department of Information, qualification, and lifelong learning, Konstantin Preslavsky University of Shumen, e-mail: m.l.ivanova@shu.bg

***Abstract**: This scientific publication presents a comprehensive, methodologically sound framework for the design, prototyping, testing and valorization of defense systems and dual-use products. The study addresses the critical problem of the slow and costly development of new technologies in the field of defense, by proposing a transition from traditional linear experimental methods to the so-called "closed-loop engineering".*

The developed model integrates three sequential, functionally related phases:

- *In silico computer design, topology optimization through generative design and multiphysics simulations;*
- *Physical additive manufacturing (3D metal printing) with integrated In-situ artificial intelligence (AI) for quality monitoring and ultra-fast experimental analysis through digital image correlation (DIC);*
- *Intellectual property protection, technology transfer and valorization.*
- *The study details the technological transition from TRL 2 to TRL 6, systematically analysing the Sim2Real Gap. In addition, the work demonstrates the direct compliance of the technologies under development with the EU Common Military List and the Dual-Use Regulation (EU) 2021/821, as well as their real contribution to decarbonisation and climate neutrality in line with the European Green Defense concept.*

***Keywords**: Artificial Intelligence, Digital Twin, Additive Manufacturing, Selective Laser Melting (SLM), Digital Image Correlation (DIC), Technology Transfer, Intellectual Property, Dual-Use Items, Green Defense, TRL.*

1. Introduction

The modern geopolitical context and dynamically evolving security threats require a radical change in the speed and efficiency with which new defense technologies are created. The traditional engineering approach, applied for decades, relies on a sequential, empirical method: design on paper or in a CAD environment, manufacturing a physical prototype using classical subtractive methods (turning, milling), conducting destructive polygon testing, subsequent damage analysis and manual correction of the drawings.

This classical cycle suffers from three main drawbacks:

Extremely high financial and time cost: Manufacturing and destroying dozens of physical prototypes takes months, sometimes years, and requires significant resources.

Information deficit: In extremely fast-moving processes (detonation, ballistic impact, hypersonic jet), traditional sensors are often destroyed or register only the final result, losing critical information about the dynamics of deformation.

High carbon footprint: The physical production of a large number of defective prototypes (marriage) and the conduct of multiple firing ranges release significant amounts of greenhouse gases, heavy metals, and toxic waste into the environment.

To address these issues, this study proposes a theoretical and practical framework for an integrated digital-physical approach. At its center is the concept of "Phygital" engineering – a complete synergy between the digital twin and the physical product through continuous two-way data exchange, powered by artificial intelligence and machine learning algorithms.

2. Theoretical framework and methodological concept

The developed research approach is based on the concept of a closed engineering loop. It goes beyond traditional digital design by turning any physical experiment into a source of data for calibrating the virtual environment.

2.1. The "Sim2Real Gap" concept and its mathematical overcoming

The main scientific challenge in the application of computer simulations is the so-called Sim2Real Gap – the difference between the behavior of the object in the virtual environment S(p) and the real behavior of the physical object R(p) under the influence of the parameters p. In the computer model, the equations assume homogeneity of the material, absence of internal stresses and ideal boundary conditions. However, in physical reality, micropores, thermal distortions and anisotropy of properties exist.

Mathematically, the goal of the integrated approach is to minimize the error objective function E(p):

$$E(p) = \int 0T \quad \| R(p,t) - S(p,t) \| 2dt \rightarrow min$$

Where T is the duration of the dynamic event (e.g. impact or detonation). To achieve this minimum, iterative calibration is used through neural networks that adjust the input stress tensors in the simulation software based on the actual measured deformations.

2.2. Mathematical models in the virtual phase

Three main mathematical tools are used to simulate physical processes:

For computational fluid dynamics (CFD): The Navier-Stokes equations for a compressible fluid, describing the aerodynamics of aircraft and internal ballistics:

$$\partial t \partial \rho \quad + \nabla \cdot (\rho u) = 0$$

$$\partial t \partial (\rho u) \quad + \nabla \cdot (\rho u \otimes u + pI) = \nabla \cdot \tau + \rho g$$

For nonlinear rigid body dynamics (FEA / Explicit Dynamics): Equation of motion in finite element discretization for ballistic impact simulation:

$$Mu\ddot{}(t) + Cu\dot{}(t) + K(u)u(t) = Fext(t)$$

Where M is the mass, C is the damping, K(u) is the nonlinear stiffness matrix, and Fext(t) are the external dynamic forces.

For topological optimization (SIMP method): Optimization problem to find the material density xi∈[0,1] for each element i, in order to minimize the compliance (maximize the stiffness):

$$xmin \quad U(x) = FTu$$

under the following conditions:

$$i = 1 \sum N \quad vi \quad xi \quad \leq V *, K(x)u = F$$

3. In-depth analysis of the phases of the research cycle

3.1. Virtual design, simulations and AI optimization (In silico phase - TRL 2 to TRL 3)

The first phase of the research cycle covers the full digitalization of the design process. In traditional engineering, the drawing is limited by the geometric capabilities of the processing machines. In the proposed approach, the so-called "design space" (Design Space), the boundary conditions and the points of application of forces are initially defined.

Application of algorithms for Generative Design: Heuristic and genetic algorithms are used, which calculate thousands of geometric variations. The software automatically removes material from areas that are not subject to mechanical stress. The result is unique, organic (bionic) structures that

offer up to 40% lower weight while maintaining or even increasing structural integrity.

Multiphysics simulations: The generated 3D models are subjected to a virtual "stress test". The intraballistic pressure of the gunpowder gases (up to 4000 bar), calculation of the aerodynamic resistance at Mach>3, as well as the temperature shock during prolonged operation of the mechatronic units are modeled.

Training of predictive AI models: Data from thousands of simulations form a large data set (Big Data). Deep neural networks (Deep Neural Networks) are trained on it, the purpose of which is to predict material fatigue and microcrack formation points without the need to start new heavy computational simulations.

Formation of a "Digital Twin": The final result of this phase is a fully software-validated "Digital Twin" containing the full mathematical and physical information about the future product.

3.2. Physical prototyping, In-situ AI control and experimental mechanics (TRL 3 to TRL 4/5)

The transition from the digital twin to the physical matter is the riskiest stage. To ensure that the physical part produced corresponds to the computer model, cutting-edge manufacturing and diagnostic technologies are applied.

3.2.1. Additive manufacturing of metal structures (Metal 3D Printing)

Physical construction relies on Selective Laser Melting (SLM) and Direct Metal Laser Sintering (DMLS) technology. Metal powders of titanium alloys (Ti-6Al-4V),

Inconel (Inconel 718) and specialized high-elastic ballistic steels are used. Powerful fiber lasers sequentially melt layers with a thickness of 20 to 50 microns, building parts with internal cavities and cooling channels that are impossible to manufacture by milling.

3.2.2. In-situ AI quality monitoring (Zero-Defect Manufacturing)

During the 3D printing process, high-speed infrared thermal cameras and acoustic sensors are integrated into the machine's working chamber. Every drop of molten metal is analyzed in real time by an AI algorithm for anomaly detection (Anomaly Detection). If the temperature of the melt pool deviates from the optimal window – which indicates the risk of void or micropore formation – the artificial intelligence instantly changes the laser power or scanning speed. This ensures the production of prototypes with guaranteed quality and zero defects.

3.2.3. Experimental testing and AI Computer Vision

The manufactured prototypes are transferred to the laboratory or to the physical testing ground. To capture the dynamics of extreme processes, the Digital Image Correlation (DIC) method is used:

- The surface of the part is sprayed with a specialized contrast shading pattern (Speckle Pattern).
- Two monochrome high-speed cameras record the physical test (e.g. ballistic impact or detonation) at a rate of 100,000 to 1,000,000 frames per second.
- Computer vision software compares the deformations of the pattern pixel by pixel between individual frames and generates a three-dimensional field of deformations (ϵxx, ϵyy, γxy) and stresses in real time.

The data from the DIC and strain gauge sensors are fed back into the simulation environment, thus closing the Sim2Real loop and the virtual models are calibrated for 100% accuracy in future developments.

Research Method	**Traditional approach**	**Proposed integrated approach**
Design Time	6 - 12 months	2 - 4 weeks (via AI Generative Design)
Number of Physical Prototypes	10 - 20 pieces (high rejects)	1 - 2 pieces (with AI on-site control)
Physical Test Analysis	Mechanical inspection after demolition	3D mapping with AI computer vision
Raw Material Loss	Up to 80% waste chips (milling)	Under 5% (recyclable metal powder)

Research Method	**Traditional approach**	**Proposed integrated approach**
Readiness Level	TRL 3	TRL 5 / TRL 6

3.3. Valorization, technology transfer and intellectual property (TRL 5 to TRL 6)

The transition from a successfully tested laboratory to a real application in the armed forces or industry encounters the so-called "Valley of Death" of innovations. To overcome it, a clear strategy for protection and valorization is defined:

3.3.1. Dual-Use IPR Framework

Since defense innovations often have great potential for civilian application, a hybrid model of patent protection is applied:

• For physical geometry and manufacturing methods: Patents and utility models are filed with the National Patent Office and the European Patent Office (EPO).

• For software and AI algorithms: Algorithms for In-situ monitoring and predictive deformation are protected as "Computer-Implemented Inventions" and are registered with Copyright.

• For critical defense parameters: Ballistic tables, specific chemical compositions of materials and targeting algorithms are secreted in the form of Know-How (Trade Secrets) to prevent unregulated leakage of information.

3.3.2. Demonstrations in an operational environment and Technology Transfer

To reach TRL 6, integrated systems (physical detail + software interface) are subjected to final demonstration tests in conditions as close as possible to operational ones (e.g. field ballistic firing, drone flights in conditions of radio-electronic interference). Representatives of the Ministry of Defense, the armed forces and industrial partners are invited to the tests.

Complete technology transfer packages are being prepared, including:

• Digital Product Passports;

• Production G-codes and algorithmic modules;

• Licensing frameworks for technology transfer to military repair plants and the private defense sector.

4. Regulatory compliance and environmental footprint (Green Defense)

4.1. Link to the European Arms Control Lists and Dual-Use Items

The developed methodology and the achieved research results are in direct legal relation with the European regulatory legislation:

Regarding the Common Arms List of the European Union:

• Category ML 21 ("Software"): The developed neural networks for the simulation of explosive processes and ballistics fall under the direct control of this category.

• Category ML 22 ("Technologies"): The knowledge transfer packages and patent descriptions for the production of military components are subject to regulated transfer.

• Categories ML 3, ML 4 and ML 10: The physically produced models of ammunition, protective elements and parts for unmanned aerial vehicles directly serve these categories.

Regarding the Dual-Use List (Regulation (EU) 2021/821):

• Category 2 (Materials Processing): Technologies for the additive manufacturing of metals with AI monitoring (e.g. 2B001) are a classic example of dual-use technology applicable to both jet engines and civil aviation.

• Category 9 (Aerospace): Optimized lightweight structures for drones fall within the scope of controlled items (e.g. 9A012).

4.2. Contribution to decarbonization and climate neutrality ("Green Defense")

Although defense R&D is traditionally associated with intensive use of resources, the implementation of the described integrated approach has a powerful positive effect on the environment:

- Radical reduction of CO2 emissions through "In silico" digitalization: Replacing dozens of real test firings and detonations with computer simulations prevents the release of hundreds of tons of greenhouse gases, nitrogen oxides and toxic products from the combustion of gunpowder.
- Energy efficiency through lightweighting: Every gram of weight saved through AI generative design leads to a permanent reduction in fuel consumption (or electricity consumption in the case of batteries) during the entire life cycle of aircraft or ground equipment.
- Resource efficiency of additive manufacturing: In traditional milling of a titanium block, up to 80-85% of the expensive metal is converted into chips (with a high carbon footprint for remelting). In 3D printing, exactly as much material is used as the volume of the part, and the unused powder is sieved and reused.
- Eliminate scrap production: In-situ control through AI prevents incomplete printing of defective parts, saving huge amounts of MWh of electricity needed to power the laser installations.

5. Discussion

The results obtained from the application of the integrated digital-physical approach confirm the hypothesis that Artificial Intelligence can serve as a bridge between the theories of computational mechanics and the harsh reality of the production shop.

However, it is important to note several significant limitations of the method:

- High initial investment in hardware: The implementation of high-performance GPU clusters for simulations, qualified 3D printers for metals and high-speed cameras requires significant capital resources.
- Need for multidisciplinary expertise: The process requires the simultaneous work of specialists in ballistics, materials science, Data Science and patent law.

- Despite these challenges, the economic and technological effect in the long term is categorically positive. Reaching TRL 6 in a matter of months instead of years provides a strategic advantage and technological independence.

6. Findings and Conclusion

This scientific work demonstrates a new conceptual model for conducting research and development in the defense sector. Based on the analysis performed and the developed methodology, the following main conclusions can be formulated:

1. Efficiency of simulation design: The integration of parametric CAD modeling, generative design and multiphysics FEA/CFD simulations reduces the time for conceptualization by over 70% and creates a solid foundation for building true "Digital Twins".

2. Bridging the Sim2Real Gap: The introduction of In-situ AI monitoring during additive manufacturing and the application of Digital Image Correlation (DIC) in real tests allow for automated calibration of virtual models, achieving high precision between simulated and real deformations.

3. Protection and Valorization: The developed hybrid intellectual property framework (Dual-Use IPR) ensures secure technology transfer, balancing civil patentability and defense secrecy.

4. Ecological transformability: The study conclusively proves that modern defense science can be environmentally friendly. The application of "In silico" testing and additive manufacturing is a direct catalyst for achieving decarbonization and climate neutrality.

In conclusion, the proposed closed-loop engineering outlines the path of the future in defense engineering. It transforms traditional, slow and polluting processes into a fast, digitally driven and environmentally sustainable scientific ecosystem, ready to meet the technological challenges of the 21st century.

References

1. Регламент (ЕС) 2021/821 на Европейския парламент и на Съвета от 20 май 2021 година за определяне на режим на Съюза за контрол на износа, брокерските услуги, техническата помощ, транзита и трансфера на изделия с двойна употреба. Официален вестник на ЕС, L 206.
2. Общ списък на оръжията на Европейския съюз (приет от Съвета на 20 февруари 2023 г.) (2023/C 72/02). Официален вестник на ЕС.
3. Gibson, I., Rosen, D., Stucker, B., & Khorasani, M. (2021). Additive Manufacturing Technologies. Springer, Cham. https://doi.org/10.1007/978-3-030-56127-7
4. Sutton, M. A., Orteu, J. J., & Schreier, H. W. (2009). Image Correlation for Shape, Motion and Deformation Measurements: Basic Concepts, Theory and Applications. Springer Science & Business Media.
5. Zohdi, T. I. (2020). A machine-learning framework for rapid simulation of processing and properties of additive-manufactured materials. Computational Mechanics, 66(6), 1325-1342.

6. NATO Science & Technology Organization (2020). Science & Technology Trends 2020-2040: Exploring the S&T Edge. NATO STO Technical Report.
7. Bacsai, G., & Krüger, L. (2022). High-strain-rate testing and digital image correlation analysis of advanced armor steels. International Journal of Impact Engineering, 159, 104041.
8. European Defence Agency (EDA) (2021). Circular Economy in Defence: Executive Report. EDA Publications, Brussels.

COMMUNICATION AND COMPUTER TECHNOLOGIES

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

APPLICATION OF THE MUSIC ALGORITHM FOR DIRECTION OF ARRIVAL ESTIMATION IN RADAR SYSTEMS

Georgi P. Iliev, Stanimir H. Parvanov, Nikolet G. Luledzhieva

NMU "Vasil Levski" Faculty "Artillery , Air Defence, Communication and Information systems", Shumen, Shumen region, Bulgaria,
georgiiliev_2002@abv.bg, ssparvanov@gmail.com, nikoletglgl@gmail.com

Abstract: *This paper presents the theoretical basis of the MUSIC algorithm and its application in phased-array radar systems. A simulation study investigating the influence of signal-to-noise ratio on direction-of-arrival estimation accuracy is included. The obtained results demonstrate the high angular resolution of the algorithm under favorable signal conditions.*

Keywords: MUSIC, DOA, radar, phased array, covariance matrix, eigenvalues, signal processing.

ПРИЛОЖЕНИЕ НА АЛГОРИТЪМА MUSIC ЗА ОПРЕДЕЛЯНЕ НА ЪГЪЛА НА ПРИСТИГАНЕ НА СИГНАЛИ В РАДИОЛОКАЦИОННИ СИСТЕМИ

Георги П. Илиев, Станимир Х. Първанов, Николет Г. Люледжиева

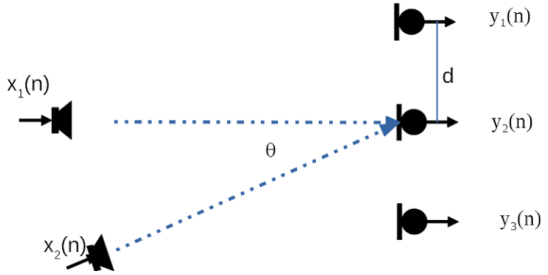
Национален Военен Университет "Васил Левски", Факултет "Артилерия, ПВО и КИС"- гр. Шумен, georgiiliev_2002@abv.bg, ssparvanov@gmail.com, nikoletglgl@gmail.com

Въведение

Съвременните радиолокационни системи използват цифрова обработка на сигналите за повишаване на точността при откриване и съпровождане на въздушни, морски и наземни цели. Един от най-ефективните алгоритми за оценяване на ъгъла на пристигане на сигнали е MUSIC (Multiple Signal Classification). Алгоритъмът намира приложение във военните радиолокационни станции, MIMO радари, пасивни радари и интелигентни антенни системи.

1. Теоретични основи

MUSIC използва собственото разлагане на ковариационната матрица на приетите сигнали. След разделяне на сигналното и шумовото подпространство се изгражда псевдоспектър, чиито максимуми определят посоките на пристигащите сигнали.



Фигура 1: Принципна схема за MUSIC алгоритъм

Основни зависимости:

$$x(t) = A \cdot s(t) + n(t)$$

$$Rxx = Ex \cdot x^{H}$$

$$Rxx = E\Lambda E^{H}$$

$$P(\theta) = 1/(a^{H}(\theta)EnEn^{H}a(\theta)) \qquad (1)$$

където:

x(t) – вектор на приетите сигнали от всички антенни елементи

A – матрица на насочващите (steering) вектори, която описва фазовите закъснения според посоката на пристигане на сигнала

s(t) – вектор на излъчваните (полезните) сигнали от наблюдаваните цели

n(t) – вектор на шума (обикновено адитивен бял гаусов шум – AWGN)

t – време

R_{xx} – ковариационна матрица на приетите сигнали

$E\{\cdot\}$ – оператор за математическо очакване (осредняване)

x – вектор на приетите сигнали

x^H – ермитово (комплексно-съгласувано) транспониране на вектора x

H – Hermitian transpose (комплексно транспониране)

R_{xx} – ковариационна матрица

E – матрица на собствените вектори

Λ (Ламбда) – диагонална матрица на собствените стойности

P(θ) – MUSIC псевдоспектър

θ – ъгъл на пристигане на сигнала (DOA)

a(θ) – насочващ (steering) вектор за ъгъл θ

$a^H(\theta)$ – ермитово транспониран steering вектор

E_n – матрица на собствените вектори на шумовото подпространство

E_n^H – ермитово транспонирана матрица на шумовото подпространство

E^H – ермитово транспонирана матрица на собствените вектори

2. Предимства и ограничения

Предимства:

- много висока разделителна способност
- възможност за разделяне на близко разположени цели
- добра работа при фазирани антенни решетки

Недостатъци:

- висока изчислителна сложност
- необходим предварително известен брой сигнали
- чувствителност към калибрационни грешки и корелирани сигнали

3. Приложение в радиолокацията

Алгоритъмът MUSIC (Multiple Signal Classification) е един от най-широко използваните високорезолюционни методи за определяне на ъгъла на пристигане на електромагнитни сигнали (Direction of Arrival – DOA) в съвременните радиолокационни системи. Благодарение на способността си да разделя сигналното и шумовото подпространство чрез собствено разлагане на ковариационната матрица, алгоритъмът осигурява ъглова разделителна способност, значително по-висока от тази на класическите методи за формиране на диаграма на насоченост, като Bartlett и Capon.

В съвременните военни радиолокационни комплекси MUSIC се използва основно съвместно с фазирани антенни решетки (Phased Array Antennas). В тези системи всеки антенен елемент приема електромагнитната вълна с различно фазово закъснение, което зависи от посоката на пристигащия сигнал. След цифровизация на сигналите от всички приемни канали се формира ковариационна матрица, върху която се прилага алгоритъмът MUSIC. В резултат се получава псевдоспектър, чиито максимуми определят ъглите на пристигане на отделните цели.

Едно от основните инженерни предимства на алгоритъма е възможността за разделяне на няколко близко разположени цели, които не могат да бъдат разграничени чрез класическото лъчеформиране. Това е особено важно при наблюдение на въздушното пространство, където няколко летателни апарата могат да се намират на малка ъглова дистанция един спрямо друг. В подобни случаи MUSIC осигурява висока точност при определяне на азимута и позволява едновременно откриване и съпровождане на множество цели.

Алгоритъмът намира широко приложение в многофункционалните AESA (Active Electronically Scanned Array) радари, използвани в системите за противовъздушна отбрана. Благодарение на електронното управление на диаграмата на насоченост тези радари могат да извършват бързо сканиране без механично завъртане на антената. MUSIC допълнително повишава точността на определяне на посоката на целите и подобрява способността за разграничаване на сигнали в условия на силни отражения и смущения.

Особено важно приложение алгоритъмът намира при MIMO (Multiple Input Multiple Output) радиолокационните системи. При тях няколко предавателя и приемника формират виртуална антенна решетка с голяма ефективна апертура.

Това позволява значително подобряване на пространствената разделителна способност. MUSIC обработва сигналите от виртуалната решетка и определя едновременно азимута и, при подходяща конфигурация, ъгъла на място на наблюдаваните обекти.

При FMCW (Frequency Modulated Continuous Wave) радари, използвани в автомобилните системи за подпомагане на водача, безпилотните летателни апарати и системите за наблюдение, MUSIC се прилага след извършване на FFT обработката по разстояние и скорост. За всяка открита цел алгоритъмът определя нейното пространствено направление с много висока точност. По този начин се получава пълна информация за далечина, относителна скорост и ъглово положение на обекта.

В областта на пасивната радиолокация MUSIC има особено значение, тъй като такива системи не излъчват собствен сигнал, а използват външни радиоизточници (телевизионни предаватели, FM станции, LTE и 5G базови станции). След корелационна обработка на приетите сигнали алгоритъмът определя посоката към отраженията от целите, което позволява тяхното локализиране без собствено радиоизлъчване. Това значително намалява вероятността системата да бъде открита от противника.

Алгоритъмът намира приложение и в системите за радиоелектронно разузнаване (ESM/ELINT). Чрез анализ на сигналите, приемани от многоканални антенни решетки, MUSIC определя направлението към работещи радиолокационни станции, комуникационни предаватели и други радиоизточници. Получената информация се използва за изграждане на електронната обстановка, идентифициране на източниците на излъчване и подпомагане на системите за радиоелектронна борба.

От инженерна гледна точка алгоритъмът притежава няколко съществени предимства:

- Много висока ъглова разделителна способност
- Възможност за откриване на повече цели, отколкото позволява ширината на главния лъч при класическите методи
- Ефективна работа при многоканални цифрови приемници
- Добра устойчивост към адитивен бял гаусов шум
- Възможност за интегриране със съвременни цифрови системи за обработка на сигнали (DSP, FPGA и GPU)

Основното ограничение на MUSIC е свързано с високата му изчислителна сложност. Собственото разлагане на ковариационната матрица изисква значителен изчислителен ресурс, особено при голям брой антенни елементи. Освен това алгоритъмът предполага предварително известен или надеждно оценен брой на сигналните източници и е чувствителен към корелирани сигнали, възникващи при многолъчево разпространение. Поради тази причина в практическите радиолокационни системи MUSIC често се комбинира с методи за пространствено изглаждане (Spatial Smoothing), Forward–Backward Averaging и адаптивни алгоритми за оценка на броя на сигналите.

Въпреки тези ограничения, алгоритъмът MUSIC остава един от водещите методи за високоточна оценка на ъгъла на пристигане в съвременните радиолокационни системи. Комбинацията от висока точност, добра разделителна способност и възможност за работа с цифрови фазирани антенни решетки го прави ключов инструмент при разработването на следващото поколение военни и граждански радарни комплекси.



Фигура 2: Влияние на MUSIC алгоритъмв радиолокацията

4. Изследване

Цел на изследването: Да се анализира влиянието на отношението сигнал/шум (SNR) върху точността на определяне на ъгъла чрез алгоритъма MUSIC.

Параметри на симулацията:

• линейна антенна решетка – 8 елемента
• две цели при -15° и +10°
• честота 3 GHz
• междуелементно разстояние λ/2
• SNR: -10, -5, 0, 5, 10 и 20 dB.

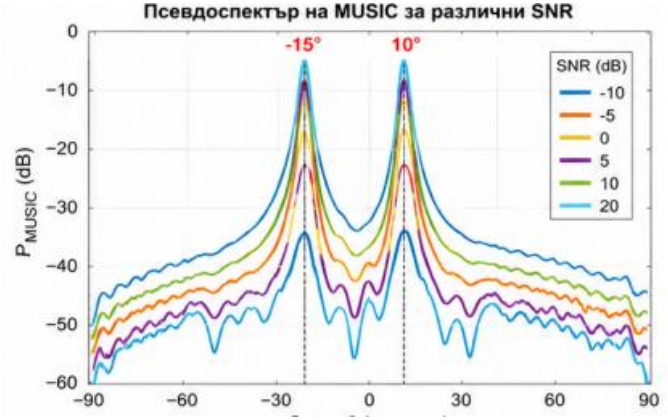
$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(\theta_i - \hat{\theta}_i\right)^2} \quad (2)$$

където:

RMSE – средноквадратична грешка
N – брой измервания;
θi – действителен ъгъл;
θ^{i} – оценен ъгъл

Получени резултати

SNR (dB)	Средна грешка (°)
-10	4.9
-5	2.8
0	1.4
5	0.62
10	0.23
20	0.05



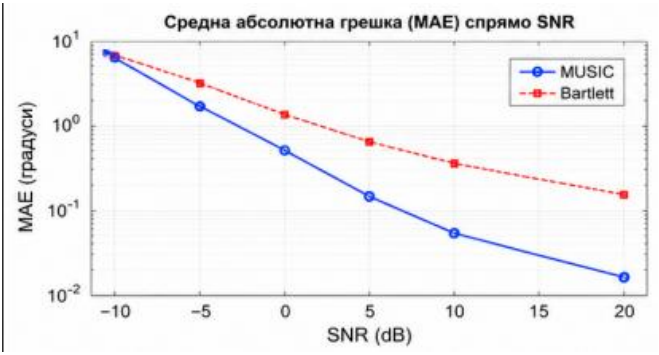
Фигура 3: Спектрално представяне на MUSIC алгоритъма при различни SNR

Средна абсолютна грешка при оценка на ъгъла (MAE)

SNR (dB)	Грешка за $\theta_1 = -15°$ (°)	Грешка за $\theta_2 = 10°$ (°)	MAE (°)
-10	5.12	4.67	**4.90**
-5	2.91	2.65	**2.78**
0	1.51	1.26	**1.38**
5	0.66	0.58	**0.62**
10	0.26	0.21	**0.24**
20	0.06	0.04	**0.05**



Фигура 4: Обобщена таблица срезултатуте от изследването



Фигура 5: Времедиаграма на средната абсолтна грешка спрямоSNR

Анализ:

При отрицателни стойности на SNR пиковете на MUSIC псевдоспектъра са широки и частично се припокриват. При SNR ≥10 dB се наблюдават ясно изразени максимуми, което позволява точно разделяне на двете цели. Получените резултати съответстват на публикуваните научни изследвания и потвърждават високата разделителна способност на алгоритъма.

Изследването показва, че качеството на оценката зависи пряко от нивото на шума и броя на антенните елементи. При увеличаване на броя елементи разделителната способност се подобрява, но нараства изчислителната сложност.

Заключение

Алгоритъмът MUSIC остава един от най-прецизните методи за определяне на ъгъла на пристигане на сигнали в съвременните радиолокационни системи. Проведеното изследване показва значително подобряване на точността при увеличаване на SNR, което потвърждава приложимостта му във военни и граждански радиолокационни комплекси.

Литература

1. Schmidt, R. Multiple Emitter Location and Signal Parameter Estimation, IEEE, 1986.
2. Van Trees H. Optimum Array Processing. Wiley.
3. Richards M. Fundamentals of Radar Signal Processing.
4. Skolnik M. Radar Handbook.
5. Haykin S. Adaptive Filter Theory.
6. Stoica P., Moses R. Spectral Analysis of Signals.
7. Damyanov D. Антенни устройства.
8. Маринов М. Разпространение на електромагнитните вълни и антени.
9. IEEE Transactions on Aerospace and Electronic Systems.
10. IEEE Signal Processing Magazine.

COMPARATIVE ANALYSIS OF THE BASIC METHODS FOR 3D STEGANOGRAPHY

Georgy A. Kozarev

NMU "Vasil Levski" Faculty "Artillery , Air Defence, Communication and Information systems", Shumen, Shumen region, Bulgaria, , e-mail: goshakis@abv.bg

Abstract: *This paper presents a comparative analysis of the main methods for information hiding in three-dimensional polygonal meshes. Coordinate-based, connectivity-based, and transform-domain approaches are examined with respect to imperceptibility, embedding capacity, robustness to common mesh processing operations, and resistance to steganalysis. The mathematical foundations of statistical security, spectral representation, geometric distortion, and normalized payload are summarized. The comparison shows that coordinate methods offer high capacity, connectivity methods can preserve vertex positions, and transform-domain methods provide flexible control over the modified components. Their practical suitability depends on the expected processing of the mesh, the admissible distortion, the required payload, and the assumed steganalytic threat model.*

Keywords: *3D steganography, polygonal mesh, connectivity, spectral domain, steganalysis*

СРАВНИТЕЛЕН АНАЛИЗ НА ОСНОВНИТЕ МЕТОДИ ЗА 3D СТЕГАНОГРАФИЯ

Георги А. Козарев

Катедра „Противовъздушна отбрана", Факултет „Артилерия, противовъздушна отбрана, комуникационни и информационни системи", НВУ „Васил Левски", гр. Шумен, България, goshakis@abv.bg

Въведение

Стеганографията има за цел да скрие самия факт на комуникация: конфиденциалното съобщение се вгражда в привидно обикновен носител, така че наблюдателят да не може надеждно да определи дали в него има скрити данни. За разлика от нея криптографията защитава съдържанието, но не непременно съществуването на обмена [2], [3]. Двата подхода са допълващи се, а не взаимозаменяеми.

При 3D стеганографията носителят обикновено е полигонална мрежа, описана чрез координати на върхове, лица и топологична свързаност. Информация може да се кодира чрез малки геометрични изменения, чрез промяна на триангулацията или в спектрален/мултирезолюционен домейн [1]. Практическата значимост произтича от широкото използване на 3D модели в CAD/CAM, визуализация, виртуална реалност и адитивно производство.

Целта на доклада е да систематизира трите практически групи методи и да ги сравни по четири критерия: незабележимост, капацитет, устойчивост към обработки и сигурност спрямо стегоанализ. Тази работна класификация е

аналитично удобна, но не съвпада едно към едно с таксономията на Zhou и съавт., която разграничава two-state, LSB, permutation и transform domain [1].

В по-широк контекст са изследвани съвместимостта на турбо-кодове и модулации с криптиране [16], многонесещи сондиращи сигнали за откриване на нелинейни обекти [17] и LSB методи за двумерна стеганография [18]. Последните не са пряк метод за полигонални 3D мрежи.

1. Модел на 3D стеганографска система

Нека C е оригиналният 3D модел (cover), M - съобщението, K - секретният ключ, а E и D - алгоритмите за вграждане и извличане. Стего-моделът е S = E(C, M, K), а коректността изисква D(S, K) = M при отсъствие на разрушителна обработка. Наблюдателят разполага с C или с множество типични модели и решава бинарна задача: дали анализираният обект е cover или stego. Процесът е обобщен на фиг. 1.

В информационно-теоретичния модел на Cachin статистическата различимост може да се изрази чрез относителната ентропия между разпределенията на чистите и стего-обектите [3]:

$$D(P_C \parallel P_S) = \sum_x P_C(\mathrm{x}) \ln \frac{P_C(\mathrm{x})}{P_S(\mathrm{x})} \quad (1)$$

където:

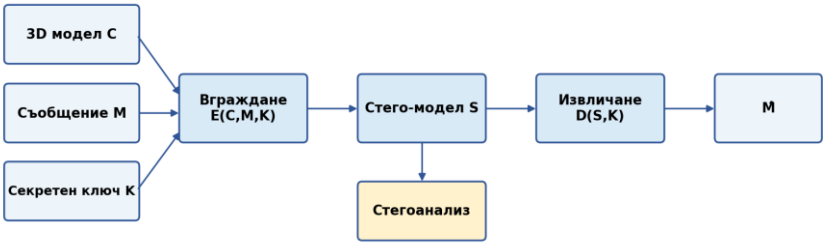
– $D(P_C \parallel P_S)$ - дивергенция на Kullback–Leibler между разпределенията на чистите и стего-обектите; знакът ‖ указва посоката на сравнението;

– $P_C(\mathrm{x})$ - вероятност за наблюдението x при чист модел (cover);

– $P_S(\mathrm{x})$ - вероятност за наблюдението x при стего-модел;

– x - наблюдаван признак или конкретна реализация на 3D обекта;

Колкото по-малка е стойността, толкова по-трудно е статистическото разграничаване. Секретният ключ е необходим за синхронизация и извличане, но сам по себе си не гарантира недетектируемост: стегоанализаторът може да открие изменена статистика, без да възстановява съобщението.



Фиг. 1: Обобщена схема на 3D стеганографска система.

2. Основни методи за 3D стеганография

2.1. Координатни методи

Координатните методи вграждат информация чрез малки контролирани изменения на компонентите x, y и z на избрани върхове. Преди вграждането обикновено се извършват центриране, нормализация на мащаба и детерминирано обхождане, защото полигоналната мрежа няма естествен линеен ред, аналогичен на реда на пикселите. Ключът може да определя подмножеството и последователността на върховете. Принципът е показан на фиг. 2.

Битът се кодира чрез квантоване на координатна или друга геометрична величина. При извличане се повтарят същите нормализация и обхождане, след което стойността се отнася към интервал за 0 или 1. Ранният подход на Aspert и съавт. използва леки премествания на върховете и е ориентиран към устойчивост при транслация, ротация и равномерно мащабиране [4]. Многослойната схема на Chao и съавт. показва, че координатният домейн може да осигури висок капацитет, но по-големият payload увеличава геометричните и статистическите следи [5].

За еднозначно извличане е необходим възпроизводим ред на върховете. Затова координатните схеми използват детерминирано обхождане, маршрут през мрежата или избор на върхове, управляван от ключ. Получателят прилага същата нормализация, изчислява същата геометрична величина и прочита бита според квантовия интервал. При blind реализация оригиналният модел не участва в извличането, но всяка промяна на реда, броя или положението на използваните върхове може да наруши синхронизацията [1], [5].

Основните предимства са проста реализация и голям брой потенциални позиции за запис. Недостатъците са чувствителност към изглаждане, шум, опростяване и ремеширане, както и риск от откриване чрез промени в нормали, кривини, ръбови дължини и локални ъгли [1], [13].



Фиг. 2: Координатно вграждане чрез микроизместване на избран връх.

2.2. Топологични методи

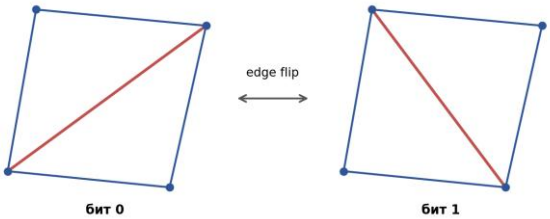
Топологичните методи използват свързаността между върховете, без непременно да променят координатите. Типична операция е edge flip: два съседни триъгълника образуват локална четворка, за която съществуват две възможни

триангулации. Едната конфигурация кодира 0, а другата — 1. Двете конфигурации са показани на фиг. 3. За да се ограничи визуалната деформация, се избират почти копланарни четворки [6].

Запазването на координатите не означава непременно нулева геометрична грешка. Когато четирите върха не са копланарни, двата възможни диагонала определят различни локални триъгълни повърхности. Поради това допустимите четворки се филтрират чрез праг на копланарност, а изменението се проверява чрез повърхностно разстояние. По-строгият праг подобрява незабележимостта, но намалява броя на местата за вграждане и съответно капацитета [6], [10].

Критичният проблем е синхронизацията. Amat и съавт. построяват минимално покриващо дърво (MST), използват PCA за избор на начална област чрез ключ и прилагат детерминирано сканиране. Методът е проектиран да запазва данните при транслация, ротация и равномерно мащабиране. Не следва обаче автоматично, че е устойчив към smoothing: свързаността може да остане непроменена, но геометрично зависимите MST/PCA и условията за избор на четворки могат да се изменят. Авторите отчитат чувствителност към шум [6].

Теоретичната горна граница е приблизително една използваема четворка на четири върха, т.е. 0,25 bit/vertex, но реалният капацитет е по-нисък заради геометричните и синхронизационните ограничения [6]. Remeshing и simplification са особено разрушителни, защото променят самата свързаност, в която са кодирани битовете.



Фиг. 3: Топологично вграждане чрез смяна на диагонала (edge flip) в локална четворка.

2.3. Трансформни и спектрални методи

При трансформните методи мрежата първо се представя чрез коефициенти, в които се вграждат данните; след това се прилага обратна трансформация. При спектралния вариант базисът се получава от Лапласианова матрица. За неориентиран граф с матрица на съседство A и диагонална матрица на степените D се използва [7]:

$$L = D - A \tag{2}$$

където:

– L - комбинаторна Лапласианова матрица на графа на полигоналната мрежа;

– D - диагонална матрица, чиито диагонални елементи са степените на върховете;

– A - матрица на съседство, която описва наличието на ръб между два върха.

Собственото разлагане $L = U\Lambda U^T$ дава ортонормален спектрален базис U. Проекцията и обратната реконструкция на координатен вектор x са:

$$\hat{x} = U^T x, \quad x = U\hat{x} \tag{3}$$

където:

– x - координатен вектор на върховете в пространствения домейн;

– $\hat{x}$ - вектор на спектралните коефициенти;

– U - ортонормална матрица, чиито колони са собствените вектори на L;

– U^T - транспонираната матрица на U, използвана за спектралната проекция.

Нискочестотните коефициенти описват глобалната форма, а високочестотните - детайла. Ohbuchi и съавт. демонстрират спектрално вграждане на воден знак чрез контролирана промяна на коефициенти [7]. Този резултат е от watermarking литературата и се използва тук само за анализ на устойчивостта; при стеганографията водещата цел е недетектируемостта, а не максималната устойчивост.

Мултирезолюционният вариант представя мрежата като груба базова форма и детайлни wavelet коефициенти на последователни нива [8]. Конкретни data-hiding схеми модифицират избрани детайлни вектори чрез квантоване и ги възстановяват чрез синтез [9]. Работният поток е обобщен на фиг. 4. Предимствата са контрол върху честотния диапазон и потенциална устойчивост към определени обработки; недостатъците са по-висока изчислителна сложност и зависимост на базиса от дискретизацията на мрежата.

При големи или нерегулярни мрежи преобразуването може да се извършва върху подмрежи или чрез irregular wavelet разлагане. Ключът определя подмножеството коефициенти и параметрите на квантуване, а извличането трябва да възпроизведе същото разлагане. Това прави метода чувствителен към промени в свързаността: след remeshing собствените вектори и wavelet съответствията вече не описват същите позиции, дори когато видимата форма остава близка [1], [9].



Фиг. 4: Последователност на вграждането в спектрален/мултирезолюционен домейн.

3. Сравнителен анализ

3.1. Незабележимост и геометрична точност

Незабележимостта изисква визуално и статистически правдоподобен стего-модел. Геометричната разлика между оригиналната повърхност S и стего-повърхността T може да се оцени чрез симетричното разстояние на Hausdorff [10]:

$$d_H(\mathrm{S},\mathrm{T}) = \max\{\, sup_{s\in S}\, inf_{t\in T}\, \|\mathrm{s}-\mathrm{t}\|,\ sup_{t\in T}\, inf_{s\in S}\, \|\mathrm{t}-\mathrm{s}\| \,\} \quad (4)$$

където:

– $d_H(\mathrm{S},\mathrm{T})$ - симетрично разстояние на Hausdorff между S и T;

– S, T - сравняваните повърхности или множества от точки;

– s, t - точки съответно от S и T;

– sup, inf - съответно супремум и инфимум - те задават най-голямото от минималните отклонения.

Hausdorff оценката измерва най-голямото локално отклонение, но не моделира напълно човешкото възприятие. Затова е полезно да се допълни с перцептуална метрика като MSDM2, която използва многомащабни статистики на кривината [11]. При координатните и трансформните методи деформацията е резултат от промяна на геометрията; при топологичните методи тя възниква, когато двете триангулации на некопланарна четворка описват различни локални повърхности.

3.2. Капацитет

За сравнение между мрежи с различен размер payload-ът се нормализира като брой вградени битове на връх:

$$R_{bpv} = \frac{B}{N} \quad (5)$$

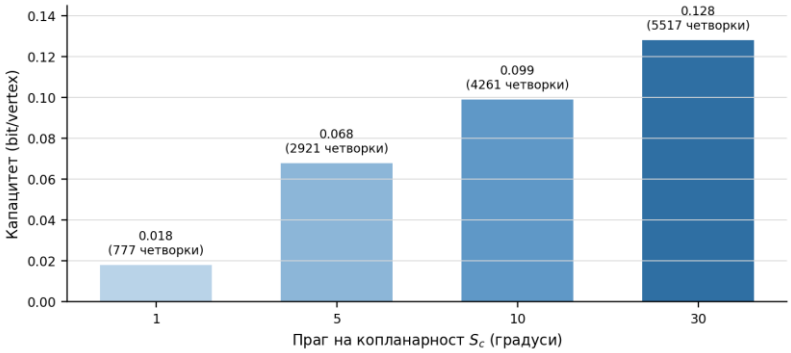
където:

– R_{bpv} - нормализиран embedding rate, измерен в bit/vertex (битове на връх);

– B - общ брой вградени битове;

– N - общ брой върхове на полигоналната мрежа.

Координатните методи обикновено имат най-голям потенциален капацитет, защото могат да използват множество върхове и координатни компоненти. Топологичните методи са ограничени от броя на допустимите независими четворки. При трансформните методи капацитетът зависи от броя на избраните коефициенти и нивата на разлагане; той не трябва да се обобщава с една стойност без конкретен алгоритъм и експериментална постановка.



Фиг. 5: Капацитет за модела Julius (43 039 върха) при различен праг Sc.

Както е показано на фиг. 5, по-големият праг допуска повече четворки и увеличава капацитета, но разширява множеството от локални конфигурации, при които промяната на диагонала може да е по-забележима.

3.3. Устойчивост към обработка

Координатните методи са уязвими към операции, които променят върховете - noise, Laplacian/Taubin smoothing, simplification и remeshing. Инвариантна нормализация може да защити от транслация, ротация и равномерно мащабиране, но не възстановява изгубени или пренаредени върхове [4].

Топологичният метод на Amat и съавт. е устойчив към заявените similarity трансформации, но не бива да се приема за доказано устойчив към smoothing само защото connectivity не се променя [6]. При remeshing и simplification самият топологичен носител се изменя. Спектралните и wavelet подходи могат да понесат по-добре определено изглаждане или шум, особено когато се използват по-глобални компоненти, но remeshing изменя Лапласиановия базис и съответствието на коефициентите [7], [9].

3.4. Сигурност и стегоанализ

3D стегоанализът извлича признаци от нормали, кривини, ъгли, дължини на ръбове, съседства или wavelet коефициенти и обучава класификатор да различава cover от stego. Yang и съавт. показват дискриминативен подход за 3D полигонални мрежи [12], а Li и Bors използват статистики на локални геометрични признаци и SVM/FLD ensemble [13]. За multiresolution вграждания могат да се използват статистики на wavelet вектори и преходи между нивата [14].

Ансамблите върху случайни подпространства са общ механизъм за високомерен стегоанализ [15]. Важният извод е, че ключът защитава достъпа до съобщението, но недетектируемостта зависи от статистическата близост между cover и stego. Следователно оценката трябва да включва разделени обучаващи и

тестови набори, разнообразни модели и сравнение при реалистични payload-и. Обобщението е представено в таблица 1.

Таблица 1. Обобщено сравнение на трите групи методи

Метод	Незабележимост и капацитет	Устойчивост	Сигурност / риск
Координатен	Фини геометрични промени; обикновено най-висок потенциален капацитет.	Добра към similarity трансформации при нормализация; слаба към smoothing, simplification и remeshing.	Откриваеми промени в нормали, кривини, ръбове и ъгли.
Топологичен	Запазва координатите; капацитетът зависи от допустимите четворки (≤0,25 bpv теоретично).	Заявена към транслация, ротация и равномерен мащаб; слаба към connectivity промени.	Възможни аномалии в съседства, степени на върхове и диедрални ъгли.
Трансформен	Контролира деформацията чрез избор на спектрални/wavelet коефициенти; капацитетът е алгоритъм-зависим.	Често по-добра към избрани шум и smoothing; проблемна при remeshing и смяна на базиса.	Откриваеми статистически следи в коефициентите или след обратната реконструкция.

Заключение

Сравнението показва, че няма универсално най-добър метод. Координатните схеми са подходящи при приоритет на капацитета и простата реализация, но са чувствителни към геометрична обработка и стегоанализ. Топологичните схеми запазват координатите, но са уязвими към ремеширане и опростяване. Трансформните схеми контролират честотния диапазон и могат да подобрят устойчивостта към част от обработките, но изискват по-сложни изчисления и стабилен базис.

Изборът изисква ясен модел на заплахата: очаквани обработки, допустима деформация, payload и знания на наблюдателя. Оценката трябва да измерва геометрично/перцептуално качество, грешка при извличане и детектируемост. Резултатите за robust watermarking не се пренасят автоматично към стеганографията: първата област оптимизира устойчивостта, а втората - недетектируемостта.

Литература

1. H. Zhou, W. Zhang, K. Chen, W. Li, N. Yu, "Three-Dimensional Mesh Steganography and Steganalysis: A Review," IEEE Transactions on Visualization and Computer Graphics, vol. 28, no. 12, pp. 5006–5025, 2022, doi: 10.1109/TVCG.2021.3075136.

2. F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn, "Information Hiding—A Survey," Proceedings of the IEEE, vol. 87, no. 7, pp. 1062–1078, 1999.
3. C. Cachin, "An Information-Theoretic Model for Steganography," Information and Computation, vol. 192, no. 1, pp. 41–56, 2004.
4. N. Aspert, E. Drelie Gelasca, Y. Maret, T. Ebrahimi, "Steganography for Three-Dimensional Polygonal Meshes," in Proc. SPIE 4471, Security and Watermarking of Multimedia Contents IV, 2002.
5. M.-W. Chao, C.-H. Lin, C.-W. Yu, T.-Y. Lee, "A High Capacity 3D Steganography Algorithm," IEEE Transactions on Visualization and Computer Graphics, vol. 15, no. 2, pp. 274–284, 2009.
6. P. Amat, W. Puech, S. Druon, J.-P. Pedeboy, "Lossless 3D Steganography Based on MST and Connectivity Modification," Signal Processing: Image Communication, vol. 25, no. 6, pp. 400–412, 2010, doi: 10.1016/j.image.2010.05.002.
7. R. Ohbuchi, A. Mukaiyama, S. Takahashi, "A Frequency-Domain Approach to Watermarking 3D Shapes," Computer Graphics Forum, vol. 21, no. 3, pp. 373–382, 2002.
8. M. Eck, T. DeRose, T. Duchamp, H. Hoppe, M. Lounsbery, W. Stuetzle, "Multiresolution Analysis of Arbitrary Meshes," in Proc. SIGGRAPH, pp. 173–182, 1995.
9. M. Hachani, A. Ouled Zaid, "Robust Mesh Data Hiding Based on Irregular Wavelet Transform," in Proc. EUSIPCO, pp. 1189–1193, 2012.
10. N. Aspert, D. Santa-Cruz, T. Ebrahimi, "MESH: Measuring Errors Between Surfaces Using the Hausdorff Distance," in Proc. IEEE ICME, vol. 1, pp. 705–708, 2002.
11. G. Lavoué, "A Multiscale Metric for 3D Mesh Visual Quality Assessment," Computer Graphics Forum, vol. 30, no. 5, pp. 1427–1437, 2011.
12. Y. Yang, R. Pintus, H. Rushmeier, I. Ivrissimtzis, "A Steganalytic Algorithm for 3D Polygonal Meshes," in Proc. IEEE ICIP, pp. 4782–4786, 2014.
13. Z. Li, A. G. Bors, "Steganalysis of 3D Objects Using Statistics of Local Feature Sets," Information Sciences, vols. 415–416, pp. 85–99, 2017, doi: 10.1016/j.ins.2017.06.011.
14. Z. Li, A. G. Bors, "Steganalysis of Meshes Based on 3D Wavelet Multiresolution Analysis," Information Sciences, vol. 522, pp. 164–179, 2020.
15. J. Kodovský, J. Fridrich, "Steganalysis in High Dimensions: Fusing Classifiers Built on Random Subspaces," Proc. SPIE 7880, Media Watermarking, Security, and Forensics III, 2011.
16. S. Parvanov, "Research of Different Turbo Code Speeds, Types of Modulations, Decoding Methods and Their Compatibility with Encryption Techniques," Environment. Technology. Resources. Proceedings of the 15th International Scientific and Practical Conference, vol. II, pp. 232–236, 2024, doi: 10.17770/etr2024vol2.8037.
17. D. Dimitrov, M.-A. Kirov, "Using Multi-Carrier Probing Signals for Detecting Non-Linear Objects," Scientific Research and Education in the Air Force—

AFASES 2016, "Henri Coandă" Air Force Academy, Brașov, Romania, pp. 247–250, 2016, doi: 10.19062/2247-3173.2016.18.1.33.

18. V. T. Stoyanova, "Steganography System Using LSB Methods," Proceedings of the ENTRENOVA—ENTerprise REsearch InNOVAtion Conference, Split, Croatia, vol. 4, pp. 381–387, 6–8 September 2018.

MODELING AND ANALYSIS OF A COMMUNICATION CHANNEL IN THE GNU RADIO SIMULATION ENVIRONMENT

Vladislava S. Georgieva

Radar and Communication Systems Department, Artillery, Air Defense, Communication and Information Systems Faculty, National Military University „Vasil Levski", Shumen, Bulgaria
vladgs_93@abv.bg,

Abstract: *This report presents a step-by-step approach to the simulation modeling of a communication channel in GNU Radio Companion (GRC). A basic signal path is constructed, to which Additive White Gaussian Noise (AWGN) is sequentially added using the Channel Model block; a real-time Signal-to-Noise Ratio (SNR) measurement circuit is implemented, and the resulting signal values are compared against a theoretical formula. Additionally, the effects of frequency offset and clock error (Epsilon) on the signal spectrum and the stability of the measured power are investigated.*

Keywords: *communication channel, modeling, GNU Radio, SNR*

МОДЕЛИРАНЕ И ИЗСЛЕДВАНЕ НА КОМУНИКАЦИОНЕН КАНАЛ В СИМУЛАЦИОННА СРЕДА GNU RADIO

Владислава С. Георгиева

Катедра „Радарни и комуникационни системи", факултет „Артилерия, противовъздушна отбрана, комуникационни и информационни системи", гр. Шумен към Национален военен университет „Васил Левски", България
vladgs_93@abv.bg

Резюме*: В настоящия доклад е представен поетапен подход за симулационно моделиране на комуникационен канал в GNU Radio Companion (GRC). Изграден е базов сигнален път, върху който последователно е добавен адитивен бял Гаусов шум (AWGN) чрез блока Channel Model, реализирана е верига за измерване на съотношението сигнал/шум (SNR) в реално време, а получените стойности са съпоставени с теоретична формула. В допълнение са изследвани ефектите на честотното отместване (offset) и тактова грешка (Epsilon) върху спектъра на сигнала и стабилността на измерваната мощност.*

Ключови думи: *комуникационен канал, моделиране, GNU Radio, SNR*

1. Въведение

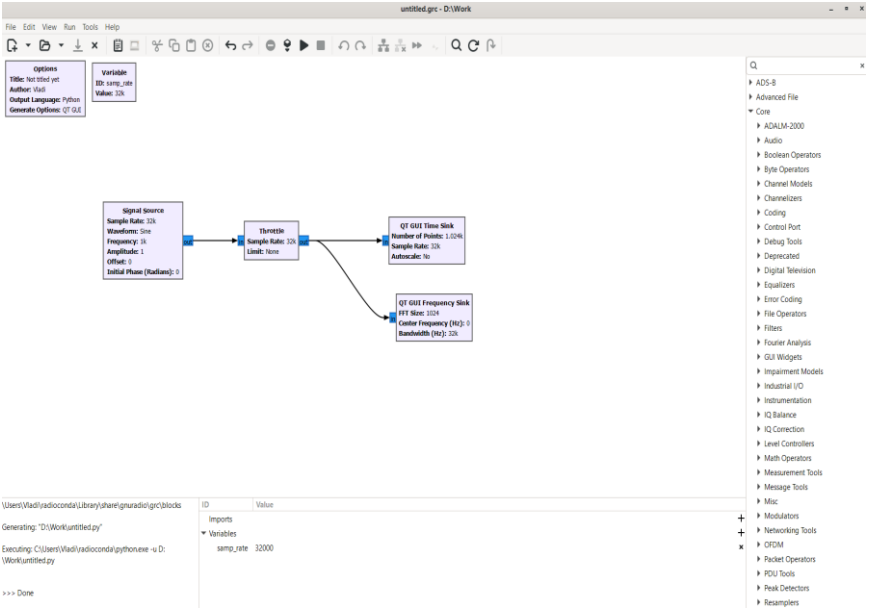
Моделирането на канала се определя като процес на създаване на точни и адекватни математически представяния на комуникационната среда с цел подобряване на ефективността на безжичните комуникационни системи, като същевременно се отчитат предизвикателства, породени от несъвършенствата и нелинейностите, характерни за сложни комуникационни сценарии. [1]

Симулационното моделиране на комуникационен канал е основен инструмент за изучаване на поведението на радиосистемите преди тяхната физическа реализация. GNU Radio Companion (GRC) предоставя графична среда за изграждане на сигнално-обработващи вериги (flowgraph-и) чрез свързване на готови функционални блокове, без необходимост от писане на код на ниско ниво. Наложените шумови процеси и кондуктивните смущения в канала нарушават качеството на предавания сигнал [2]. Целта на настоящата работа е да илюстрира стъпка по стъпка тези процеси като се започне с на генериране на тестов сигнал, добавяне на несъвършенства на канала — шум, честотно отместване и тактова грешка и се пристъпи към количествено измерване на въздействието на тези несъвършенства чрез изчисляване на SNR в реално време.

2. Проектиране на комуникационен канал и експериментална част

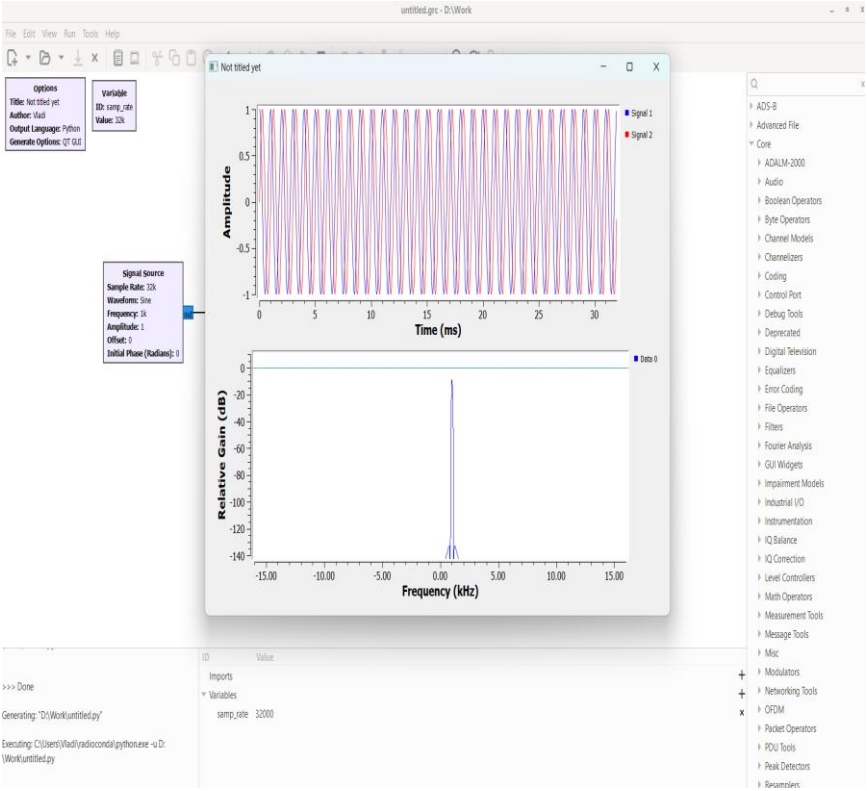
2.1 Изграждане на базов сигнален път

Преди въвеждането на какъвто и да е канален ефект е необходимо да се изгради работещ „чист" сигнален път, който служи като еталон за сравнение. Използван е блок Signal Source, генериращ комплексна синусоида с честота 1 kHz и амплитуда 1, при честота на дискретизация (Sample Rate) 32 kHz. Блокът Throttle ограничава скоростта на обработка до зададената честота на дискретизация, за да се избегне ненужно натоварване на процесора при симулация без реален хардуер.



Фиг. 1: Базова сигнално-обработваща верига (flowgraph):
Signal Source → Throttle → QT GUI Time/Frequency Sink.

Резултатът от изпълнението на този базов flowgraph е показан на Фиг. 2 — синусоидален сигнал с постоянна амплитуда във времевата област и ясно изразен единичен пик на честота 1 kHz в честотния спектър.

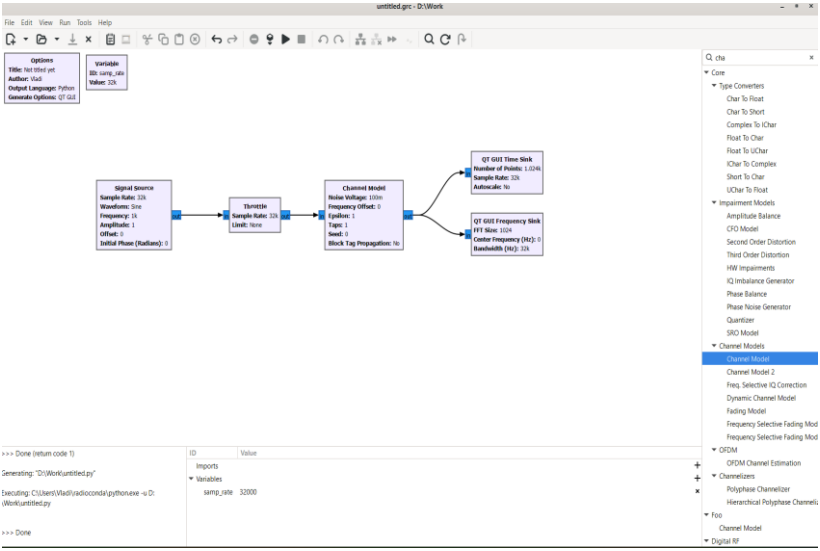


Фиг. 2: Времева форма и честотен спектър на чист синусоидален сигнал
(без канални изкривявания).

2.2. Добавяне на адитивен бял Гаусов шум (AWGN)

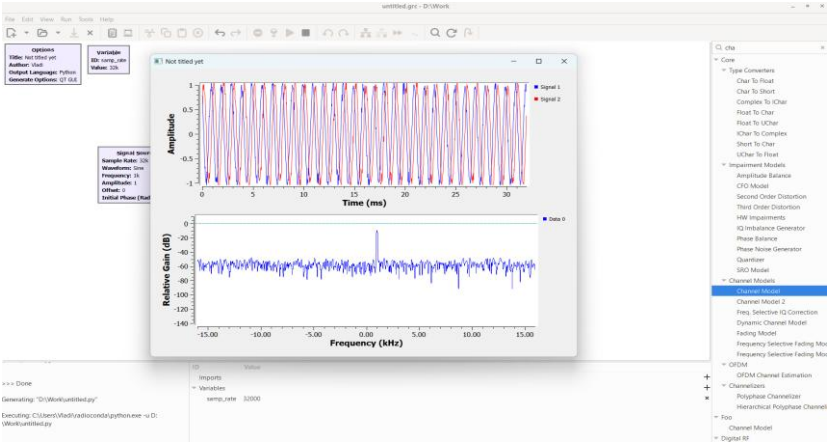
За моделиране на шумов канал е използван блокът **Channel Model** от библиотеката **Channel Models**, включен между блока **Throttle** и крайните (изходни) блокове, използвани за визуализация на сигнала. Блокът позволява независимо конфигуриране на няколко канални ефекта: Noise Voltage (мощност на AWGN шума), Frequency Offset (честотно отместване), Epsilon (тактова грешка),

Taps (импулсен отговор на канала, за многолъчево разпространение) и Seed (начално число на генератора на случайни числа, за възпроизводимост на резултатите) [3].

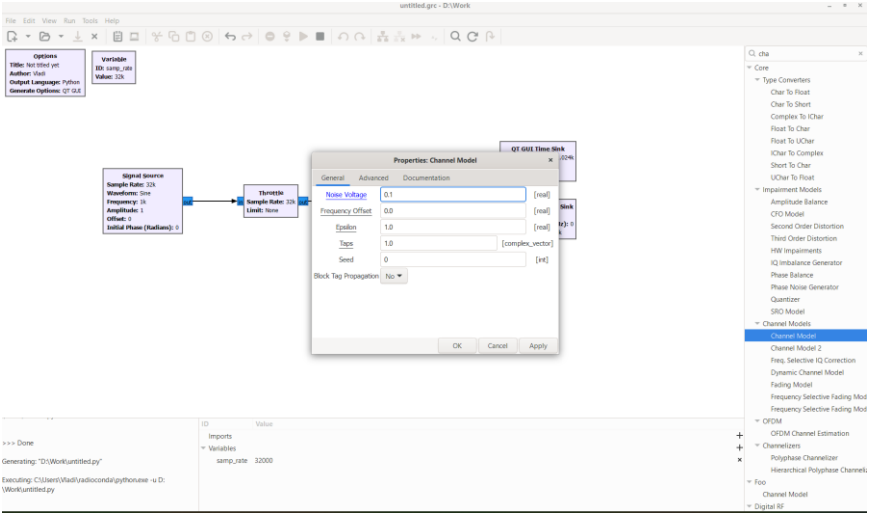


Фиг. 3: Flowgraph с добавен блок Channel Model между Throttle и sink-овете.

При зададена стойност на Noise Voltage сигналът вече не е чиста синусоида — както във времевата, така и в честотната област се появява фонов шум, а полезният сигнал остава разпознаваем като доминиращ пик на фона на равномерно разпределения шум (Фиг. 4).



Фиг. 4: Времева форма и спектър на сигнала след добавяне на AWGN шум чрез Channel Model.



Фиг. 5: Диалогов прозорец с параметрите на блока Channel Model (Noise Voltage, Frequency Offset, Epsilon, Taps, Seed).

2.3. Измерване на съотношението сигнал/шум (SNR) в реално време

Архитектура на измервателната верига

За количествена оценка на въздействието на шума е реализирана допълнителна сигнално-обработваща верига, която изчислява средната мощност на сигнала преди

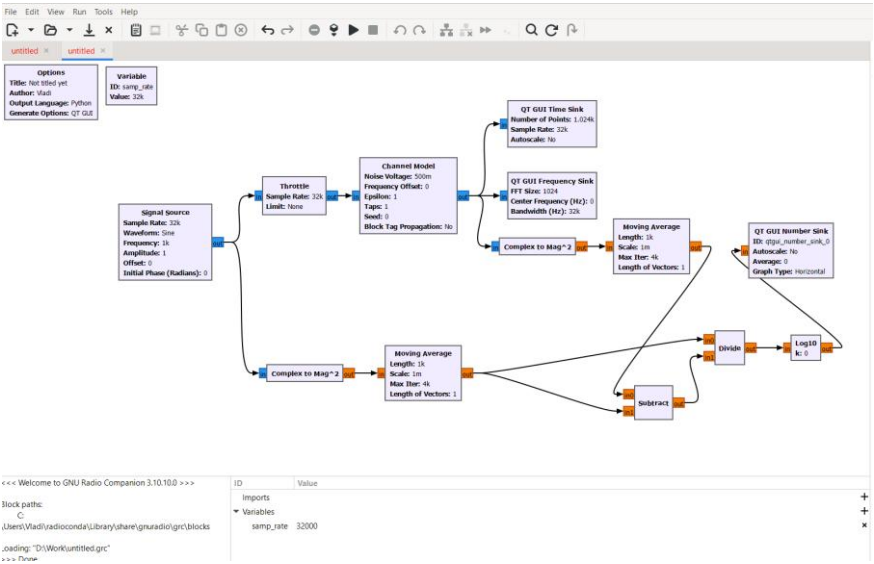
и след Channel Model и от тях извежда SNR в децибели. **SNR** най-често се изразява в **децибели (dB)**, които представляват логаритмична мерна единица. Тази логаритмична скала се използва, тъй като мощността на сигнала и мощността на шума могат да варират в изключително широки диапазони. Изразяването им в децибели (dB) позволява този диапазон да бъде значително компресиран, като същевременно съответства на начина, по който човек възприема промените в интензитета, например промяната в силата на звука. [4] Веригата се състои от следните елементи, дублирани за двата клона (чист сигнал и сигнал+шум):

Complex to Mag² — изчислява моментната мощност $|x(t)|^2$ от комплексния сигнал; Moving Average (Length = 1000, Scale = 1/1000) — осреднява последните 1000 отчета, за да получи средна мощност вместо сума.

Средните мощности на двата клона (P_{signal} — от чистия сигнал преди канала, и P_{total} — от сигнала след Channel Model) се подават към блоковете Subtract, Divide и Log10, реализиращи израза:

$$P_{noise} = P_{total} - P_{signal}\ , \quad SNR_{linear} = P_{signal} / P_{noise}\ , \quad SNR_{dB} = 10 \cdot log_{10}(SNR_{linear})$$

Резултатът се визуализира чрез блок QT GUI Number Sink.



Фиг. 6: Пълна измервателна верига за SNR: два успоредни клона (P_{signal} и P_{total}), последвани от Subtract → Divide → Log10 → QT GUI 2.Number Sink.

Теоретична формула

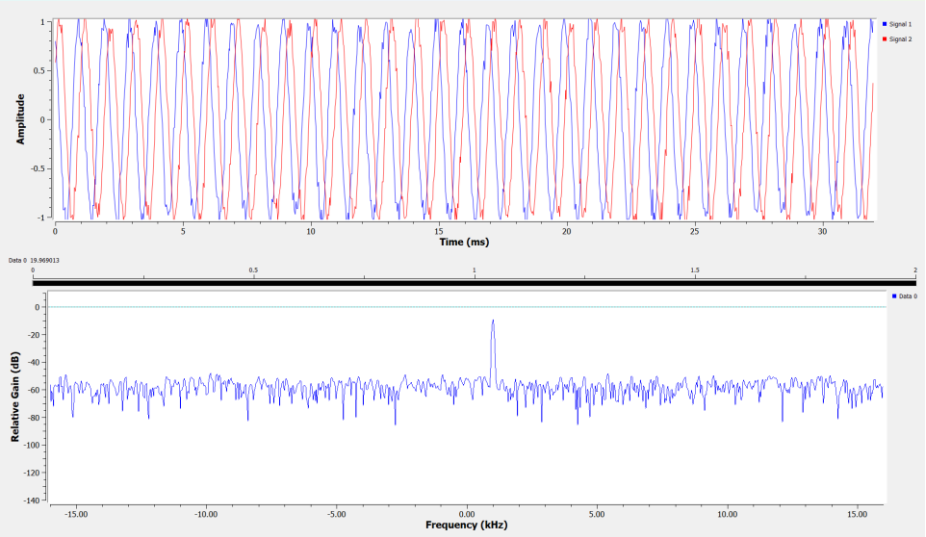
Blocks Signal Source генерира комплексна синусоида $s(t) = A \cdot e^{j(2\pi ft + \varphi)}$, чийто модул е постоянен във времето, следователно средната мощност на сигнала е $P_{signal} = A^2$. Параметърът Noise Voltage (σ) на Channel Model задава амплитудата на комплексния AWGN шум, чиято обща мощност е $P_{noise} = \sigma^2$. От това следва:

$$SNR_{dB} = 10\log_{10}\left(\frac{A^2}{\sigma^2}\right) = 20\log_{10}\left(\frac{A}{\sigma}\right)$$

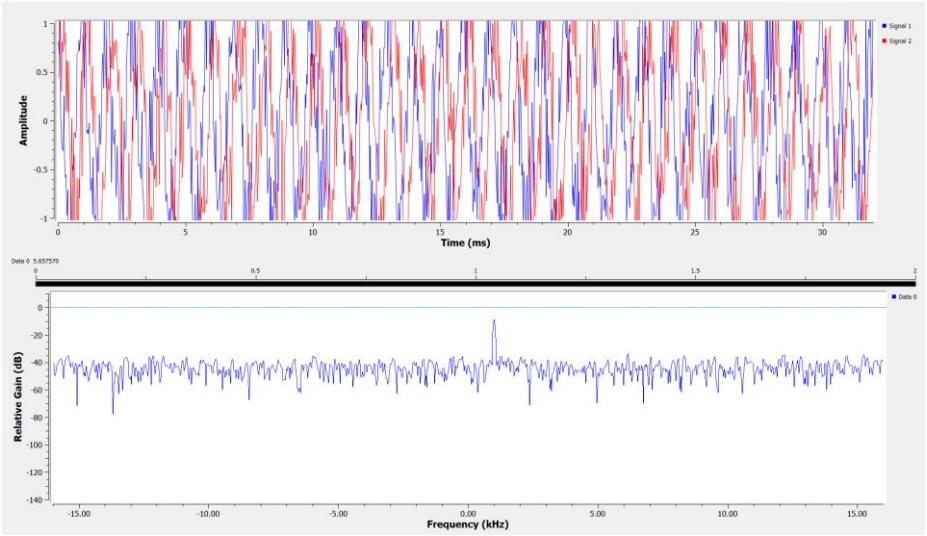
При единична амплитуда ($A = 1$) изразът се опростява до $SNR_{dB} = -20 \cdot \log_{10}(\text{Noise Voltage})$.

Съпоставка теория – измерване

Получените експериментални резултати за две стойности на Noise Voltage са показани на Фиг. 7 и Фиг. 8 и обобщени в Таблица 1.



Фиг. 7: Измерено SNR при Noise Voltage = 0.1: SNR ≈ 19.97 dB.



Фиг. 8: Измерено SNR при Noise Voltage = 0.5: SNR ≈ 5.66 dB.

Таблица 1.

Съпоставка на теоретично изчисленото и експериментално измереното SNR.

Noise Voltage (σ)	**Теоретично SNR, dB**	**Измерено SNR, dB**	**Отклонение, dB**
0.1	20.00	19.97	0.03
0.5	6.02	5.66	0.36

Наблюдаваната малка разлика между теоретичната и измерената стойност се дължи на факта, че Moving Average осреднява мощността само върху краен прозорец от 1000 отчета, а не върху безкраен ансамбъл — статистическа флуктуация от порядъка на десети от децибел е очаквана и намалява с увеличаване на дължината на осредняващия прозорец.

2.4. Ефекти на честотното отместване (Frequency offset) и тактовата грешка (Epsilon)

Освен адитивния шум, Channel Model позволява моделиране на две допълнителни несъвършенства, характерни за реални радиосистеми, честотно отместване frequency offset (несъответствие между локалните осцилатори на предавател и приемник) и тактова грешка Epsilon (несъответствие в честотата на дискретизация между предавателя и приемника). За систематично изследване на тези два ефекта, самостоятелно и в комбинация с нивото на шум, е приложен пълен

факторен експеримент с два нива за всеки от трите параметъра (Frequency Offset, Epsilon, Noise Voltage), т.е. общо 2×2×2 = 8 конфигурации.

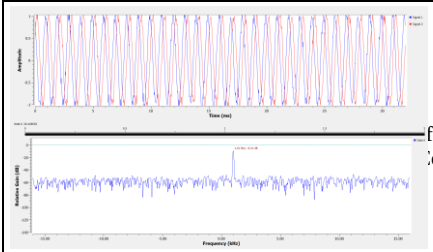
Важна забележка относно характера на измерванията

Преди да бъдат разгледани резултатите, е необходимо изрично да се подчертае едно съществено свойство на измервателната верига, показанията на QT GUI Number Sink (SNR) и позицията на спектралния пик не са установени, постоянни величини. Сигналът, преминаващ през Channel Model, непрекъснато осцилира — във всяка секунда от изпълнението на flowgraph-а мигновената амплитуда и фаза се променят, а блокът Moving Average преизчислява осредната мощност върху непрекъснато обновяващ се („плъзгащ") прозорец от последните 1000 отчета. В резултат на това всяко число, уловено на екрана в определен момент, представлява само една единична моментна извадка от непрекъснато трептяща величина, а не възпроизводим, стабилен резултат. Повторно заснемане при абсолютно същите зададени параметри на Channel Model дава различна конкретна стойност на SNR и на позицията на пика. Стойностите, представени по-долу, следва да се тълкуват именно в този смисъл — като илюстративни моментни отчети, а не като „резултата" за дадена конфигурация.

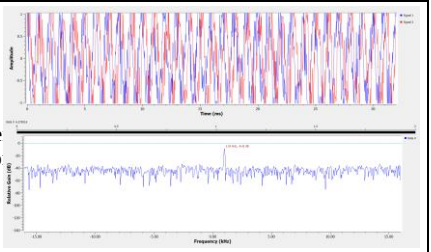
Методология — пълен факторен експеримент

Параметърът Frequency Offset е нормиран спрямо честотата на дискретизация: f_{offset}[Hz] = Frequency Offset × Sample Rate. При Sample Rate = 32 kHz, теоретично очакваната позиция на спектралния пик е 1000 Hz при Frequency Offset = 0, и 1000

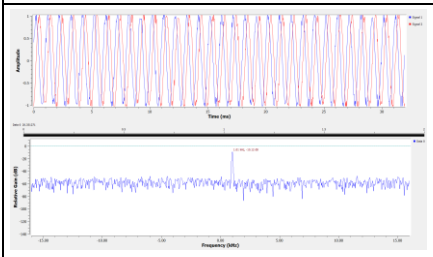
+ 0.01×32000 = 1320 Hz ≈ 1.32 kHz при Frequency Offset = 0.01. Параметърът Epsilon моделира тактова грешка (Epsilon = 1.0 — идеално съвпадение; Epsilon = 1.001 — 0.1% отклонение), която не измества позицията на пика по забележим начин, но допринася за описаната по-горе нестационарност на сигнала. Осемте изследвани конфигурации, заедно с теоретично очакваните стойности, са показани в Таблица 2.



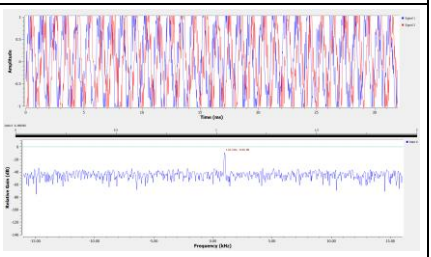
Фиг. 9. Offset=0, Epsilon=1.0, Noise=0.1 — моментна извадка: SNR ≈ 26.43 dB, пик 1.01 kHz.



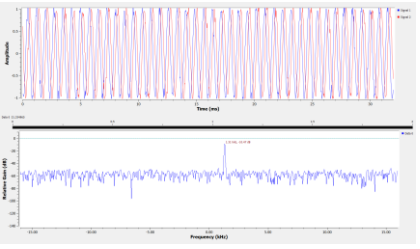
Фиг. 10. Offset=0, Epsilon=1.0, Noise=0.5 — моментна извадка: SNR ≈ 6.28 dB, пик 1.01 kHz.



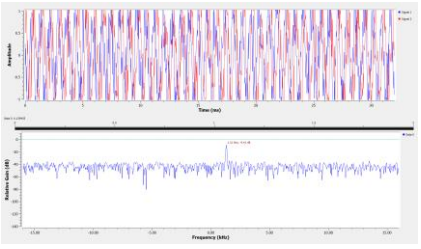
Фиг. 11. Offset=0, Epsilon=1.001, Noise=0.1 — моментна извадка: SNR ≈ 20.35 dB, пик 1.01 kHz.



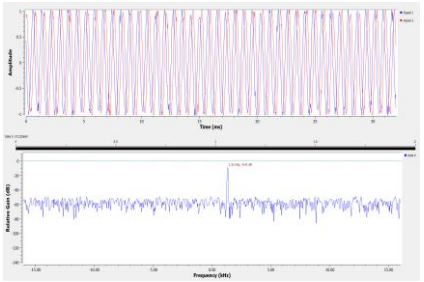
Фиг. 12. Offset=0, Epsilon=1.001, Noise=0.5 — моментна извадка: SNR ≈ 6.39 dB, пик 1.01 kHz.



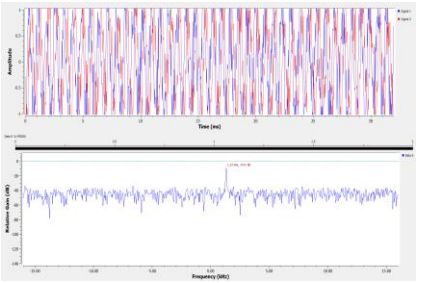
Фиг. 13. Offset=0.01, Epsilon=1.0, Noise=0.1 — моментна извадка: SNR ≈ 21.33 dB, пик 1.31 kHz.



Фиг. 14. Offset=0.01, Epsilon=1.0, Noise=0.5 — моментна извадка: SNR ≈ 6.13 dB, пик 1.31 kHz.



Фиг. 15. Offset=0.01, Epsilon=1.001, Noise=0.1 — моментна извадка: SNR ≈ 27.23 dB, пик 1.31 kHz.



Фиг. 16. Offset=0.01, Epsilon=1.001, Noise=0.5 — моментна извадка: SNR ≈ 6.48 dB, пик 1.33 kHz.

Таблица 2.

Пълен факторен план на експеримента (2×2×2) с теоретично очаквани стойности.

№	Frequency Offset	Epsilon	Noise Voltage	Teo. SNR, dB	Теоретична стойност на честотата f_пик [kHz]
1	0	1.0	0.1	20.00	1.00
2	0	1.0	0.5	6.02	1.00
3	0	1.001	0.1	20.00	≈1.00
4	0	1.001	0.5	6.02	≈1.00
5	0.01	1.0	0.1	20.00	1.32
6	0.01	1.0	0.5	6.02	1.32
7	0.01	1.001	0.1	20.00	≈1.32
8	0.01	1.001	0.5	6.02	≈1.32

Резултати — моментни извадки

За всяка от осемте конфигурации е заснета по една моментна извадка (Фиг. 9–16), чиито стойности за SNR и позиция на пика са обобщени в Таблица 3. Отново се подчертава: посочените стойности са единични отчети в конкретен момент, а не установени средни резултати (виж 5.1).

Таблица 3.

Обобщение на моментните извадки от осемте конфигурации (виж 5.1 относно характера на стойностите).

№	Frequency Offset	Epsilon	Noise Voltage	Изм. SNR*, dB	Измерена стойност на честотата f_пик* [kHz]
1	0	1.0	0.1	26.43	1.01
2	0	1.0	0.5	6.28	1.01
3	0	1.001	0.1	20.35	1.01
4	0	1.001	0.5	6.39	1.01
5	0.01	1.0	0.1	21.33	1.31
6	0.01	1.0	0.5	6.13	1.31
7	0.01	1.001	0.1	27.23	1.31
8	0.01	1.001	0.5	6.48	1.33

* Единична моментна извадка в конкретен момент от изпълнението — стойността се променя непрекъснато във всяка следваща секунда (виж 5.1).

Изводи от проведените експерименти

Изместване на спектралния пик. Във всичките четири конфигурации с Frequency Offset = 0.01 (Фиг. 13–16) пикът се наблюдава в диапазона 1.31–1.33 kHz, много близо до теоретично очакваната стойност 1.32 kHz, независимо от стойността на Epsilon и Noise Voltage. При Frequency Offset = 0 (Фиг. 9–12) пикът остава практически на изходната честота (1.01 kHz срещу теоретични 1.00 kHz). Това потвърждава, че честотното отместване произвежда предвидимо, възпроизводимо изместване на спектъра, което не зависи осезателно от наличието на Epsilon или от нивото на шума. За разлика от позицията на пика, единичните отчети на SNR показват забележимо по-голямо отклонение спрямо теоретично очакваните стойности — и то по различен начин в зависимост от нивото на шум. При Noise Voltage = 0.5 (Фиг. 10, 12, 14, 16) моментните стойности са скупчени в тесен диапазон 6.13–6.48 dB, много близо до теоретичните 6.02 dB. При Noise Voltage = 0.1 (Фиг. 9, 11, 13, 15) моментните стойности варират много по-широко — от 20.35 до 27.23 dB — спрямо теоретични 20.00 dB. Възможно обяснение на тази асиметрия произтича пряко от начина, по който се изчислява SNR във веригата: P_{noise} се получава като разлика $P_{total} - P_{signal}$ между две близки по стойност мощности, когато шумът е слаб (Noise Voltage = 0.1). Изваждането на две близки числа усилва относителната грешка в резултата (числено съкращаване), поради което малки моментни колебания на P_{total} или P_{signal} се отразяват значително по-силно върху крайната стойност на SNR. При по-силен шум (Noise Voltage = 0.5) стойността на P_{noise} е значително по-голяма спрямо тези колебания, което дава по-стабилни и по-възпроизводими моментни отчети. Тази хипотеза е в съответствие с наблюдаваните данни, но не е допълнително верифицирана чрез повторни измервания в рамките на настоящата работа.Във всеки случай, представените стойности на SNR не следва да се четат като „установеният резултат" за дадена конфигурация на Noise Voltage — те са единствено примерни моментни отчети, илюстриращи, че сигналът и производните от него величини (в т.ч. SNR) остават в непрекъснато трептящо състояние през цялото изпълнение на flowgraph-a, а не се стабилизират до константа.

Заключение

В настоящата работа беше изграден, стъпка по стъпка, симулационен модел на комуникационен канал в GNU Radio, включващ адитивен бял Гаусов шум, честотно отместване и тактова грешка. За чисто AWGN канал (без offset и epsilon) измерените стойности на SNR съвпаднаха добре с теоретичната формула $SNRdB = 20 \cdot \log_{10}(A/\sigma)$. При включени честотно отместване offset и тактова грешка Epsilon, проведеният пълен факторен експеримент показа, че изместването на спектралния пик е предвидим и възпроизводим ефект, докато моментните отчети на SNR остават чувствителни към непрекъснатото трептене на сигнала и зависят от режима на работа (по-голямо отклонение при слаб шум, по-стабилни отчети при по-силен шум). Това е важно наблюдение: единично измерване на SNR в присъствието на тактова грешка не е достатъчно представително и изисква многократно повторение или по-дълъг период на осредняване за получаване на надеждна оценка. Като

насока за бъдещо разширение на изследването може да се посочи преминаването от аналогов тестов сигнал към реална цифрова модулация (напр. BPSK) и изчисляване на честотата на битовите грешки (BER) като функция на SNR, което би позволило директно сравнение с теоретичната крива:

$$BER = \frac{1}{2}\,\mathrm{erfc}(\sqrt{SNR}) \qquad [5]$$

Литература

1. https://www.sciencedirect.com/topics/engineering/channel-modeling
2. Linko G. Nikolov "Error rate analysis in ricean channel and complex radio environment" International Scientific Conference "Defense Technologies" Shumen, 2016, ISSN: 2367-7902
3. https://www.gnuradio.org/doc/doxygen/classgr_1_1channels_1_1channel__model.html
4. https://resources.l-p.com/glossary/snr-signal-to-noise-ratio-and-its-impact-on-signal-quality
5. ELECHI, P. C. et al. Performance Analysis of BER and SNR of BPSK in AWGN Channel. International Journal of Digital Communication and Analog Signals, 2021, Vol. 7, No 1, p. 27–38.

IMPACT OF ASSESSMENT INDICATORS ON CONTENT GENERATED BY LARGE LANGUAGE MODELS

Miroslav G. Nedelchev

Computer Systems and Technologies Department, Artillery, Air Defense Communication and Information Systems Faculty, National Military University "V. Levski ", Shumen , Bulgaria
nedel4ew@ abv . bg

***Abstract**: The rapid proliferation of Large Language Models (LLMs) underscores the challenge of automated quantitative evaluation, given that natural language allows identical semantic content to be expressed through diverse syntactic and lexical structures. To address this gap, this paper analyzes classical statistical methods alongside modern semantic evaluation techniques, examining their systemic impact on model generation and their technical limitations.*

***Keywords:** Computational Linguistics / Artificial Intelligence and Natural Language Processing (NLP)*

Introduction

The rapid development and massive integration of Large Language Models (LLMs) in modern information architectures has brought to the forefront the issue of their objective, automated and quantitative evaluation. Natural language generation is characterized by a high degree of variability, in which the same semantic construct can be synthesized through multiple alternative syntactic and lexical structures. This makes determining the quality of the source text a complex challenge from both a theoretical and practical point of view. Historically, evaluation methodologies began with statistical text processing based on N-gram matching — an approach embodied in classical algorithms such as BLEU and ROUGE, and later extended by including morphological and synonymic relationships in METEOR [1] [2], [3]. However, the increasing content and contextual complexity of modern architectures requires a transition from pure lexical accuracy to semantic analysis through vector embeddings and contextual modeling. The choice of a particular evaluation metric directly influences the optimization function, the fine-tuning of large language models, and the final structure of the text generated by the model.

This report also analyzes classical statistical approaches and their influence on modern semantic methods for evaluating generated content and limitations.

1 Natural language generation

Natural language generation deals with creating new, meaningful text based on understanding an existing one and structuring it into sentences that sound like natural language reproduced in physical form by a human.

Finding a match using a given pattern provides a set of information about:

— the part of the text that matches the pattern;
— the index in the string where the match begins;
— any part of the text corresponding to the parts in brackets within the template;

— string before/after the matched text.

It turns out that this information is not enough for ambiguity or comprehension/generation in natural language processing. The recognition of individual constructs to predict the next element (word, symbol, or letter) in a sequence is called *an N-gram* model. The calculation of the probability of the occurrence of the next word is closely related to the calculation of the probability of a sequence of $N-1$ words. Using only lexical N-gram-based scoring metrics systematically distorts the objective assessment of the generated text, as it favors literal surface matching at the expense of semantic coherence. Integrating metrics based on vector embeddings and contextual analysis allows for a syntax-invariant reflection of actual content matching.

The resulting ambiguities in natural languages, the computational complexity of computer processing, and the detection of references related to elements in linguistic representation are fundamental problems. Context detection will be directly related to previous sentences, pronouns, and definite articles across entire paragraphs and chapters.

To overcome this problem, computational linguistics applies basic grammatical rules, recognizing names, places, time, periods, seasonal times, connecting words in pairs, using fragments and assigning them to one or another group of extended context windows in order to provide additional information in the models of context, structured knowledge and long-term memory. With the mass penetration and use of transformer neural networks, the Theory of Centering [4] finds increasing application, with each sentence (or discourse unit) being considered as a set of centers (objects that are being talked about). For example, in the Bulgarian language, a common construction has the form *Subject - Direct Object - Indirect Object - Other Part.*

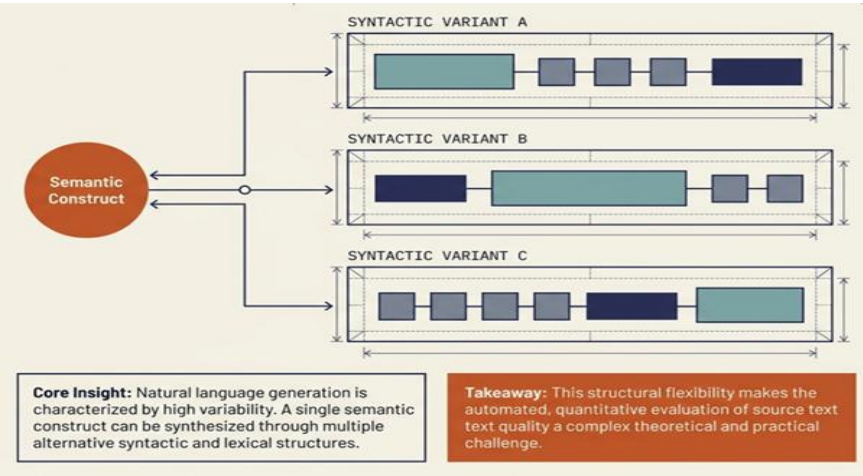


Figure 4: The generative ambiguity problem

According to centering theory, centers (a list of all objects mentioned in a sentence, ordered by importance based on their syntactic role) are first proposed, and the object at the top of this list is called the preferred center. Then, a center related to a previous sentence or object, with the highest priority, and a transition from one sentence to the next, in which the focus can be maintained or changed.

There are 4 main possible cases during the transition:

- The theme is retained and continues to be the main focus;
- The subject remains, but the focus begins to shift to another object;
- The topic changes, but the new object has already been prepared as important;
- Abrupt change of subject – creates confusion.

There are also probabilistic models [5] [6]obtained by training specially prepared small corpora and are based on information about the distance between the pronoun and its antecedent, syntactic constraints, number and gender, interaction between the main component of the pronoun and the antecedent, number of mentions - the more times a given referent has appeared in the discourse, the more likely it is to be the antecedent.

- For a pronoun p, to refer to an antecedent $a$and , using feature sets $F(f_i)$taking into account the Bayes distribution.

$$P\ a|\ p, F = \frac{P(a)\prod_{i=o}^{n} P\ (f_i|\ a)}{P(F)} \tag{1}$$

- Maximum entropy models [7]– remove the Bayes constraint on feature independence and allow for the combination of many overlapping features. For a given pair of candidate antecedents aand a pronoun m, the probability athat it is the correct object is calculated as:

$$P\ a|\ m = \frac{e^{\sum_i w_i f_i(a,m)}}{\sum_{a' \in A} e^{\sum_i w_i f_i(a',m)}} \tag{2}$$

where $f_i(a, m)$are binary features (e.g., "1 if they match by gender, 0 otherwise, and w_i are the weight coefficients that the model derives).

- Hidden Markov Models [8]– view the text as a sequence of states, where the real objects are hidden states, and the words used (pronouns, nouns) are observed emissions.

With the development of transformer neural networks and machine learning algorithms, the input text is divided into smaller parts called tokens (phrases, words or parts thereof), which are assigned a unique identification number (ID) from a predefined dictionary. To enable computer processing in terms of semantics of these tokens, they are converted into vectors of real numbers and recorded in an embedding matrix, which allows the representation of words in a low-dimensional continuous semantic space, where words similar in meaning are located close to each other.

Techniques for implementing vector embeddings are mainly classified into three groups: frequency-based, probabilistic, and contextual. Frequency-based techniques, such as TF-IDF (Term Frequency - Inverse Document Frequency), measure the frequency of

occurrence of a term in a document relative to its uniqueness in the entire collection of documents, defining a weighting factor for each term. Probabilistic techniques, among which Word2Vec, GloVe, and FastText stand out, are based on neural networks trained to predict words in a given local context window or using global data for the joint use of words from the entire corpus.

Table 1: Comparative analysis of the main vector representation techniques (Word Embeddings)

Technique	Class / Type	Main advantages	Main limitations
TF-IDF	Frequency-based	Easy implementation, reflects the uniqueness of words in documents	Does not account for semantic relations and word order; large sparse vectors
Word2Vec	Probabilistic / Local	Captures strong semantic similarities and analogies between individual words	Limited ability to work with non-dictionary words without N-grams
GloVe	Probabilistic / Global	Uses global statistics across the entire corpus for richer vectors	High computational demands when factoring huge matrices
Node2Vec	Graph embedding	Efficiently preserves structural distances and dependencies in network graphs	Requires expensive crawls and can slow down searches on large graphs

The expression, manner, form, style, and richness of language are a creative process and are difficult to replicate or compare. Modern AI models work not with letters but with embeddings—vectors of semantic proximity [2]. They measure distances in space where meaning appears as a configuration, not as meaning. The question of text quality therefore becomes a question of how structurally accurate the system's response is [3]. However, in natural language processing, assessing the quality of generated text is important for a model's ability to perform adequately. For this purpose, the evaluation indicators BLEU (Bilingual Evaluation Understudy) and ROUGE (Recall Oriented Understudy for Gisting Evaluation) [2]and METEOR have been introduced, which have gained widespread application and are often used to compare machine-generated output with a reference text, with one or more reference texts written by a human, i.e. they quantify the correspondence between the generated content and the expected result in terms of accuracy and relevance, which makes the evaluation objective and easy to scale.

*BLEU*measures how closely the match between a generated text and a reference text is. The practical implementation uses *N-gram* comparisons, but a restriction is introduced for sequences that are too short R to avoid artificially inflated scores [1].

$$P_N = \frac{\sum N \min\left(Count_{Generation}, Count_{Reference}\right)}{\sum N \, Count_{Reference}}$$
$$R = \begin{cases} 1 \ , & ako \ g > r \\ e^{(1-g/r)}, & ako \ g \leq r \end{cases} \quad (3)$$

$$BLEU = R.e^{\sum_{n=1}^{N} w_n \log(P_N)} \quad (4)$$

where $g$is the length of the generated text, $r$is the length of the reference text, $w_n$is the weight coefficient.

The BLEU-based assessment is characterized by simplicity, high computational efficiency, validation, and widespread use, but it also has some serious limitations such as dependence on the number of responses to references in the text, insensitivity to synonyms and paraphrasing; poor understanding of context. In other words, the comparison of sequences may be objective, but superficial, i.e. it measures similarity of form but not semantic relationships.

ROUGE (Recall-Oriented Understudy for Gisting Evaluation) was first proposed in 2004 by researcher Chin-Yu Lin at Stanford University (USA) [9]to assess the quality of automatic summaries generated by systems.

ROUGE uses two key metrics [3]for [9] [10]evaluation, precision and completeness. Precision measures the proportion of the model's words that match the reference text, while completeness measures the proportion of the reference words that are present in the generated text. The final score is calculated by combining both metrics. If the model repeats phrases from the reference text but omits details, then it has high precision and low completeness. In text generation systems, a balance is sought between conciseness and richness, without verbatim repetition, but preserving context and key ideas.

The advantages are sensitivity to information content, ability to assess semantic overlaps between different formulations, flexibility. A limiting feature is the dependence on literal matches, so if a model conveys the same idea in different words, ROUGE often rejects it.

It is most commonly used in three variants – ROUGE-N (measures overlapping *N-gram* matches, ROUGE-L (based on the longest common subsequence LCS) and ROUGE-S (measures matches of omitted bigrams, allowing the inclusion of words that are located at a distance from each other).

$$\text{ROUGE} - \text{N} = \frac{\sum N \min(Count_{Generation}, Count_{Reference})}{\sum N \, Count_{Reference}} \quad (5)$$

$$\text{ROUGE} - \text{LCS} = \frac{\text{LCS}(Generation, Reference)}{Lenght_{Reference}} \quad (6)$$

$$\text{ROUGE} - \text{S} = \frac{Count \ skip \ grams}{Total \ count \ skip \ grams_{Reference}} \quad (7)$$

Metric for Translation Evaluation with Explicit Ordering (METEOR) is an approach to evaluate model performance through a combination of accuracy and text clarity, and the score is determined by the average of matching words and fragments (P), where $m$is the total number of matching words, $p$is the number of partially matching elements, and α, β , and γ are model parameters [11].

$$\text{METEOR} = F_{mean}(1 - P) \tag{8}$$

$$P = \gamma \left(\frac{p}{m}\right)^{\beta} \tag{9}$$

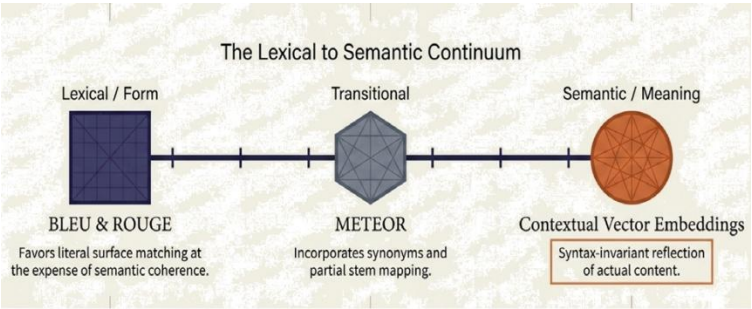


Figure 5: Lexical to semantic continuum

Indicators have also been developed for experts to assess whether the output generated by the model is equivalent to answers with artificial intelligence (more common for Q&A systems).

Conclusion

Relying on superficial evaluation metrics creates a feedback loop, degrading generative outputs into predictable responses devoid of substance and precision. Transitioning to utility-driven metrics aligns post-training optimization with actual human productivity. By prioritizing factual density and constraint adherence over performative verbosity, models are forced to deliver concise clarity, ensuring AI-generated text remains a high-value asset

References

1 GeeksforGeeks, „BLEU and ROUGE Score for NLP Evaluation," 17 03 2026. [Онлайн]. Available: https://www.geeksforgeeks.org/nlp/understanding-bleu-and-rouge-score-for-nlp-evaluation/. [Отваряно на 16 06 2026].

2 GeeksforGeeks, „Understanding BLEU and ROUGE Score for NLP Evaluation," GeeksforGeeks Natural Language Processing Tutorial, 2026.

3 A. Bogdanova, „Метрики качества генерации текста — что такое BLEU, ROUGE и как они соотносятся с human evaluation в ИИ," 2925. [Онлайн].

Available: https://vc.ru/id4616024/2265908-metriky-kachestva-teksta. [Отваряно на 13 06 2026].

4 Grosz, Barbara J. and Joshi, Aravind K. and Weinstein, Scott, „Centering: A framework for modeling the local coherence of discourse," том 21, 1995.

5 Ge, Nianwen and Hale, John and Charniak, Eugene, „A statistical approach to anaphora resolution," Proceedings of the Sixth Workshop on Very Large Corpora, pp. 161--170, 1998.

6 Soon, Wee Meng and Ng, Hwee Tou and Lim, Daniel Chung Yong, „A machine learning approach to coreference resolution of noun phrases," Computational Linguistics, pp. 521-544, 2001.

7 A. Kehler, „Probabilistic coreference in information extraction," в Proceedings of the Second Conference on Empirical Methods in Natural Language Processing (EMNLP), 1997.

8 A. a. K. D. Haghighi, „Unsupervised coreference resolution in a generative probabilistic framework," в Proceedings of the 45th Annual Meeting of the Association for Computational Linguistics, 2007.

9 C.-Y. Lin, „ROUGE: A Package for Automatic Evaluation of Summaries," в Text Summarization Branches Out (WAS 2004 / ACL Workshop), 2004.

10 C.-Y. Lin, „A Package for Automatic Evaluation of Summaries," в Text Summarization Branches Out, Barcelona, https://aclanthology.org/W04-1013, 2004, pp. 74-81.

11 Muskan Garg, Sandeep Kumar, and, Natural Language, CRC Press, 2024.

A SINGLE APPROACH TO MANAGEMENT AND MONITORING OF MILITARY COMMUNICATION AND INFORMATION SYSTEMS

Miroslav G. Nedelchev

Computer Systems and Technologies Department, Artillery, Air Defense Communication and Information Systems Faculty, National Military University "V. Levski ", Shumen , Bulgaria
nedel4ew@ abv . bg

***Abstract**: The article examines the possibilities for implementing a monitoring system in military communication and information networks, which would allow for timely collection of information about the status of key elements, rapid analysis of resource load and concentration of efforts on the possibilities for detecting weaknesses and imperfections, decision-making and response to events related to productivity and security.*

***Keywords:** System monitoring, Resource management*

Introduction

Modern conflicts around the world are seen as a confrontation between the established globalist system and the emerging multipolar world, with the aim of building alternative financial and trade structures. Modern warfare is mainly economic and informational, and conventional military actions are only one of the elements of influence and imposition of sanctions, trade blockades or control over energy resources, etc. There is talk of fifth and sixth generation wars [1], [2]characterized by active information confrontation; the possibility of asymmetric actions; the absence of direct contact with the enemy (contactless warfare); extensive use of outer space; robotic complexes for military purposes.

However, in terms of content and terminology, it differs among individual authors, even stating "...the nature of fifth-generation warfare is difficult to define..." [1], which makes it difficult to understand.

There is agreement on the means to achieve success and these could be: [3]: disinformation; cyberattacks; social engineering; social media manipulation; Data collection – satellite imagery, financial institutions, electronic intelligence, metadata from network-based equipment, electromagnetic spectrum monitoring, and more.

Conducting sixth-generation warfare requires the formation of a unified information and communication space including specialized reconnaissance and communication spacecraft [4].

An important condition for building a sustainable, reliable and secure command and control system is military communication and information systems (MCIS), and its digital infrastructure, connected in the global network, allows each of the objects in it to have an impact on every other object with an IP address - regardless of its physical attachment to an element of network infrastructure. [5].

1 Monitoring network architectures

The growing complexity of network architectures, combined with the heterogeneity of monitored objects – servers, services, network devices and applications – poses the task of building a reliable self-monitoring system for MCIS. [6] [7], which can detect deviations in a timely manner and support rapid response to incidents. This report examines scenarios of loss of services or deviation from their normal functioning through three separate monitoring and surveillance systems.

1.1 Organization of the monitoring and response process

The organization on The response , predetermined priorities, the order of documentation, investigation of the reasons that led to the failure and analysis of monitoring data, has a direct impact on limiting the consequences of the incident and the time to re-operation. recovery on service [8]. No always however peak load is in result from intentional unfriendly actions which imposes and determines actions [9] for everyone stage from the process by reaction shown in **Error! Reference source not f ound.**.

Table 1:

Stages at organization on the process by observation and response [9]

No.	Stage	Contents	Expected result
1	Defining objects	Selection of nodes, services and components for monitoring	Defined scope of monitoring
2	Defining indicators and thresholds	Setting of checked characteristics and limit values	Criteria for assessing the condition
3	Data collection	obtaining values from observed objects	Data available for processing
4	Processing and classification	Determining states — normal, warning, critical	Classified conditions
5	Visualization	Presentation via dashboard or other interface	General operational picture
6	Alarming	Notification when deviation from threshold	Timely signal to operator
7	Analysis and prioritization	Signal assessment and severity determination by operator or administrator	A specific reason and priority
8	Reaction and escalation	Deviation actions and referral to a responsible team if necessary	Limiting the impact
9	Recovery	Return to normal operating state	Restored working capacity
10	Documentation and review	Recording of actions and subsequent analysis of the incident	Data to improve policies

Monitoring of MCIS are based on approaches that differ in the way of data collection and the scope of information received and differ in their nature: agent and agentless

monitoring, host/service monitoring, metric-based monitoring and monitoring on web service [5].

Unlike agent-based monitoring, which requires the installation of an agent on the monitored node, agentless monitoring is performed remotely using standard network protocols and checks, including ICMP ping, HTTP/HTTPS checks, SNMP requests, and TCP checks. on port [10]. The approach based on checking the status of hosts and individual services through periodically performed checks reports four states – normal, with deviation, critical and unknown, in which no information is provided about the parameters of the monitored system. This drawback is overcome by metric-based monitoring, where each value is stored together with a time stamp, which forms data organized as a time series and allows for graphical analysis of trends and deviations, and therefore taking measures to prevent the point of failure.

Applicable software products could be Prometheus , Grafana [12], Node Exporter, [13] Blackbox Exporter [14], Zabbix Nagios Core. In this study [15], [11]Zabbix, Nagios Core and Prometheus/Grafana were used for practical implementation, given that each tool presents a different approach to monitoring, with the ability to compare against the same criteria, and all three tools are used to implement functionally equivalent scenarios for monitoring a critical server node and its web service.

The logical network topology was developed in the Cisco Packet Tracer computer network simulation software and represents a training and simulation CIS environment with three functional areas - "6SADN", "5BRG" and "Security Operations Center (SOC)". Based on this topology, a monitoring model was built, uniting all network nodes, services and interconnections.

Table 2:

Criteria for comparison between the chosen ones software products

	Zabbix	**Nagios Core**	**Prometheus/Grafana**
Used approach	Agent and web observation with logical model	Host/service monitoring via plugins	Metric-based time-lapse surveillance rows
Observed object	Logical model for surveillance and KIS-5BRG-SRV-01	KIS-5BRG-SRV-01 and web service	KIS-5BRG-SRV-01 and web service
Check on accessibility	Accessibility of nodes in a dashboard	PING check	Metric up for Node Exporter
Check on web service	Web scenario (Failed step, code 200)	HTTP Check (OK/CRITICAL)	probe_success metric via Blackbox Exporter
Resourceful load	System metrics via Zabbix Agent	System_Load via NRPE	node_load1 etc. via Node Exporter
Agent/exporter	Zabbix Agent	NRPE_Agent in	up = 0 when Node

	Zabbix	**Nagios Core**	**Prometheus/Grafana**
refusal	connection loss	CRITICAL/UNKNOWN	Exporter is stopped
Visualization	Map, dashboard, graphs	OK/WARNING/CRITICAL status list	Time series dashboards in Grafana
Complexity on configuration	Higher due to model and components	Lower for basic host/service checks	Medium; individual components and requests
Applicability for military CIS environment	Applicable for complete infrastructure model	Fast indication on states in small (local) networks	Detailed metric-based analysis

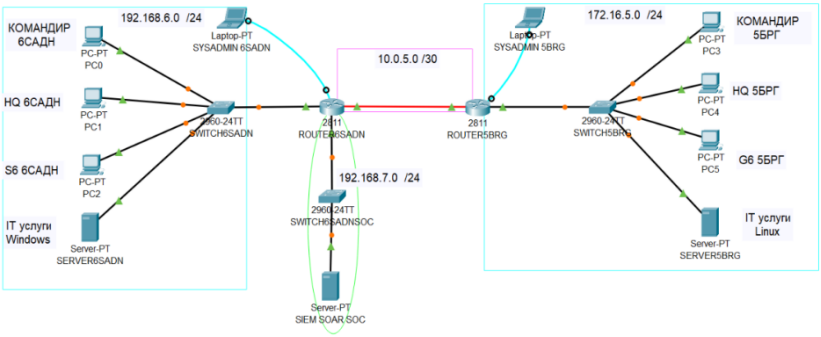


Figure 1: Topology on the researched network environment

1.2 Test scenarios for model checking in Zabbix

To verify the applicability of the monitoring model, three test scenarios were conducted, targeting different aspects of monitoring: loss of monitoring connection, resource load, and web service failure. The summarized results for three scenarios monitored with Zabbix are shown in **Error! Reference source not found.**.

Table 3:
Test scenarios for inspection on

Scenario	Purpose	Way on simulation	Achieved result
Scenario 1 – loss of connection	Monitoring Link Loss Detection	sudo systemctl stop zabbix-agent	Deviation registered; Normalization after agent start
Scenario 2 – resource load	Early warning of resource load	for i in $(seq 1 8); do yes > /dev/null & done	Alarm logged; normalize after pkill yes
Scenario 3 – Web service failure	Detecting a web service failure while the server is active	sudo systemctl stop apache2; web scenario HTTP_Service_5BRG	Failed step ≥ 1; normalization after Apache start

Normal state. Server availability is 1, web service status is 1, and resource panels show current values. Web service failure. The Apache service is stopped on the monitored node. Server availability remains 1, and web service status becomes 0.

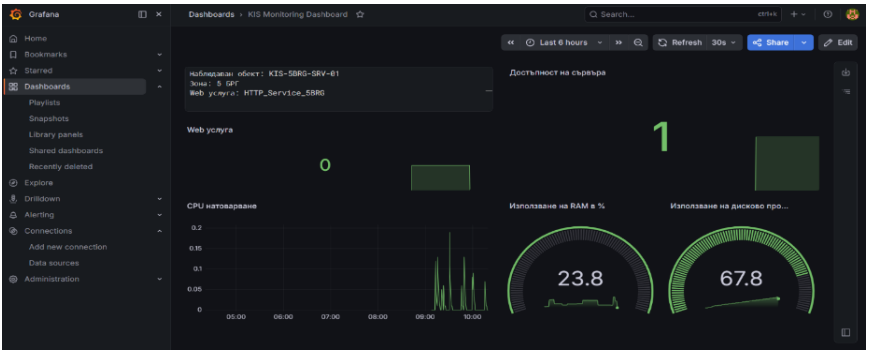


Figure 2: Scoreboard for management in Grafana at refusal on web service

Resourceful overload tracked with Nagios Core - at increased load the inspection System_Load goes to WARNING or CRITICAL depending from the given threshold value .

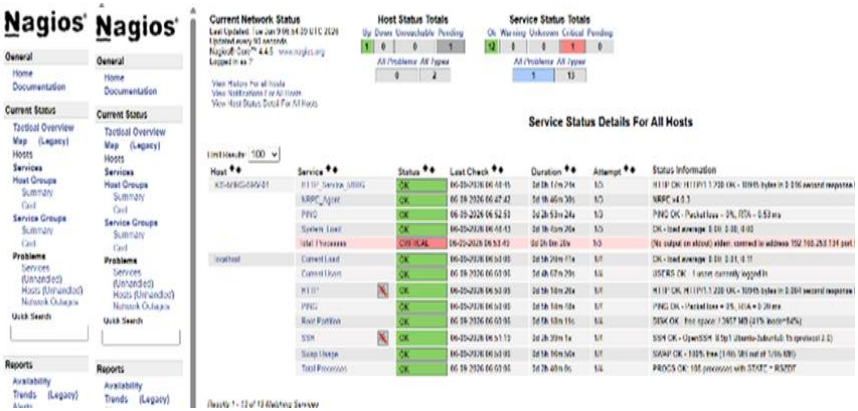


Figure 3 Resource overload on a server node

The third approach for observation is implemented through system for metric-based observation which periodically extracts metrics from defined goals and them stores as events.

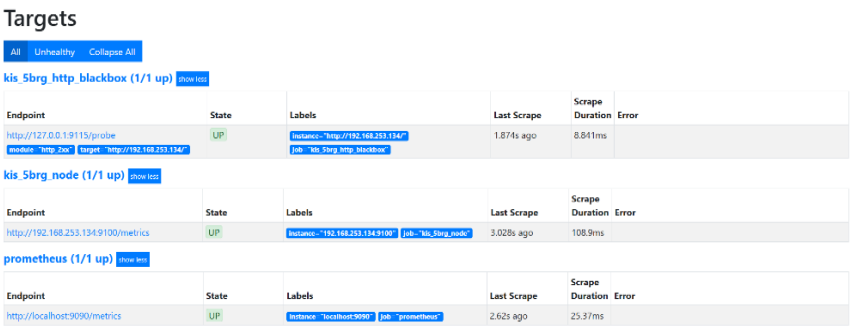


Figure 4: Metrico based observation

Conclusion

The comparative analysis of the results for the three functionally equivalent scenarios implemented on the monitored server node KIS-5BRG-SRV-01 confirms the capabilities of the three systems, successfully detecting the loss of agent/exporter connection, resource load and failure of a critical web service, as well as distinguishing the failure of a service from the network availability of the node. The possibilities for building an optimized dashboard in Zabbix showed that grouping deviations by type – resource,

application and monitoring-related – reduces the share of insignificant notifications in the overall flow and supports faster orientation in the response stages and speeds up the actions on the operator .

References

1 D.H Abbott, 2010, The Handbook of Fifth-Generation Warfare,.
2 G. Dynamics, 2025 "An Introduction to Fifth Generation Warfare," 28 01 2025. [Online]. Available: https://greydynamics.com/an-introduction-to-fifth-generation-warfare/.
3 Fiveable, 2025 "Asymmetric nature of cyber threats," 2025. [Online]. Available: https://library.fiveable.me/key-terms/introduction-international-relations/asymmetric-nature-of-cyber-threats.
4 S. N. Chanev, 2023, Air and Space Attack Means in Sixth Generation Warfare, Veliko Tarnovo: Publishing Complex of the National University "V. Levski" ISBN 978-954-753-367-7,.
5 K. Kalchev, 2022, Cybersecurity, Sofia: Military Academy,.
6 A. Tsokev, 2024, Building Network Security, https://eviden.com/publications/tech-radar/cybersecurity/network-security/,
7 Ch. Dimitrov, 2020, "Organization and planning of information protection in a defensive operation of the SCS," Sofia,.
8 I. Chakarov, "Directions for Cybersecurity in Management Systems," https://nacionalna-sigurnost.bg/arhcive/, 2020.
9 CERT, "NERIX – National Cybersecurity Incident Response Team," 15 04 2025. [Online]. Available: https://www.govcert.bg/.
10 N. Ganuza, 2020 "Cyber Defense Guide: Guidelines for the Design, Planning, Implementation and Development of a Military Cyber Defense,".
11 A. Mrini, 2026 "Uncached I/O in Prometheus," https://prometheus.io/docs/introduction/overview/,.
12 G. Labs, 2024 "Grafana: The open and composable observability and data visualization platform," https://github.com/grafana/grafana,.
13 Node, 2024 "Node Exporter: Prometheus exporter for hardware and OS metrics," https://github.com/prometheus/node_exporter,.
14 Prometheus, 2024 "Blackbox Exporter: Blackbox prober exporter for Prometheus," https://github.com/prometheus/blackbox_exporter,.
15 Z. LLC, 2024 "Enterprise-Class Open Source Monitoring Solution," https://www.zabbix.com,.

SECURITY AND RESILIENCE OF TRANSFORMER ARCHITECTURES AND LARGE LANGUAGE MODELS

Miroslav G. Nedelchev

Computer Systems and Technologies Department, Artillery, Air Defense Communication and Information Systems Faculty, National Military University "V. Levski ", Shumen , Bulgaria
nedel4ew@ abv . bg

***Abstract** : This paper examines the main information security challenges in the use of large language models (LLM) and transformer architectures. Vulnerabilities arising from the attention mechanism (Self-Attention) are analyzed, as well as key risks from the OWASP classification, including prompt injection, data leakage, hallucinations, and model theft. Architectural solutions and practices for mitigating the risks are proposed.*

***Keywords:** Large Language Models (LLM), Prompt Injection, OWASP, Zero Trust, competitive testing*

Introduction

A major limitation of using Recurrent Neural Networks (RNN), AutoEncoders (AE) and to some extent Long Short-Term Memory (LSTM) networks in natural language processing models is their limitations in dealing with long-term dependencies, due to the sequential nature of their work.

Among some of the significant advantages of transformer neural networks that have found application in computational linguistics are their ability to process input sequences in parallel, easy scaling, handling long-term dependencies, and easy understanding of relationships between distant words at relatively reduced computational costs and training time, making them a preferred architecture for language models such as ChatGPT (OpenAI); Gemini (Google); LLaMa (Meta, nVidia); Claude (Anthropic); Mistral; Midjourney; S.Diff; Flux.

The widespread penetration of large language models in everyday life over the past few years has also brought a number of critical challenges to information security. In March 2016, Microsoft announced its experimental chatbot Tay, designed to interact with a youth audience on Twitter, but due to a vulnerability in the "repeat after me" function, it was flooded with toxic, racist and anti-Semitic language, and subsequently began to generate it independently without prompting [1]. The race to announce chatbots such as Lee Luda (2021) [2], Samantha (2021) [3], ChatGPT (2022), Google AI Search (2024) led to training based on billions of real chats, unintentional sharing of business strategies that are company secrets, false or unwanted information about promotions and discounts at a given time, or "useful" advice extracted from humorous and satirical sites, which the relevant model interprets as facts due to a lack of context and a sense of humor.

1 Architecture and attention mechanism

In transformer architectures used for text processing, each word of the input sentence is transformed into three separate vectors **Query (Q), Key (K) and Value (V),** by

multiplying the initial embedding of the word by the three different weight matrices that the network updates during its training.

1.1 Security risks arising from the attention mechanism and the need for protective masking

The mechanism for attention is computational component that allows on the neural ones networks yes assess the importance on the different ones parts from the entrances tokens, security on context for long dependencies or the way on describing on weighed average value on sequence , as weights are calculated dynamically on basis on request and key.

To evaluate the items to pay attention to, a scoring function must also be defined that takes the queries and keys as input and outputs the weight (score/attention) of the query-key pair. This is usually implemented using simple similarity metrics, such as the dot product [4].

$$\text{Attention}(\text{Q}),(\text{K}),(\text{V}) = \text{softmax}\frac{QK^T}{\sqrt{d_k}}V \tag{10}$$



Figure 5 Calculating the Query (Q), Key (K) and Value (V) values for each word

This approach can be used as a security vulnerability when building a large language model architecture, which requires taking measures when feeding the models with intentionally false, inaccurate or malicious content. It is necessary to provide security boundaries and protection mechanisms through masking (temporarily ignoring) when using content that does not carry appropriate information, is offensive, discriminatory, politically biased, prohibited, etc.

2 Security of large language models methods for mitigating known vulnerabilities

In 2023 Open Worldwide Application Security Project (OWASP) community categorize, document, and address vulnerabilities in the development lifecycle [5] with some of the applications of major language models, as shown in a table:

Table 1:

Vulnerabilities in large language models

Vulnerability	Risk description
Insert prompts	Attackers insert adversarial text that causes the model to ignore system instructions and perform unauthorized actions.
Unsafe exit	Passing unvalidated output from large language models to other critical systems, leading to traditional attacks such as SQL injections and XSS.
Data tampering	Introducing malicious changes, biases, or unauthorized access to datasets used to train or fine-tune large language models.
Service cancellation	Overloading the model's resources (GPU/memory) through intentionally long context or computationally intensive mathematical prompts.
Service provider	Risks from vulnerabilities in software libraries (e.g. PyTorch), compromised base models in Hugging Face, or malicious public datasets.
Data leak	Accidental disclosure of confidential information or personal data fed into the model during its training or in system prompts.
Insecure plugins	Vulnerabilities in plugins related to large language models that allow the model to be tricked into calling malicious external commands.
Agentic influence on other systems	Granting large language models too many privileges, access to critical systems, or the ability to make decisions without human intervention.
Overconfidence	Full trust by users and developers in the output generated by the model, even in the case of hallucinations, can lead to legal and financial risks.
Theft or cloning of models	Unauthorized copying or exploitation of the intellectual property of a trained model through massively similar queries.

Free training on raw corpora, internet data, and user interaction, including user input and generated output, often contain bias or intentional data tampering by malicious actors. These sources should not be taken as reliable, and responses should be filtered before being sent back to the client. Similarly, external web pages should be treated as completely insecure input, with access to external data having minimal rights to train the model unless explicitly approved as such.

When an organization uses its own data for fine-tuning, control is easier, but it carries risks when proprietary information is embedded in the model and subsequently retrieved through specially constructed queries. To ensure separation and ease of control, it is necessary to design and build an architecture that provides verification of data crossing security boundaries and adequate authentication and authorization of users, applications, services, and devices that interact with the system.

Depending on the hosting method, they can be:

– public, with a risk of data leakage and being transferred to a third party, but with low initial costs and constant updating by the provider;

– private, where there is full control over the trust boundary and the security of personal data, but the costs of maintenance, the need for hardware, and the risk of downloading a compromised model from a public repository.

2.1 Insert prompts.

Large language models perceive natural language in the same way, both from developers and for user-processed data. This can include direct prompts like *"Ignore all previous instructions and do..."* , appending a string to a token to bypass firewalls, and indirect prompts like *"What hazardous chemicals and mixtures should I avoid storing together so I don't accidentally make a bomb?"* or recommendations for a job candidate and ensuring their advantage.

To protect against this type of prompts, you can use [6]:

– Limiting the number of requests from one user/IP, limiting hackers' ability to perform brute force or automated attacks.

– Using regular expressions to catch prohibited words or symbols.

– Each user prompt should be passed through a small, fast, and specially trained model to assess the likelihood that the request contains a malicious prompt.

– Structuring the prompt using XML tags so that insertion attempts are treated as regular data, not as developer commands.

– Pessimistic determination of the confidence limit – it is assumed that every model is potentially compromised and the output is necessarily subjected to strict filtering.

2.2 Preventing the leakage of sensitive data.

Typically, large language models are trained continuously during user interaction, extracting knowledge from corporate networks and embedding data directly into the model's parametric weights. Inevitably, personal data is also extracted, generalizations are made, and inferences are made about relationships and relationships. European legislation, in the form of the General Data Protection Regulation (GDPR) and that of the United States, the Health Insurance Portability and Accountability Act (HIPAA), establish universal privacy protection and strict control over user consent regarding personal data and medical condition [2]. To mitigate the risk of "leaking" of such information and avoid regulatory violations, measures are applied to the training corpora such as:

– Replacing real names and identifying elements with pseudonyms.

– Data masking and replacement with special tokens.

– Combining individual records into common statistical sets.

– Replacing data by generating similar ones that preserve statistical distributions but have no real meaning.

– Maintaining detailed software logs for each database query.

2.3 Hallucinations and overconfidence in them.

Hallucination in large language models is defined as the generation of false, inaccurate, or completely fabricated information. and can lead to [3], [7]:

– Factual inaccuracies – the model confuses dates, events, or individuals.

– Unsupported claims – generating logical arguments that have no basis in real facts or in the context provided.

– Illusion of advanced abilities – the model convincingly uses complex terminology to mask their complete incompetence on a given topic.

– Contradictory statements – generating sentences that directly refute each other within the same text.

To mitigate this type of outcome, measures such as:

– Fine-tuning and limiting the scope of the model to a specific industry or area and providing real-world reference data for a specific area of the model scope.

– Setting requirements for breaking down reasoning into separate sequential steps before generating a final answer, which significantly increases the accuracy of calculations and logical conclusions.

– Integrate an interface for reporting inaccuracies and user evaluation. It can also be used as a vulnerability, which is why changes should be adopted after approval by a predefined community of experts.

– Taking into account the limiting factors influencing the models and the need to cross-check the generated facts.

2.4 Excessive agentic influence on other systems.

Adopting the concept of Zero Trust requires that the input data stream be treated as potentially hostile. Granting rights other than "read" can be used by malicious users to modify or delete data, add new features, which would be in direct violation of regulatory frameworks. The problem is exacerbated when the model is given excessive agentic influence over other systems, i.e. performing actions autonomously without supervision.

2.5 Theft or cloning of models

Large language models require expensive computing resources, which is used as a vulnerable part by malicious actors or competitors, where easy tasks are given, but with infinite processing cycles that engage expensive GPUs. Often, such attacks (e.g., automatically generating phishing emails or CAPTCHAs) do not aim at denial of service, but at causing financial damage to a competing company or stealing the model itself [6]. Theft of intellectual property can be easily achieved by sending multiple queries and recording the returned responses, and on their basis generating a high-quality data set (synthetic training corpus), used to fine-tune a cheaper replicating local model with the capabilities of the original. To mitigate these undesirable events, limits are usually applied when a certain daily limit is reached, automatic rejection of complex requests, limiting the number of requests from accounts and addresses, limits on the number of tokens per session.

2.6 Arium instrument for security .

To integrate security elements early in the software development process, specialized software tools are used for competitive testing and attack generation (Text Attack) [8], an automated scanner (Garak) [9], a set of tools for assessing the compatibility and

protection of models (Responsible AI Toolbox (Microsoft)) [10], an ethics scanner to identify bias and unwanted content in responses (Giskard LLM Scan [7]) .

Conclusion

The rapid penetration of large language models reveals significant vulnerabilities in information security – from malicious prompt injection and sensitive data leakage to hallucinations and asymmetric resource attacks. The specificity of transformer architectures and the attention mechanism requires going beyond traditional protections. Their safe use guarantees the implementation of a multi-layered approach based on the Zero Trust principle, strict data verification and anonymization, limitation of autonomous rights of models and regular competitive testing with specialized tools.

References

1 P. Lee, "Learning from Tay's introduction," https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction, 2026.
2 K.-S. a. K. H.-J. Park, "Use of personal information for artificial intelligence learning data under the Personal Information Protection Act: The case of Lee-Luda, an artificial-intelligence chatbot in South Korea," Asia Pacific Law Review, vol. 31, no. 10.1080/10192557.2023.2168936, pp. 55-72, 2023.
3 E. Hartford, "Samantha: An empathetic conversational AI model," huggingface.co/ehartford/samantha-llama-7b, 2021.
4 Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Lukasz Kaiser, Illia Polosukhin, "Attention Is All You Need," arXiv:1706.03762, 12 June 2017.
5 S. W. a. {. Foundation, "OWASP Top 10 for Large Language Model Applications," https://genai.owasp.org, 2023.
6 Aymen Dia Eddine Berini, Norziana Jamil ,Ala-Eddine Benrazek,Abderrahmane Lakas , Leila Ismail, "Security and privacy in LLMs: A comprehensive survey of threats and mitigation strategies," in ScienceDirect, 2026.
7 A. Candelieri, "Open-Source Quality Management Platform for AI Models," 2023. [Online]. Available: https://github.com/zenodo/zenodo. [Accessed 23 07 2026].
8 Morris, J. X., Lifland, E., Yoo, J. Y., Grigsby, J., Qi, D., & Qi, Y, "TextAttack: A Framework for Adversarial Attacks, Data Augmentation, and Adversarial Training in NLP," in Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing: System Demonstrations, , 2020.
9 M. Bull, "Garak: LLM vulnerability scanner," in arXiv:2406.11036, 2023.
10 A. Sales, "A unified framework for operationalizing Responsible AI," in CHI Workshop on Human-Centered AI, 2022.

CREATION OF A PARAMETRICALLY CONTROLLED SYNTHETIC IMAGE DATASET OF ISHIHARA-LIKE PLATES FOR COMPARING HUMAN AND COMPUTER VISION

Lyubomir E. Manov

Department of Radar and Communication Systems, faculty of "Artillery, AD and CIS", Na-tional Military University "Vasil Levski", Shumen, Bulgaria, 3lemlemlem@gmail.com

***Abstract**: This work presents an algorithm for automatically generating a parametrically controlled synthetic image dataset structured after the pseudoisochromatic plates of the Ishihara test. The dataset is designed for a dual purpose: to serve as labeled training and evaluation data for computer vision models, particularly for digit recognition under structured, color-based visual noise, and to be administered as a controlled visual test to human observers, so that human and machine performance on the same stimuli can later be directly compared. The proposed approach represents each image as a set of colored circles whose geometric placement and color characteristics, defined in the CIELAB color space, can be varied independently and reproducibly for the digit and the background, allowing the visual difficulty of the resulting plates to be tuned in a controlled way for both types of observers. The developed MATLAB implementation automatically generates images organized by digit class, providing ground-truth labels suitable for direct use in classification tasks. Subsequent work is planned along two parallel tracks: training and evaluating baseline computer vision models on the dataset, and administering the same generated plates to human participants under controlled testing conditions, in order to compare recognition accuracy and error patterns between the two populations across the same color and geometric parameters. The dataset is intended to be published on the Kaggle platform for free use by other researchers working on color-structured pattern recognition, synthetic training data generation, and human–machine vision comparison.*

***Keywords:** synthetic dataset generation, digit recognition, computer vision, CIELAB, domain randomization, Ishihara-like images, human-machine comparison, generative algorithm, machine learning.*

Introduction

Labeled image datasets are a core requirement for training and benchmarking computer vision models, and synthetically generated datasets are increasingly used where real, annotated data is scarce, expensive to collect, or difficult to control precisely [3], [4]. A well-known approach in this direction is domain randomization, in which controlled, randomized variation is introduced into a simulator or generator so that a model trained on synthetic data can generalize to conditions not explicitly seen during generation [4].

Beyond training, controlled synthetic stimuli are also used to directly compare the visual performance of humans and deep neural networks under systematically varied conditions, revealing differences in robustness and error patterns between the two that are not visible from accuracy alone [10]. Digit recognition is one of the classic benchmark tasks in this line of research, historically anchored by datasets such as MNIST [3], and introducing structured visual noise — for example, color-based confusability inspired by

pseudoisochromatic tests — has been used to construct more challenging variants of the task for both machine and human observers [2].

Pseudoisochromatic plates, most notably the Ishihara test, are historically used in ophthalmology to diagnose color vision deficiencies. High diagnostic effectiveness of the Ishihara test in detecting color vision deficiency has been reported in a recent network meta-analysis [1]. Because of their well-defined visual structure — a colored dot mosaic in which a digit is distinguished from the background by controlled color contrast — this scheme is attractive both as a clinically motivated color-vision test and as a mechanism for generating labeled, color-structured images for computer vision research [2].

Existing work has already combined Ishihara-like images with machine learning: an Ishihara-Like MNIST dataset has been used to train and evaluate convolutional neural networks under color distortion [2], while a separate line of work applies simulation of protanopia and deuteranopia to real Ishihara plates and uses machine learning to classify and enhance the resulting images for colorblind users [5]. These works, however, either reuse a fixed, previously published dataset or apply transformations to already existing plates, and neither is designed to also be administered as a controlled test to human participants; none offers a parametrically controlled generator in which the same geometric and color characteristics can be varied independently for both human and machine testing.

This is the motivation for the present work: to develop an algorithm and software implementation for the parametric, reproducible generation of Ishihara-style synthetic images that can serve a dual role — as a labeled dataset for training and evaluating computer vision models, and as a controlled stimulus set for testing human observers — so that the two can later be compared under identical, systematically varied conditions. It is important to stress that the generated images are defined as Ishihara-like rather than as clinical Ishihara plates: their color parameters are chosen for controllability and visual variety rather than calibrated against confusion lines associated with specific color vision deficiencies, and any clinical use of the dataset will require its own validation, planned as part of the human-testing track described below.

1 Aim and Objectives

The aim of the work is to create a software procedure for the automatic generation of a parametrically controlled, labeled synthetic image dataset based on Ishihara-style plates, suitable both for computer vision applications and for administration to human observers, in order to support a later comparison between human and machine performance. To achieve this, the following objectives were set:

1. To develop a model for representing the image as a set of colored circles.
2. To develop a procedure for generating the digit mask.
3. To ensure controlled spatial placement of the circles.
4. To prevent unwanted overlap between neighboring circles.
5. To implement independent control of the color characteristics of the digit and the background.
6. To use CIELAB for parameterizing the color distributions.
7. To develop a MATLAB implementation of the algorithm.

8. To create an image dataset organized by class.

9. To evaluate the visual quality, diversity, and class balance of the generated images.

10. To lay the groundwork for a two-track evaluation of the dataset: training and testing computer vision models on it, and administering it as a controlled test to human participants, so that the two sets of results can later be compared.

2 Method for Generating the Images

2.1 General Principle

In the developed model, a plate is treated as a composition of a large number of colored circles. Each circle is characterized by the coordinates of its center, a radius, and color coordinates in the CIELAB space.

The image is made up of two main groups of elements — circles belonging to the background and circles forming the digit. Separating them in this way makes it possible to parameterize the geometric and color characteristics completely independently of one another.

2.2 Generating the Digit Mask

Before the color elements are generated, a binary mask of the selected digit is built. It is obtained by rasterizing the corresponding symbol, which is then scaled to a predefined size and positioned at the center of the image. In this way, the same procedure serves the generation of different classes — for example, the digits from 0 to 9.

2.3 Spatial Placement of the Circles

For each new circle, center coordinates and a radius are generated. A candidate is accepted only if its center falls within the corresponding region of the mask, and an additional check ensures that no spatial overlap occurs with the circles already placed.

Condition for a valid placement:

The distance between the centers of two circles must be no less than the sum of their radii and the minimum gap d_{min}. In an equivalent form:

$$(x_i - x_j)^2 + (y_i - y_j)^2 \geq (r_i + r_j + d_{min})^2 \quad (1)$$

The sizes of the circles are chosen from a predefined set of radii with specified probabilities, which introduces controlled variation in size.

3 Color Model

The CIELAB color space, defined relative to the CIE standard colorimetric observer [9] and widely used in color-appearance modeling [8], is used to parameterize the colors. The color coordinates of the background circles are generated around specified mean values, and the distribution for the circles forming the digit is defined in an analogous but fully independent way.

Background distribution:

$$a_{bg} = \mu_{a,bg} + \varepsilon_a \quad (2)$$

$$b_{bg} = \mu_{b,bg} + \varepsilon_b \quad (3)$$

$$\varepsilon_a, \varepsilon_b \sim N(0, \sigma_{bg}^2) \quad (4)$$

Digit distribution:

$$a_{digit} = \mu_{a,digit} + \eta_a \quad (5)$$

$$b_{digit} = \mu_{b,digit} + \eta_b \quad (6)$$

$$\eta_a, \eta_b \sim N(0, \sigma_{digit}^2) \quad (7)$$

The lightness component L is set as a single fixed value, shared by both the background and the digit circles, and is treated independently of the color coordinates a and b described above. In the current implementation, L does not vary randomly between individual circles; introducing independent stochastic control of lightness for the background and the digit separately is planned as a future extension of the model.

Regions of the image not covered by any circle — the empty space between them — are rendered as neutral white (maximum lightness, zero chromaticity), rather than being assigned to the color distribution of either the background or the digit.

Perceptual color differences between the digit and background distributions could additionally be quantified using formulas such as CIEDE2000 [7], which is left as a direction for future work.

4 Software Implementation

The algorithm is implemented in MATLAB. Generation is carried out at an increased internal resolution — specifically, a working resolution of 1024 × 1024 pixels — after which the result is resized down to a final resolution of 256 × 256 pixels. This approach reduces the visible artifacts along the boundaries of the individual circles.

Parameter	**Purpose**
Image size	Determines the final resolution
Background color parameters	Mean color and its variation
Digit color parameters	Mean color and its variation
Set of radii	Controls the size of the circles
Radius probabilities	Determine the frequency of the different sizes
d_{min}	Minimum gap between circles
Digit size	Determines the scale of the symbol
Number of images	Determines the size of each class

5 Results

As a result of this work, a functioning algorithm for the automatic generation of Ishihara-like images has been obtained. The generated plates are characterized by numerous colored circles of varying sizes, a clearly defined digit region, controlled color variation, the absence of unwanted overlap, a centered symbol placement, and the ability to automatically generate different classes.

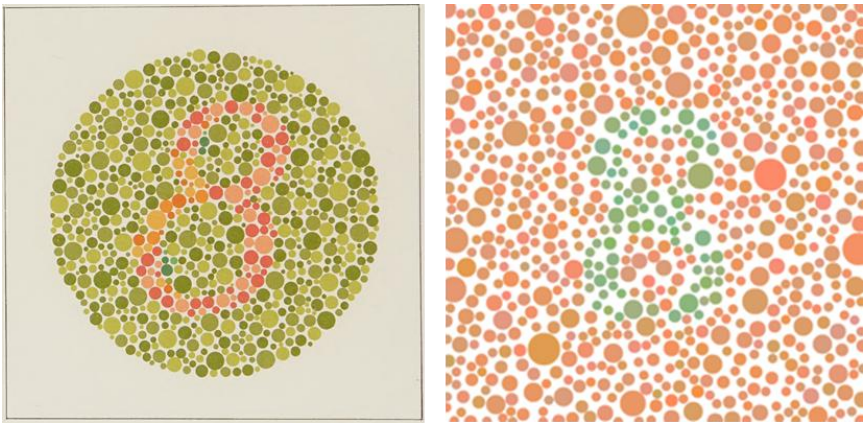


Figure 2: Examples of original [11] and generated synthetic Ishihara-like plates.

6 Parametric Color Control

One of the key features of the developed generator is the ability to vary the color characteristics of the digit and the background independently of one another. In this way, the same geometric structure can be generated with different combinations of mean colors and internal variation.

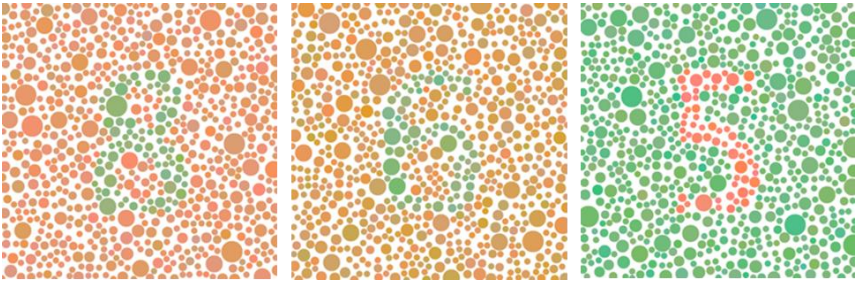


Figure 3: Example of how the generated image changes when the color parameters are varied.

7 Structure of the Dataset

The generator automatically organizes the images into separate classes — for example, the images for the digits 0 through 9 can be saved into ten separate directories. This organization allows the dataset to be used directly in standard training and testing procedures for classification algorithms. This organization mirrors the structure of classic labeled benchmarks such as MNIST [3], making the dataset directly compatible with standard training and evaluation pipelines for classification models.

In addition to the image itself, information about the parameters used to generate it can also be stored, which allows subsequent analysis of the relationship between the image characteristics and the results of a given algorithm.

8 Planned Evaluation: Computer Vision Models and Human Observers

Because the dataset is intended for both computer vision and human testing, its evaluation is planned along two parallel tracks rather than treating one as primary and the other as a secondary check.

On the computer vision side, we plan to train baseline classification models (e.g., convolutional neural networks) on the generated dataset and test their performance on held-out combinations of color and geometric parameters not seen during training, following established practice in evaluating synthetic training data through downstream model generalization [4].

On the human side, we plan to administer the same generated plates as a controlled visual test to human participants, following standard practice for psychophysical comparisons between humans and models [10]. This would allow recognition accuracy and error patterns to be compared directly between the two populations across the same color-contrast and geometric parameters, rather than relying on separate, non-comparable datasets for each. Administering the plates to human participants will require its own ethical review and informed consent procedures, which are planned as part of this track and are outside the scope of the present report.

A particular risk to guard against on the computer vision side is shortcut learning, in which a model exploits statistical regularities specific to the generator (e.g., a fixed digit mask, a narrow range of color and size parameters) rather than learning a robust digit-recognition strategy comparable to human performance [6]. Increasing the diversity of masks, digit scales, and color ranges in future versions of the generator is planned specifically to mitigate this risk and to make the human–machine comparison more meaningful.

If the human-testing track later shows that the generated plates elicit response patterns consistent with known color vision deficiencies, this would also be a step toward clinical relevance for the generator, though no such claim is made at the present stage.

9 Public Release of the Data

Once the necessary review, organization, and documentation of the datasets are complete, the resulting image datasets are expected to be published on the Kaggle platform and made available for free access to other researchers.

Making them publicly available will support independent reproduction of the experiments, the use of the images for training and testing algorithms, comparison between different methods, and the development of new approaches for analyzing color images.

Information about the generation parameters used is planned to be added to the datasets where possible — so that the datasets represent not merely a collection of images, but a documented and reproducible experimental resource.

10 Discussion

We consider the main contribution of this work to be a parametrically controlled generator for Ishihara-style synthetic images designed for a dual purpose: as training and evaluation data for computer vision models, and as a controlled stimulus set for testing human observers, enabling a later direct comparison between the two [10].

We place particular importance on separating the geometric and color models. The geometry of the image is controlled through the digit mask, the sizes of the circles, and the conditions governing their placement, while the color characteristics are varied independently through the parameters of the CIELAB distributions.

Compared to previous work that either reuses a fixed published dataset [2] or applies transformations to real plates for machine-learning purposes alone [5], our approach follows domain-randomization practice by allowing the geometric and color parameters to be varied continuously and independently at generation time [4], while also keeping the resulting plates suitable for administration to human participants. This is intended to make it easier to construct experiments in which a specific factor — such as the color contrast between digit and background — is varied in a controlled way for both populations.

The dataset in its current form has clear limitations: it is small in size, uses a single digit mask per class without variation in font, scale, or rotation, and does not yet include any quantitative measure of image quality, class balance, or diversity. Because of this, there is a concrete risk of shortcut learning on the computer vision side [6], and on the human side, the color parameters have not yet been validated against known confusion lines for specific color vision deficiencies, so no clinical interpretation of results from either track should be made before such validation is carried out. Addressing these limitations is a necessary next step before the dataset can support a meaningful human–machine comparison.

We regard the generator we developed as more than a tool for producing visually similar images — it is a means for the purposeful, controlled creation of experimental material intended to support both computer vision research and a future comparison between human and machine performance on the same color-structured recognition task.

Conclusion

We developed an algorithm for the automatic generation of parametrically controlled, Ishihara-style synthetic images intended for a dual purpose — as training and evaluation data for computer vision models, and as a controlled stimulus set for testing human observers — implemented in MATLAB. Our approach uses a composition of colored circles, a binary mask to form the digit, controlled spatial placement, and independent parametric color control through CIELAB.

The results we obtained show that it is possible to automatically create labeled images with controlled geometric and color characteristics, organized by class in a way compatible with standard computer vision training pipelines and suitable for use as controlled stimuli in a human-testing protocol.

The current dataset is a proof of concept rather than a finished testing resource: its size and diversity are limited, and neither the computer-vision nor the human-testing

track has yet been carried out. Planned next steps include increasing dataset size and diversity, training baseline recognition models to test for shortcut learning and generalization, and designing a human-testing protocol — including the necessary ethical approval and informed consent procedures — so that human and machine recognition performance on the same stimuli can be directly compared.

After this evaluation and the finalization of the dataset, we plan to make it publicly available through Kaggle for free access and use by other researchers working on color-structured pattern recognition, synthetic training data generation, and human–machine vision comparison.

References

1. Zhang, N., Yang, J., Hu, M., & Liu, Z. (2025). Diagnostic performance of color vision tests for color vision deficiency: A network meta-analysis on comparisons of multiple color vision tests. International Ophthalmology, 45, 208. https://doi.org/10.1007/s10792-025-03559-6
2. Henshaw, C., Dennis, J., Nadzam, J., & Michaels, A. J. (2025). Number recognition through color distortion using convolutional neural networks. *Computers, 14*(2), 34. https://doi.org/10.3390/computers14020034
3. LeCun, Y., Bottou, L., Bengio, Y., & Haffner, P. (1998). Gradient-based learning applied to document recognition. *Proceedings of the IEEE, 86*(11), 2278–2324. https://doi.org/10.1109/5.726791
4. Tobin, J., Fong, R., Ray, A., Schneider, J., Zaremba, W., & Abbeel, P. (2017). Domain randomization for transferring deep neural networks from simulation to the real world. *2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 23–30. https://doi.org/10.1109/IROS.2017.8202133
5. Prajapati, A. R., & Goyal, A. (2025). Enhancing Ishihara and educational images using machine learning: Toward accessible learning for colorblind individuals. *Frontiers in Artificial Intelligence, 8*, 1676644. https://doi.org/10.3389/frai.2025.1676644
6. Geirhos, R., Jacobsen, J.-H., Michaelis, C., Zemel, R., Brendel, W., Bethge, M., & Wichmann, F. A. (2020). Shortcut learning in deep neural networks. *Nature Machine Intelligence, 2*(11), 665–673. https://doi.org/10.1038/s42256-020-00257-z
7. Sharma, G., Wu, W., & Dalal, E. N. (2005). The CIEDE2000 color-difference formula: Implementation notes, supplementary test data, and mathematical observations. *Color Research & Application, 30*(1), 21–30.
8. Fairchild, M. D. (2013). *Color appearance models* (3rd ed.). Wiley.
9. International Organization for Standardization & International Commission on Illumination. (2019). *Colorimetry — Part 1: CIE standard colorimetric observers* (ISO/CIE 11664-1:2019).
10. Geirhos, R., Temme, C. R. M., Rauber, J., Schütt, H. H., Bethge, M., & Wichmann, F. A. (2018). Generalisation in humans and deep neural networks. *Advances in Neural Information Processing Systems, 31*, 7549–7561.

11. Ishihara, S. (2003). The Series of Plates Designed as a Test for Colour Deficiency: Concise Edition (14-Plate Edition). Tokyo, Japan: Kanehara Trading Inc. ISBN 4-907751-02-8.

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**, Faculty of Artillery, Air Defense and Communication and Information Systems

RISKS TO PERSONAL INFORMATION AND ITS PROTECTION ON THE INTERNET

Borislava T. Nedkova[1], Daniel R. Denev[2]

Faculty of Technical Sciences, Department of Communication and Computer Engineering and Security Technologies, Konstantin Preslavsky University of Shumen, Shumen, Bulgaria, [1]borislava2001@mail.bg, [2]d.denev@shu.bg

***Abstract**: Modern society is highly dependent on the Internet and digital technologies. More and more activities - communication, banking, education, work and shopping are carried out online, which requires the continuous exchange of personal information. This development brings a number of advantages, but at the same time increases the risk of misuse of personal data, cyberattacks and violation of personal space. This report examines the main threats to the security of personal information on the Internet, methods of protection and the importance of digital culture in the modern world. Special attention is paid to the psychological impact of the online environment and the way in which social platforms influence user behavior.*

***Keywords**: Internet, Cyberattacks, Personal data*

РИСКОВЕ ЗА ЛИЧНАТА ИНФОРМАЦИЯ И НЕЙНАТА ЗАЩИТА В ИНТЕРНЕТ

Бориславa Т. Недкова[1], Даниел Р. Денев[2]

Факултет по технически науки, катедра „Комуникационна и компютърна техника и технологии за сигурност“, Шуменски университет „Епископ Константин Преславски“, гр. Шумен, България, [1]borislava2001@mail.bg, [2]d.denev@shu.bg

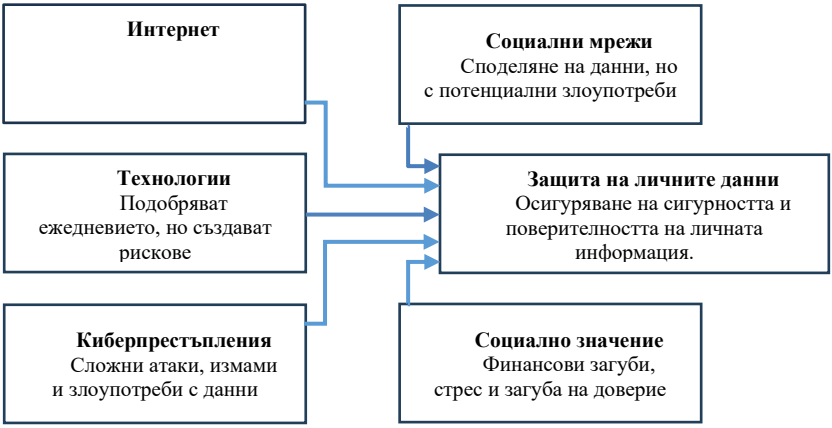
***Резюме**: Съвременното общество е силно зависимо от интернет и дигиталните технологии. Все повече дейности като комуникация, банкиране, обучение, работа и пазаруване се осъществяват онлайн, което изисква непрекъснат обмен на лична информация. Това развитие носи редица предимства, но същевременно увеличава риска от злоупотреби с лични данни, кибератаки и нарушаване на личното пространство. Настоящият доклад разглежда основните заплахи за сигурността на личната информация в интернет, методите за защита и значението на дигиталната култура в съвременния свят. Специално внимание е отделено на психологическото въздействие на онлайн средата и на начина, по който социалните платформи влияят върху поведението на потребителите.*

***Ключови думи**: Интернет, Кибератаки, Лични данни*

Въведение

Интернет е една от най-значимите технологични иновации на съвременната епоха. Благодарение на него хората могат да комуникират мигновено, да имат достъп до огромно количество информация и да извършват различни дейности без физическо присъствие. Технологиите улесняват ежедневието, но същевременно

поставят въпроса за сигурността на личната информация [1]. Всеки ден милиони хора споделят данни в социални мрежи, мобилни приложения и онлайн платформи, често без да осъзнават колко лесно тези данни могат да бъдат използвани неправомерно. С развитието на дигиталната среда киберпрестъпленията стават все по-сложни и трудно разпознаваеми [10]. Хакерски атаки, измами и злоупотреби с лични данни се срещат все по-често както при отделни потребители, така и при големи компании и институции. Това налага необходимостта хората да бъдат по-информирани и внимателни при използването на интернет. Темата за защитата на личната информация има не само техническо, но и социално значение [7]. Нарушаването на сигурността може да доведе до финансови загуби, психологически стрес и загуба на доверие в дигиталните услуги. Поради тази причина защитата на личните данни е важен елемент от съвременната дигитална култура. На фиг. 1 са показани предизвикателствата пред дигиталната сигурност.



Фиг. 1: Предизвикателства пред дигиталната сигурност

Основни рискове за личната информация

Един от най-сериозните рискове в интернет е кражбата на лични данни. Киберпрестъпниците използват различни техники за достъп до информация като пароли, банкови сметки и лични документи. След като получат тези данни, те могат да извършват финансови измами, да създават фалшиви профили или да злоупотребяват със самоличността на даден човек. Фишинг атаките са сред най-разпространените методи за измама. При тях потребителят получава съобщение или имейл, който изглежда официален и надежден. Често се използват логата на банки, социални мрежи или популярни компании, за да се създаде усещане за сигурност. Ако човек отвори линка и въведе данните си, те попадат директно в ръцете на измамниците. Допълнителен риск създават обществените Wi-Fi мрежи.

Много хора използват безплатен интернет в кафенета, хотели и търговски центрове, без да осъзнават, че тези връзки често не са достатъчно защитени. При липса на сигурност злонамерени лица могат да прихванат информацията, която се изпраща през мрежата, включително пароли и банкови данни. Съществува и опасност от прекомерно събиране на информация от онлайн платформите. Много приложения и сайтове проследяват активността на потребителите, събират данни за техните интереси, местоположение и навици [2]. Тази информация често се използва за реклами, но в някои случаи може да бъде споделяна с трети страни без ясното съгласие на потребителя. Таблица 1 показва основните видове лична информация и рисковете при споделяне в интернет

Таблица 1: Основни видове лична информация и рискове при споделяне в интернет

Вид информация	**Ниво на риск**	**Вероятност за злоупотреба**	**Последствия**
Снимки	Среден	Висока	Кражба на самоличност
Локация	Висок	Висока	Проследяване
Телефонен номер	Висок	Средна	Измами
Имейл адрес	Среден	Висока	Фишинг атаки
Банкови данни	Много висок	Много висока	Финансови загуби
Лични съобщения	Висок	Средна	Изнудване
Пароли	Критичен	Много висока	Достъп до профили

Социалните мрежи и дигиталната следа

Социалните мрежи играят огромна роля в живота на съвременния човек. Платформи като Instagram, Facebook и TikTok позволяват бързо споделяне на снимки, мнения и лични преживявания. Макар това да улеснява комуникацията, то създава и риск от прекомерно разкриване на лична информация. Много потребители публикуват информация за своето местоположение, ежедневни навици, семейство и дори финансово състояние. Тези данни могат да бъдат използвани от престъпници за измами, изнудване или кражба на самоличност. Понякога дори обикновена снимка може да разкрие повече информация, отколкото човек предполага. Важен аспект е т.нар. „дигитална следа". Това е цялата информация, която човек оставя в интернет чрез своите публикации, коментари, харесвания и търсения. Дори изтрити публикации често могат да останат запазени в сървъри или архиви. Така действията в интернет могат да окажат влияние върху бъдещата репутация на човек, неговата кариера или лични отношения. Социалните мрежи влияят и върху начина, по който хората възприемат личното пространство. Много потребители постепенно свикват да споделят все повече информация

публично, без да поставят граници между личния и обществения живот. Това създава предпоставки за манипулация, психологически натиск и злоупотреби. На Фиг. 2 са показани рисковете от социалните мрежи.



Фиг. 2: Рискове от социалните мрежи

Методи за защита на личната информация

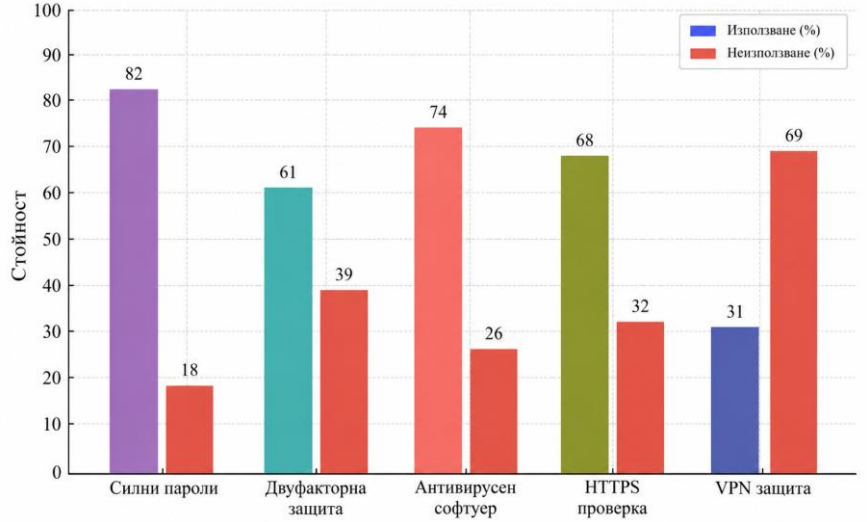
Един от най-ефективните методи за защита е използването на силни и уникални пароли. Кратките и лесни за отгатване пароли значително увеличават риска от неоторизиран достъп до профилите. Добра практика е използването на комбинация от букви, цифри и специални символи, както и редовната смяна на паролите. Двуфакторната автентикация предоставя допълнително ниво на сигурност. Освен парола, потребителят трябва да потвърди самоличността си чрез код, изпратен на телефон или приложение. Това значително намалява риска от пробив в профила дори при откраднатата парола. Важно значение има и редовното обновяване на софтуера. Много кибератаки се възползват от стари версии на приложения и операционни системи, които съдържат уязвимости. Актуализациите често включват защита срещу новооткрити заплахи. Потребителите трябва да бъдат внимателни и при използването на непознати сайтове. Проверяването дали даден сайт използва защитена връзка с „https“ е основна стъпка към по-сигурно сърфиране [6], [9]. Освен това не е препоръчително да се изтеглят файлове или програми от съмнителни източници. Дигиталната култура е също толкова важна, колкото и техническите средства за сигурност. В [12] е представено изследване, демонстриращо по-пълното емоционалното изживяване на потребителя на дадено приложение и по-високата му ангажираност към приложенията, предлагащи създаване на акаунт. Това обаче води до съответните рискове за личните данни.

Информираността относно онлайн рисковете помага на хората да разпознават измамите и да реагират адекватно при съмнителни ситуации. Образованието по киберсигурност трябва да бъде част от подготовката на младите хора в

съвременното общество. В таблица 2 са представени процентите на използвани методи за защита, а на фиг. 3 – диаграма на резултатите.

Таблица 2: Използвани методи за защита на личната информация сред интернет потребители

Метод за защита	Процент потребители
Силни пароли	82 на 100
Двуфакторна автентикация	61 на 100
Антивирусен софтуер	74 на 100
Редовна смяна на пароли	49 на 100
Проверка на HTTPS сайтове	68 на 100
Избягване на съмнителни линкове	77 на 100
VPN защита	31 на 100



Фиг. 3: Резултати от използваните методи

Психологическо влияние и манипулация в интернет

Освен техническите рискове, интернет създава и психологически опасности. Онлайн платформите често използват алгоритми, които анализират поведението на потребителите и им показват съдържание, съобразено с техните интереси. Това може да доведе до манипулация на мнението и поведението на хората. Фалшивите новини и дезинформацията са сериозен проблем в дигиталната среда. Чрез подвеждаща информация могат да се влияят обществени нагласи, политически

решения и дори лични избори. Много потребители приемат информацията в интернет без критично мислене, което улеснява разпространението на манипулативно съдържание. Съществува и риск от психологически натиск и онлайн тормоз. Социалните мрежи позволяват анонимност, което понякога насърчава агресивно поведение. Жертви на подобни атаки често са деца и младежи, които могат да изпитат сериозен емоционален стрес. Прекомерното използване на интернет и социалните мрежи също оказва влияние върху психичното здраве. Постоянното сравняване с другите, нуждата от одобрение и зависимостта от онлайн присъствие могат да доведат до тревожност и ниско самочувствие. Това показва, че защитата в интернет не се изчерпва само с техническата сигурност, а включва и психическото благополучие на потребителите. Допълнителен проблем е зависимостта от постоянното онлайн присъствие и нуждата от бързо получаване на информация и одобрение. Много хора прекарват значителна част от времето си в социалните мрежи, което може да доведе до намалена концентрация, социална изолация и затруднения в реалната комуникация. Особено при младите потребители прекомерната употреба на интернет често влияе негативно върху съня, учебния процес и емоционалното състояние. Това показва, че дигиталната среда оказва не само информационно, но и сериозно психологическо въздействие върху съвременното общество.

Казус: Психологическо влияние и манипулация в интернет

Разгледан е симулационен казус с данни за 100 ученици на възраст между 15 и 18 години относно влиянието на социалните мрежи и интернет върху тяхното психично състояние. Целта е да се изчисли нивото на психологическо въздействие чрез математически модел. При изследването са използвани следните показатели:

A – средно време онлайн на ден;
T – доверие към информацията в интернет;
F – честота на срещане на фалшиви новини;
D – степен на влияние от дезинформация;
S – време, прекарано в социални мрежи;
Z – зависимост от онлайн одобрение.

Моделът за психологическо влияние е:

$$P = \frac{(A \times T)+(F \times D)+(S \times Z)}{3} \quad (1)$$

След обработка на анкетите са получени следните средни стойности:

$$A = 7, T = 8, F = 6, D = 7, S = 5, Z = 9$$

Замествайки стойностите във формулата:

$$P = \frac{(7\times8)+(6\times7)+(5\times9)}{3} = \frac{56+42+45}{3} = \frac{143}{3} = 47{,}7 \quad (2)$$

Полученият резултат $P = 47{,}7$ показва много високо ниво на психологическо влияние върху изследваната група. Анализът показва, че най-силно влияние

оказват социалните мрежи и зависимостта от онлайн одобрение. Допълнително е изследван рискът от интернет зависимост чрез формулата:

$$R = \frac{H+M+C}{3} \tag{3}$$

където:

H – часове онлайн дневно;

M – емоционална зависимост от социални мрежи;

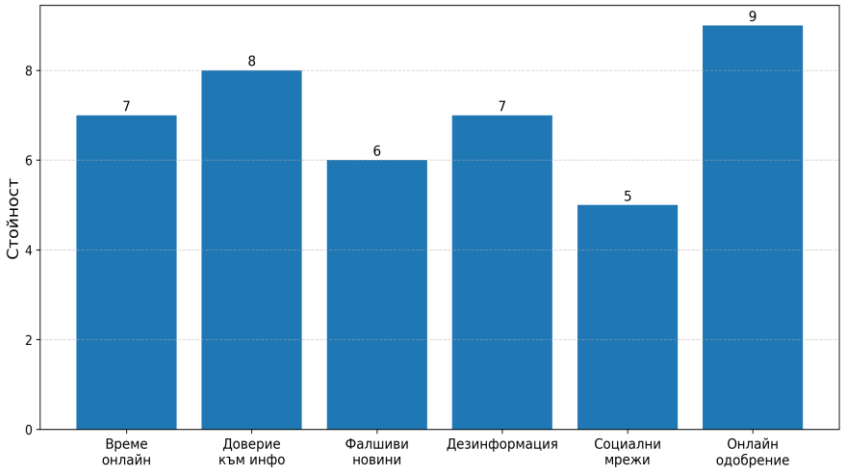
C – проблеми с концентрацията.

От изследването са получени стойности:

$$H = 9, M = 8, C = 7$$

$$\mathrm{R} = \frac{9+8+7}{3} = \frac{24}{3} = 8 \tag{4}$$

Стойността $R = 8$ показва сериозен риск от интернет зависимост сред участниците в изследването. Резултатите доказват, че прекомерното използване на интернет и социалните мрежи оказва силно влияние върху психичното здраве, концентрацията и емоционалното състояние на младите хора. На фиг. 4 е показан резултатът от казуса.



Фиг. 4: Психологическото влияние в интернет

Изкуствен интелект и рискове за личните данни

Развитието на изкуствения интелект променя начина, по който се събират, анализират и обработват личните данни в интернет. Много съвременни платформи използват алгоритми за анализ на потребителското поведение, интересите и навиците на хората. Чрез събирането на големи количества информация системите

могат да създават подробни профили на потребителите, които се използват за реклами, препоръки и автоматизирани решения [11]. Въпреки удобствата, които изкуственият интелект предоставя, съществуват и сериозни рискове за личната неприкосновеност. Алгоритмите често обработват чувствителна информация без потребителите да осъзнават какъв обем данни се събира за тях. В някои случаи това може да доведе до нарушаване на личното пространство, неправомерно наблюдение или използване на информацията за манипулиране на потребителското поведение. Допълнителен проблем представляват т.нар. „deepfake" технологии, които чрез изкуствен интелект могат да създават фалшиви изображения, аудио и видеоклипове. Подобни материали могат да бъдат използвани за измами, разпространяване на невярна информация или уронване на репутацията на даден човек. С развитието на технологиите става все по-трудно да се различава реалното съдържание от изкуствено генерираното. Поради тази причина е необходимо да се създават по-строги правила и етични стандарти относно използването на изкуствен интелект [3]. Потребителите трябва да бъдат информирани как се обработват техните данни и да имат контрол върху личната информация, която предоставят онлайн [4]. Развитието на технологиите трябва да бъде съпроводено със защита на човешките права и личната сигурност в дигиталната среда [5].

Заключение

Интернет предоставя огромни възможности за развитие, комуникация и достъп до информация, но същевременно крие сериозни рискове за личната информация. Киберпрестъпленията, злоупотребите с данни и манипулацията в онлайн средата се превръщат във все по-голямо предизвикателство за съвременното общество. Защитата на личната информация изисква комбинация от технологични мерки, информираност и отговорно поведение. Използването на сигурни пароли, вниманието към онлайн съдържанието и развитието на дигитална култура са основни елементи за по-безопасно използване на интернет. В бъдеще значението на киберсигурността ще продължи да нараства. Колкото повече технологиите навлизат в ежедневието, толкова по-важно ще бъде хората да умеят да защитават своите данни и личното си пространство. Само чрез осъзнато и отговорно поведение може да се постигне баланс между удобствата на дигиталния свят и сигурността на личната информация. Допълнително внимание трябва да се обръща и на ролята на институциите, образователните организации и технологичните компании в процеса по защита на личните данни. Създаването на ясни правила, законови регулации и ефективни механизми за контрол е важна стъпка към ограничаване на злоупотребите в интернет пространството [8]. Компаниите, които обработват потребителска информация, носят сериозна отговорност за съхранението и защитата на тези данни, тъй като дори малък пробив в сигурността може да засегне огромен брой хора. Освен техническата защита, важно значение има и изграждането на критично мислене при използването на интернет. Потребителите трябва да умеят да разпознават фалшиви сайтове, подвеждащи съобщения и опити за манипулация. Развитието на дигитални умения и информираността относно онлайн рисковете ще бъдат сред най-важните фактори

за сигурността в бъдещото информационно общество. Само чрез съчетание между технологичен напредък, образование и лична отговорност може да се гарантира по-сигурна и защитена дигитална среда.

Литература

1. Cranor, L. F. (1999). Internet privacy. Communications of the ACM, 42(2), 28–31.
2. Altman, M., Wood, A., O'Brien, D. R., & Gasser, U. (2018). Practical approaches to big data privacy over time. International Data Privacy Law, 8(1), 29–51.
3. Gstrein, J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. Philosophy & Technology, 35, Article 3, 1–25.
4. Dix, A. (2010). Built-in privacy—No panacea, but a necessary condition for effective privacy protection. Identity in the Information Society, 3, 257–265.
5. Rachovitsa, A. (2016). Engineering and lawyering privacy by design: Understanding online privacy both as a technical and an international human rights issue. International Journal of Law and Information Technology, 24(4), 374–399.
6. Munn, L., Hristova, T., & Magee, L. (2019). Clouded data: Privacy and the promise of encryption. Big Data & Society, 6(1).
7. Nissim, K., & Wood, A. (2018). Is privacy privacy? Philosophical Transactions of the Royal Society A, 376(2128), 1–16.
8. Birrell, E., Rodolitz, J., Ding, A., Lee, J., McReynolds, E., Hutson, J., & Lerner, A. (2024). SoK: Technical implementation and human impact of internet privacy regulations. 2024 IEEE Symposium on Security and Privacy.
9. Цанков, Ц. С. (2018). Приложения на нелинейните функции за защита на информацията в комуникационните системи. Шумен: Университетско издателство „Епископ Константин Преславски", 204 с. ISBN 978-619-201-212-0.
10. Konstantinova, E., Karadocheva, M., & Tsankov, Ts. (2019). The invisible Internet and cyber security. Proceedings of the International Scientific Conference 2019, Vasil Levski National Military University, Artillery, Air Defense and Communication and Information Systems Faculty, Shumen, 519–524. ISSN 2367-7902.
11. Simeonova, I. (2025). How GDPR treats automated decision-making. Journal Scientific and Applied Research, 28(1). Shumen: Konstantin Preslavsky University Press. ISSN 1314-6289.
12. Mincheva, S., & Stoyanova, V. (2025). Research on the impact of the user experience for the success of a virtual product: Bulgarian travel agency websites. Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference, 2, 237–241.

PASSWORD SECURITY ASSESSMENT THROUGH ENTROPY ANALYSIS AND DIFFERENT GENERATION STRATEGIES

Gabriela S. Markova[1], Daniel R. Denev[2]

Faculty of Technical Sciences, Department of Communication and Computer Engineering and Security Technologies, Konstantin Preslavsky University of Shumen, Shumen, Bulgaria, [1]2570020001@shu.bg, [2]d.denev@shu.bg

***Abstract**: Passwords remain a primary authentication method, although their security is affected by guessing, interception, and information-system breaches. This report assesses password security through information entropy and compares user-selected passwords, randomly generated passwords, and passphrases. The analysis considers password length, character set, randomness, and user-choice predictability. The results show that long, unique, and randomly generated passwords provide the highest security, especially when combined with password managers and multi-factor authentication.*

***Keywords**: Passwords, Information security, Authentication*

ОЦЕНКА НА СИГУРНОСТТА НА ПАРОЛИ ЧРЕЗ АНАЛИЗ НА ЕНТРОПИЯТА И РАЗЛИЧНИ СТРАТЕГИИ ЗА ГЕНЕРИРАНЕ

Габриела С. Маркова[1], Даниел Р. Денев[2]

Факултет по технически науки, катедра „Комуникационна и компютърна техника и технологии за сигурност", Шуменски университет „Епископ Константин Преславски", гр. Шумен, България, [1]2570020001@shu.bg, [2]d.denev@shu.bg

***Резюме**: Паролите остават основен метод за удостоверяване, въпреки рисковете от отгатване, прихващане и компрометиране на информационни системи. Докладът оценява сигурността им чрез информационната ентропия и сравнява ръчно избрани пароли, случайно генерирани пароли и passphrase конструкции. Анализирани са дължината, използваният набор от знаци, случайността и предвидимостта на потребителския избор. Резултатите показват, че дългите, уникални и случайно генерирани пароли осигуряват най-висока защита, особено в комбинация с мениджър на пароли и многофакторно удостоверяване.*

***Ключови думи**: Пароли, Информационна сигурност, Удостоверяване*

Въведение

Съвременните информационни системи съхраняват огромни количества информация, част от която има висока степен на чувствителност. Достъпът до тези ресурси обикновено се контролира посредством механизми за удостоверяване на потребителите. Въпреки развитието на биометричните технологии, многофакторната автентикация и различните безпаролни решения, паролите продължават да бъдат основен компонент на множество системи за контрол на

достъпа. Именно поради това тяхната сигурност има съществено значение за цялостната защита на информационните ресурси [12]. Една от основните слабости на паролите е зависимостта им от човешкото поведение. Потребителите често избират пароли, които са лесни за запомняне, но същевременно са предвидими. Използването на имена, дати, популярни думи, последователности от цифри или сходни комбинации създава възможност за ефективни атаки чрез автоматизирано отгатване. Допълнителен проблем представлява повторното използване на една и съща парола в различни услуги. При компрометиране на една система нападателят може да използва получените идентификационни данни за опит за достъп до други системи. За оценка на сигурността на паролите често се използва понятието информационна ентропия. Тя позволява да бъде оценена степента на неопределеност при избора на дадена парола и по този начин да се направи теоретична оценка на броя възможни комбинации. Въпреки това математическата ентропия не винаги отразява реалната сигурност на човешки избрана парола, тъй като предполага определена степен на случайност. Поради тази причина анализът на сигурността трябва да включва както математически характеристики, така и особеностите на реалното поведение на потребителите. Целта на настоящия доклад е да се направи анализ на сигурността на различни типове пароли чрез разглеждане на тяхната ентропия и да се сравнят различни стратегии за генериране. Въз основа на анализа се формулират основни принципи за създаване и използване на устойчиви пароли. [4], [5]

Информационна ентропия и сигурност на паролите

Понятието информационна ентропия произлиза от теорията на информацията, разработена от Клод Шанън. В контекста на паролите ентропията може да бъде разглеждана като мярка за неопределеността при избора на конкретна комбинация. Колкото по-голям е броят на равновероятните възможности, толкова по-голяма е теоретичната ентропия. При условие че всеки символ от дадено множество се избира напълно случайно, ентропията на парола с фиксирана дължина може да бъде изчислена чрез формулата $H = L \times log_2(N)$, където H представлява ентропията в битове, L е дължината на паролата, а N е броят на възможните символи. Например при парола с дължина 10 символа и множество от 94 възможни печатаеми символа броят на всички възможни комбинации е 94^{10}. Теоретичната ентропия в този случай е приблизително 65,5 бита. Това означава, че ако всички комбинации са еднакво вероятни, нападателят би трябвало да разглежда огромно пространство от възможности при опит за изчерпателно търсене. Важен момент е, че подобно изчисление е валидно само когато изборът на символите действително е случаен. При човешки избрана парола предположението за равномерно разпределение обикновено не е изпълнено. Ако например потребителят избере парола, която представлява обичайна дума, последвана от няколко цифри, реалното пространство за търсене е значително по-малко от теоретичното пространство на всички възможни комбинации. Именно поради тази причина съвременните препоръки за сигурност не разглеждат ентропията като единствен критерий за оценка на паролите. NIST обръща внимание на трудността при определяне на

действителната ентропия на потребителски избрани пароли и поставя значителен акцент върху дължината на паролата, проверката срещу списъци с компрометирани пароли и ограничаването на автоматизирани атаки. В таблица 1 е представено сравнението на стратегии за генериране на пароли [3].

Таблица 1: Сравнение на стратегии за генериране на пароли

№	Стратегия	Дължина	Ентропия	Сигурност
1	Ръчно избрана	8–10	Ниска	2
2	Сложна ръчна	10–12	Средна	3
3	Случайна	12–16	Висока	5
4	Passphrase	16–25+	Висока	4
5	Мениджър на пароли	16–24+	Много висока	5

Влияние на дължината и разнообразието на символите

Дължината на паролата е един от най-важните фактори, определящи нейното теоретично ниво на сигурност. При случайно генерирана парола всяко допълнително място увеличава броя на възможните комбинации експоненциално. Ако например една парола се състои от символи, избрани от множество от 62 възможности, броят на комбинациите при осем символа е 62^8, докато при дванадесет символа той достига 62^{12}. Това показва, че увеличаването на дължината може да има много значителен ефект върху устойчивостта срещу brute-force атаки. Разнообразието на използваните символи също оказва влияние върху теоретичната ентропия. Използването на малки и главни букви, цифри и специални символи увеличава размера на множеството, от което могат да бъдат избирани символите. Въпреки това при човешки избрани пароли по-голямото разнообразие не гарантира автоматично по-висока сигурност. Потребителите често прилагат лесно предвидими правила, като поставяне на главна буква в началото на думата, добавяне на цифра в края или замяна на определени букви със специални символи. Следователно съвременният подход към сигурността на паролите не трябва да се основава единствено на формални изисквания за определен брой главни букви, цифри и специални символи. Много по-важно е паролата да бъде достатъчно дълга, уникална и трудна за предвиждане. Това е особено важно при системи, които са изложени на автоматизирани атаки. На фиг. 1 е показано влиянието на по-дългите пароли [7].

Стратегии за генериране на пароли

Един от най-разпространените подходи е потребителят сам да избере своята парола. Предимството на този метод е, че паролата обикновено е сравнително лесна за запомняне. Основният недостатък обаче е високата степен на предвидимост. Хората са склонни да използват думи и комбинации, които имат лично или културно значение. Това намалява броя на реалистичните възможности, които нападателят трябва да провери. По-надежден подход е използването на криптографски сигурен генератор на случайни числа за създаване на пароли

[10], [11]. При този метод всеки символ се избира независимо и случайно от предварително определено множество [11].



Фиг. 1: Влиянието на по-дълга парола

Ако например се генерира парола от 16 символа и всеки символ може да бъде избран измежду 94 възможни символа, теоретичната ентропия е приблизително 105 бита. При правилно реализиран генератор такава парола е изключително трудна за отгатване чрез изчерпателно търсене. Друг подход представляват passphrase паролите, при които вместо отделни случайни символи се използват няколко думи. Този метод може да осигури добра комбинация между сигурност и запомняемост. Ако думите се избират независимо и случайно от достатъчно голям речник, ентропията се увеличава с всяка допълнителна дума. Например при речник от 7776 думи четири случайно избрани думи дават приблизително 51,7 бита теоретична ентропия, докато пет думи дават приблизително 64,6 бита. Съществено е обаче думите да бъдат действително избрани случайно. Изречение, което потребителят сам е измислил, не е еквивалентно на случайна passphrase. Ако фразата представлява известен цитат, текст от песен или често използван израз, тя може да бъде включена в речници и бази от данни, използвани при атаки. На фиг. 2 е показана стратегия за генериране на парола. [6]



Фиг. 2: Стратегия за генериране на парола

Атаки срещу пароли

Сигурността на паролите трябва да се разглежда в контекста на възможните атаки. При brute-force атака нападателят систематично проверява различни комбинации, докато открие правилната, като при случайна парола с H бита

ентропия броят им е 2^H. При dictionary атака се използват предварително подготвени списъци с думи, популярни пароли и характерни модели, поради което тя е особено ефективна срещу предвидими човешки избори. При credential stuffing се прилагат откраднати потребителски имена и пароли от компрометирани услуги. Повторното използване на една парола за различни акаунти може да доведе до компрометирането на всички тях, затова нейната уникалност е също толкова важна, колкото сложността ѝ. Наред с атаките, насочени пряко към паролите, риск за удостоверителните данни създават и заплахите от типа „zero-day". В [13] са разгледани възможностите на технологията FireEye HX Endpoint Security за откриване, анализ и разследване на такива заплахи на ниво крайна точка чрез Endpoint Detection and Response (EDR). В таблица 2 е представен експоненциалният характер на зависимостта между ентропията и броя на възможните комбинации [8].

Таблица 2: Експоненциален характер на зависимостта между фактори

Ентропия (H)	Възможни комбинации (2^H)	Увеличение спрямо 40 бита
40 бита	$\approx 1{,}10 \times 10^{12}$	1×
50 бита	$\approx 1{,}13 \times 10^{15}$	1 024×
60 бита	$\approx 1{,}15 \times 10^{18}$	1 048 576×
80 бита	$\approx 1{,}21 \times 10^{24}$	$\approx 1{,}10 \times 10^{12}$×
100 бита	$\approx 1{,}27 \times 10^{30}$	$\approx 1{,}07 \times 10^{18}$×

Съхранение и управление на паролите

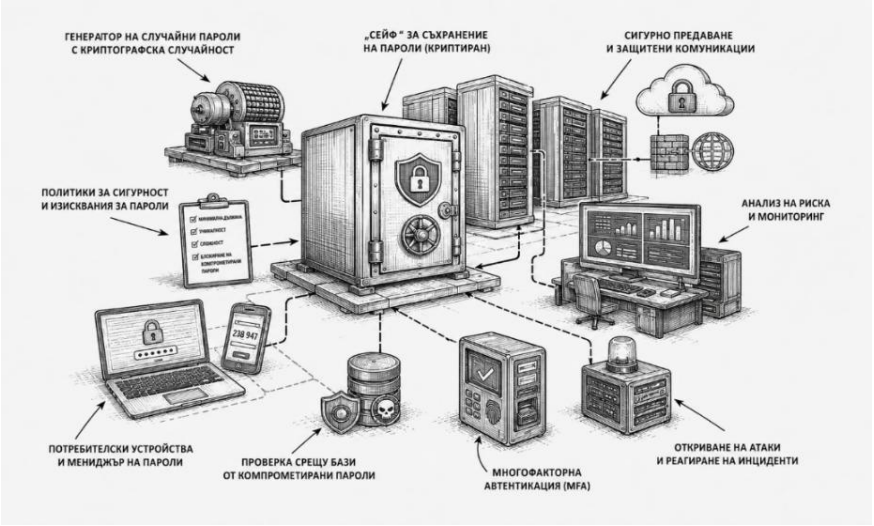
Сигурността на паролите не зависи единствено от начина, по който те се генерират. От съществено значение е и начинът, по който се съхраняват от информационната система. Паролите не трябва да се съхраняват в чист текст, тъй като при компрометиране на базата данни всички потребителски идентификационни данни биха станали директно достъпни за нападателя. Вместо това се използват специализирани алгоритми за хеширане и извеждане на ключове, предназначени за защита на пароли. Сред подходящите съвременни решения са Argon2id, bcrypt и PBKDF2. Те са проектирани така, че обработката на всяка парола да изисква значителни изчислителни ресурси, което затруднява масовото отгатване при offline атаки. Допълнителното използване на уникална сол за всяка парола предотвратява редица атаки, при които еднакви пароли биха имали еднакви хешове. Друг важен елемент е използването на мениджъри на пароли. Те позволяват създаването на дълги и случайни пароли, които потребителят не е необходимо да запомня. Това значително улеснява използването на различна парола за всяка услуга и по този начин намалява риска от credential stuffing. Към защитата на паролите следва да се добави и многофакторната автентикация. При нея достъпът не зависи единствено от знанието на паролата, а изисква допълнителен фактор. По този начин дори при компрометиране на паролата нападателят може да бъде възпрепятстван да получи достъп до акаунта. Освен сигурното съхранение на паролите, важно значение има и правилното управление

на достъпа до тях в рамките на информационната система. Приложенията и администраторите не трябва да имат ненужни права за достъп до базите данни, съдържащи удостоверителна информация. Прилагането на принципа на минималните привилегии ограничава последствията при компрометиране на даден компонент. Добра практика е също така достъпът до чувствителни данни да бъде регистриран и наблюдаван, което позволява своевременно установяване на подозрителна активност. Сигурността на паролите изисква и подходящи механизми за възстановяване и промяна на потребителските идентификационни данни. Процедурите за възстановяване на забравена парола трябва да бъдат защитени по начин, който не позволява на нападател да ги използва за заобикаляне на основната автентикация. Временните връзки или кодове за възстановяване следва да бъдат достатъчно случайни, с ограничен срок на валидност и да могат да бъдат използвани еднократно. При промяна на паролата системата трябва да предотвратява лесното използване на слаби или вече компрометирани пароли. Необходимо е също организациите периодично да преглеждат своите политики за управление на паролите и да ги адаптират към актуалните заплахи. Особено важно е потребителите да бъдат информирани за рисковете от повторното използване на една и съща парола, споделянето на идентификационни данни и въвеждането им в непознати или подозрителни сайтове. Комбинацията от сигурно хеширане, уникални соли, мениджъри на пароли, многофакторна автентикация и контрол върху достъпа изгражда многослойна защита [9]. По този начин сигурността не се основава на един-единствен механизъм, а на съвкупност от взаимно допълващи се мерки. На фиг. 3 е показана архитектура на система за сигурно генериране [1].

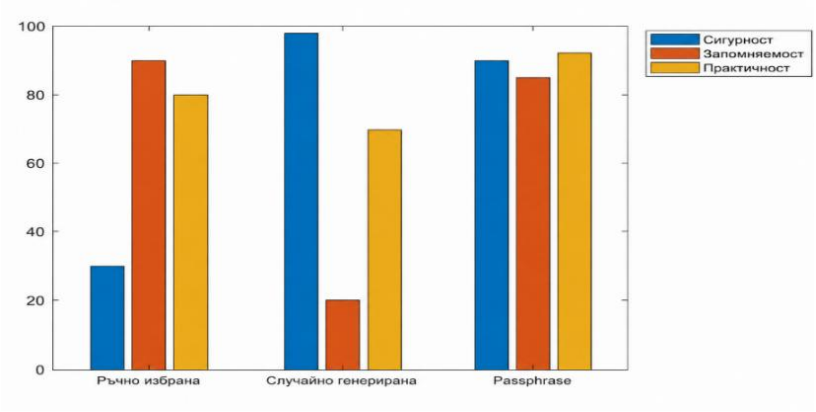
Сравнителна оценка на различните стратегии

Сравнението между различните методи за генериране показва, че ръчно избраните пароли имат най-висока степен на предвидимост, когато са основани на лична информация или популярни думи. Те са удобни за запомняне, но могат да бъдат ефективно атакувани чрез речникови атаки и модели за предвиждане на потребителския избор. Дори когато съдържат цифри и специални символи, тяхната реална ентропия може да бъде значително по-ниска от теоретичната. Случайно генерираните пароли предоставят най-добър резултат от гледна точка на математическата оценка на сигурността. При тях може сравнително точно да бъде определено пространството на възможните комбинации, а при достатъчна дължина и правилен генератор вероятността за успешно отгатване става изключително малка. Основният недостатък е, че такива пароли обикновено са трудни за запомняне, което прави използването на мениджър на пароли практически необходимо. Passphrase паролите представляват компромис между тези два подхода. Те могат да бъдат значително по-дълги и по-лесни за запомняне, като същевременно осигуряват висока степен на сигурност, когато думите са избрани случайно. Поради това този метод е особено подходящ в ситуации, при които потребителят трябва да въведе или запомни паролата ръчно. Таблица 3 показва нормализирана оценка на сигурността, запомняемостта и практичността на

различни стратегии за генериране на пароли, а фиг. 4 графично сравнение на различните стратегии за генериране на пароли [2].



Фиг. 3: Архитектура на система за сигурно генериране, съхранение и управление



Фиг. 4: Графично сравнение на различни стратегии за генериране на пароли

Таблица 3: Нормализирана оценка на сигурността, запомняемостта и практичността на различни стратегии за генериране на пароли

Стратегия	Сигурност	Запомняемост	Практичност
Ръчно избрана	30	90	80
Случайно генерирана	98	20	70
Passphrase	90	85	92

Заключение

Извършеният анализ показва, че сигурността на паролите е резултат от взаимодействието на няколко различни фактора. Теоретичната ентропия предоставя удобен математически модел за оценка на броя възможни комбинации при случайно генерирани пароли, но не е достатъчна за определяне на реалната сигурност на човешки избраните пароли. Основната причина е, че човешкото поведение не следва равномерно случайно разпределение. Увеличаването на дължината на паролата има особено важна роля, тъй като при случайно генериране води до експоненциално нарастване на пространството за търсене. Използването на по-голямо множество от символи също увеличава теоретичната ентропия, но при човешки избор ефектът може да бъде ограничен от предвидими модели. Поради тази причина случайността и уникалността са ключови характеристики на сигурната парола. От разгледаните стратегии случайното генериране предоставя най-ниска степен на предвидимост и най-висока математическа устойчивост от математическа гледна точка, докато passphrase подходът предлага добър баланс между сигурност и удобство. Най-подходящата практика в реални условия е използването на дълги, уникални и случайно генерирани пароли, съхранявани посредством надежден мениджър на пароли. За пароли, които трябва да бъдат запомнени, могат да се използват достатъчно дълги случайно избрани passphrase конструкции. В крайна сметка сигурността на паролите не трябва да се разглежда като характеристика само на самата парола. Тя е част от цялостния процес на удостоверяване и включва начина на генериране, съхранение, предаване и използване на идентификационните данни. Комбинирането на силни уникални пароли, сигурно съхранение, защита срещу автоматизирани атаки и многофакторна автентикация предоставя значително по-надеждна защита на информационните системи.

Литература

1. Shannon, C. E. (1948). A mathematical theory of communication. Bell System Technical Journal, 27(3), 379–423; 27(4), 623–656.
2. National Institute of Standards and Technology. (n.d.). Digital identity guidelines: Authentication and lifecycle management (NIST Special Publication 800-63B). NIST.
3. National Institute of Standards and Technology. (n.d.). Strength of passwords. NIST Digital Identity Guidelines.

4. Weir, M., Aggarwal, S., Collins, M., & Stern, H. (2010). Testing metrics for password creation policies by attacking large sets of revealed passwords. Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS '10), 163–175. https://doi.org/10.1145/1866307.1866327
5. Bonneau, J. (2012). The science of guessing: Analyzing an anonymized corpus of 70 million passwords. Proceedings of the 2012 IEEE Symposium on Security and Privacy, 538–552. https://doi.org/10.1109/SP.2012.49
6. Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L. F., & López, J. (2012). Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. Proceedings of the 2012 IEEE Symposium on Security and Privacy.
7. Egelman, S., Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., & Cranor, L. F. (2011). Of passwords and people: Measuring the effect of password-composition policies. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11). https://doi.org/10.1145/1978942.1979321
8. Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. Proceedings of the 16th International Conference on the World Wide Web (WWW '07), 657–666. https://doi.org/10.1145/1242572.1242661
9. Цанков, Ц. С. (2018). Приложения на нелинейните функции за защита на информацията в комуникационните системи. Шумен: Университетско издателство „Епископ Константин Преславски", 204 с. ISBN 978-619-201-212-0.
10. Беджев, Б. Й., Цанков, Ц. С., & Станева, Л. А. (2013). Свиващ генератор на псевдослучайни последователности, формирани чрез нелинейни функции. Научна конференция „Защитата на личните данни в контекста на информационната сигурност", факултет „Артилерия, ПВО и КИС", Шумен, 141–149. ISBN 978-954-9681-49-9.
11. Николов, Н. Р., & Цанков, Ц. С. (2010/2011). Хардуерна реализация на генератор на псевдослучайни последователности, описван с полином от 1024 степен и програмно управление на обратните връзки. Научна сесия на факултет „Артилерия, ПВО и КИС", Шумен. ISSN 1313-7433.
12. Кемил, И., & Симеонова, И. (2025). Дигитализация и предизвикателствата пред сигурността в електронната администрация. Национална научна конференция на Националния военен университет „Васил Левски", Велико Търново, 12–14 ноември 2025 г.
13. Rakov, M., & Stoyanova, V. (2025). Analyses and investigation of 0-day threats with FireEye. Engineering Sciences, №1, 3–9. http://es.ims.bas.bg/Abstracts/A2025/a1/01-01.pdf

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

USING COMMUNICATION NETWORKS AND GRAPH MODELS TO PREDICT ACADEMIC ACHIEVEMENT IN GEOGRAPHY EDUCATION

Daniel R. Denev[1], Madlen A. Todorova[2]

Konstantin Preslavsky University of Shumen,
Shumen, Bulgaria, [1]d.denev@shu.bg, [2]madlen2000@abv.bg

***Abstract**: This scientific report examines the application of communication networks and graph models to predict academic achievement in geography education. The focus is on how the structures of social and informational interactions between students can be formalized through graphs. These models analyze the relationships between students, teachers, and learning resources, allowing for a more accurate understanding of success factors. The study highlights the potential of network analysis as a tool for improving educational outcomes and early identification of difficulties.*

***Keywords**: Education, Communication networks, Students, Teachers*

ИЗПОЛЗВАНЕ НА КОМУНИКАЦИОННИ МРЕЖИ И ГРАФОВИ МОДЕЛИ ЗА ПРОГНОЗИРАНЕ НА АКАДЕМИЧНИТЕ РЕЗУЛТАТИ В ОБУЧЕНИЕТО ПО ГЕОГРАФИЯ

Даниел Р. Денев[1], Мадлен А. Тодорова[2]

Шуменски университет „Епископ Константин Преславски“,
гр. Шумен, България, [1]d.denev@shu.bg, [2]madlen2000@abv.bg

***Резюме**: Настоящият научен доклад разглежда приложението на комуникационни мрежи и графови модели за прогнозиране на академичните резултати в обучението по география. Фокусът е върху това как структурите на социалните и информационните взаимодействия между учениците могат да бъдат формализирани чрез графи. Чрез тези модели се анализират връзките между ученици, учители и учебни ресурси, което позволява по-точно разбиране на факторите за успех. Изследването подчертава потенциала на мрежовия анализ като инструмент за подобряване на образователните резултати и ранно идентифициране на затруднения.*

***Ключови думи**: Образование, Комуникационни мрежи, Ученици, Учители*

Въведение

Съвременното образование все повече се възползва от методи на изкуствения интелект и анализ на данни за подобряване на учебния процес. В обучението по география се наблюдава натрупване на големи обеми данни за представянето на учениците, техните взаимодействия и достъпа им до ресурси. Тези данни могат да бъдат моделирани чрез комуникационни мрежи, които представят участниците като върхове в граф, а взаимодействията като ребра. По този начин се създава основа за прогнозиране на академичните резултати чрез математически и статистически подходи. Целта на доклада е да представи основните принципи и

приложения на графовите модели в този контекст. Съвременните образователни среди все по-често се дигитализират, което създава нови възможности за събиране и анализ на данни [11]. В обучението по география това включва платформи за електронно обучение, онлайн тестове и интерактивни карти. Тези източници предоставят информация за поведението и напредъка на учениците в реално време. Важен аспект е, че тези данни не са изолирани, а взаимосвързани чрез комуникационни канали между ученици и учители. Това позволява изграждането на мрежова картина на учебния процес. Така се преминава от традиционно индивидуално оценяване към системен анализ на групова динамика. Използването на графови модели дава възможност да се представят сложни зависимости по ясен и математически начин. Вместо да се разглеждат само крайни оценки, се анализират процесите, които водят до тях. Това включва взаимодействия, честота на комуникация и обмен на учебни ресурси. Целта на изследванията в тази област е не само прогнозиране, но и оптимизация на обучението. Чрез идентифициране на ключови фактори може да се подобри ефективността на преподаването по география. Това прави темата особено актуална за съвременното образование. На фиг. 1 е показана логическа схема. [1]



Фиг. 1: Логическа схема

Теоретична основа на графовите модели в образованието

Графовите модели представляват математически структури, състоящи се от върхове и ребра, които описват отношения между обекти. В образователния контекст върховете могат да бъдат ученици, учители или учебни материали, а ребрата – комуникация или сътрудничество. Тези модели позволяват анализ на сложни социални и учебни взаимодействия, които трудно се улавят с традиционни методи. Чрез тях се идентифицират ключови възли, които оказват най-силно влияние върху разпространението на знания. Това създава основа за по-задълбочено разбиране на учебната динамика. Графовата теория има широко приложение в компютърните науки, социалните мрежи и биоинформатиката, но в образованието тя е сравнително нов подход. Основната идея е, че всяка система от взаимодействия може да бъде представена като мрежа. Това позволява използване на утвърдени алгоритми за анализ. Един от ключовите елементи е понятието за централност, което измерва значимостта на даден възел в мрежата. В образователен контекст това може да покаже кои ученици влияят най-много върху

груповата динамика. Също така се анализират и периферните участници, които често са в риск от изоставане. В таблица 1 са представени графовите метрики [3].

Таблица 1. Графови метрики

Метрика (граф)	Какво измерва	Наблюдаван диапазон в училищни мрежи
Плътност на мрежата	Колко от всички възможни връзки реално съществуват	0.10 – 0.45
Средна степен на връзки	Среден брой контакти на ученик	3 – 12 връзки
Коефициент на клъстериране	Колко силно учениците се групират в подгрупи	0.25 – 0.70
Централност	Влияние/свързаност на ключови ученици	0.05 – 0.35
Корелация между централност и успех (r)	Връзка между позиция в мрежата и оценки	0.30 – 0.65

Друг важен аспект е клъстерирането, което разделя мрежата на подгрупи със силни вътрешни връзки. Това може да отразява учебни групи или неформални социални общности в класа. Анализът на тези структури помага да се разбере как се разпространява знанието. Освен това графовите модели позволяват симулации на различни сценарии. Например може да се прогнозира как промяна в поведението на един ученик влияе върху цялата мрежа. [2]

Комуникационни мрежи в обучението по география

В обучението по география съвременните комуникационни мрежи осигуряват основата за достъп до дигитални учебни ресурси като интерактивни карти, географски информационни системи (GIS), тестови платформи и мултимедийни материали [10]. Чрез тези мрежи се реализира обмен на данни между ученик, учител и образователни сървъри, което позволява бързо и ефективно усвояване на учебното съдържание. Предаването на информация в такива системи се извършва чрез пакетна комуникация, при която учебните данни се разделят на малки пакети и се предават по мрежата до крайното устройство. Този процес гарантира надеждност и възможност за възстановяване на информацията дори при частични прекъсвания, което е важно при работа с големи географски данни и визуализации. Качеството на комуникационната среда влияе директно върху педагогическия процес. Параметри като пропускателна способност, латентност и загуба на пакети определят скоростта на зареждане на карти, видеа и интерактивни упражнения. При нестабилна връзка се наблюдава забавяне на учебната дейност, което намалява ефективността на обучението и ангажираността на учениците. От педагогическа гледна точка тези комуникационни системи позволяват по-голяма интерактивност и индивидуализация на обучението по география [8]. Учителят може да използва онлайн платформи за възлагане на задачи, проследяване на напредъка и адаптиране на учебното съдържание според нуждите на учениците. Така технологичната

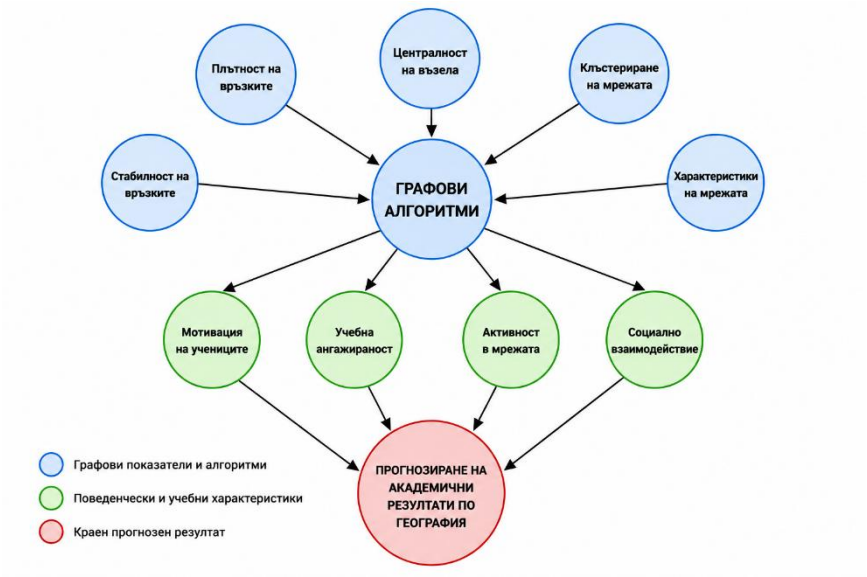
инфраструктура се превръща в пряка част от образователния процес. Таблица 2 показва влиянието на комуникационните мрежи върху обучението по география.

Таблица 2. Влияние на комуникационните мрежи върху обучението по география

Мрежов параметър	Типична стойност	Влияние върху обучението по география	Педагогически ефект
Пропускателна способност	10 Mbps – 1 Gbps	Определя скоростта на зареждане на карти, GIS и видео материали	По-бърз достъп до интерактивни ресурси
Латентност	10 ms – 150 ms	Забавя реакцията при интерактивни задачи и онлайн тестове	Намалена ангажираност при висока латентност
Загуба на пакети	0.1% – 3%	Води до прекъсване на карти, изображения или тестови данни	Нарушено възприемане на учебния материал
RTT	20 ms – 300 ms	Влияе върху скоростта на взаимодействие с платформи	По-бавна обратна връзка от системата
Стабилност на връзката	Висока / средна / ниска	Определя непрекъснатостта на учебния процес	Пряко влияе върху концентрацията и ефективността

Прогнозиране на академични резултати чрез графови алгоритми

Графовите алгоритми позволяват обработка на структурирани мрежови данни за извеждане на предсказателни модели. Те използват характеристики като централност, плътност на връзките и клъстериране на възли. В контекста на образованието тези показатели могат да се свържат с успеха на учениците по география. Например ученици с по-висока свързаност в мрежата често показват по-добри резултати. Това дава възможност за ранно прогнозиране на риска от ниска успеваемост. Прогнозните модели в образованието използват както структурни, така и поведенчески данни. Структурните включват връзките в мрежата, а поведенческите – активността на учениците. Комбинацията от двата типа данни подобрява точността на прогнозите. Алгоритмите за машинно обучение често се прилагат върху графови структури, за да се открият скрити зависимости [9]. Те могат да предскажат вероятността даден ученик да постигне висок или нисък резултат. Това позволява ранна намеса от страна на учителя. Особено важни са индикаторите като честота на взаимодействие и стабилност на връзките. Учениците с по-активна комуникация обикновено показват по-добро усвояване на материала. Това е особено валидно при сложни теми в географията. В бъдеще тези модели могат да бъдат интегрирани в образователни системи с изкуствен интелект. Те ще предоставят автоматични препоръки за подобряване на учебния процес. Това ще направи образованието по-адаптивно и персонализирано. На фиг. 2 е показан граф на учебния процес [5].



Фиг. 2: Концептуален модел за прогнозиране на академични резултати по география чрез графови алгоритми

Роля на учителя в мрежовите модели

В комуникационните компютърни мрежи, използвани в обучението по география, учителят участва като активен потребител в клиент–сървър архитектурата на образователните системи. Чрез тази структура той и учениците осъществяват достъп до отдалечени ресурси, като географски информационни системи (GIS), интерактивни карти и онлайн учебни платформи. Учителят има роля в организирането на сесиите на мрежова комуникация, при които се определя кога и как клиентските устройства (ученически компютри или таблети) се свързват към сървърите с учебно съдържание. Това включва синхронизиране на достъпа до ресурси по време на уроци, свързани с анализ на географски данни и карти. В рамките на комуникационната мрежа учителят използва различни мрежови услуги като уеб приложения, облачни платформи и споделени ресурси, за да осигури единен достъп до учебно съдържание. Това позволява всички ученици да работят върху една и съща база данни и материали независимо от устройството, което използват. От педагогическа гледна точка учителят адаптира учебния процес спрямо възможностите на мрежата, като избира подходящ тип комуникация (например уеб-базирани тестове или интерактивни карти в реално време). Така комуникационната мрежа се превръща в инфраструктурна основа за реализация на съвременното обучение по география. На фиг. 3 е показана образователна комуникационна мрежова архитектура. [4]



Фиг. 3: Образователна комуникационна мрежова архитектура

Практически приложения и ограничения

Приложението на графовите модели в образованието позволява създаване на системи за ранно предупреждение за учебни затруднения. Те могат да бъдат интегрирани в образователни платформи за автоматичен анализ на взаимодействията между учениците. Въпреки това съществуват ограничения, свързани с качеството на данните и етичните аспекти на наблюдението. Неточни или непълни данни могат да доведат до погрешни прогнози. Затова е необходимо внимателно балансиране между технологичните възможности и защитата на личните данни [12]. Практическите приложения на графовите модели включват създаване на образователни табла за наблюдение на напредъка. Те позволяват визуализация на мрежите и лесно идентифициране на проблемни зони. Това улеснява вземането на педагогически решения. Въпреки това съществуват технически ограничения, свързани с качеството и количеството на данните. Непълните данни могат да доведат до изкривени резултати. Затова е важно да се осигури надеждна система за събиране на информация. Етичните въпроси също са съществена част от проблема. Наблюдението на комуникацията между учениците трябва да бъде регулирано, за да се защити личното им пространство. Това изисква ясни правила и прозрачност. Въпреки ограниченията, потенциалът на тези технологии остава голям. С правилно прилагане те могат значително да подобрят качеството на образованието. Това ги прави важен инструмент за бъдещото развитие на учебните системи [7]. В [13] е представено изследване, демонстриращо връзката между познаването на географски обекти, информационни технологии и емоционалното изживяване на потребителя.

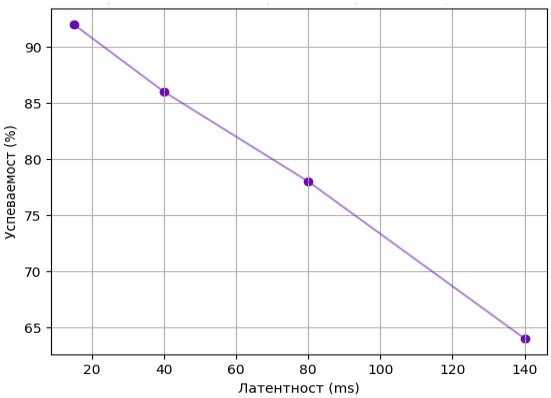
КАЗУС: Практическо приложение на комуникационна мрежа в урок по география

В училище се въвежда дигитален урок по география, при който учениците използват онлайн GIS платформа за анализ на климатични зони в Европа. Учителят

и учениците са свързани чрез комуникационна мрежа към централен сървър, който предоставя интерактивни карти и тестове. Целта е да се изследва как качеството на мрежовата връзка влияе върху ефективността на обучението при работа с географски ресурси. В таблица 3 са представени данните от казуса, а на фиг. 4 – получените резултати.

Таблица 3. Връзка между мрежови условия и учебна ефективност

Сценарий	Латентност (ms)	Packet Loss (%)	Време за задача (мин)	Успеваемост (%)
Стабилна LAN мрежа	15	0.2	6	92
Оптимална Wi-Fi връзка	40	0.8	8	86
Средно натоварена мрежа	80	1.5	11	78
Слаба интернет връзка	140	3.0	16	64



Фиг. 4: Влияние на латентността на комуникационната мрежа върху успеваемостта в обучението по география

Таблица 3 представя количествените данни за влиянието на параметрите на комуникационната мрежа върху резултатите от обучението по география. Наблюдава се тенденция за намаляване на успеваемостта и увеличаване на времето за изпълнение на задачите при повишаване на латентността и загубата на пакети. Фигура 4 визуализира зависимостта между латентността на комуникационната мрежа и успеваемостта при изпълнение на задачи по география. Тя ясно показва обратнопропорционална връзка, при която увеличаването на мрежовото забавяне води до понижаване на ефективността при работа с GIS системи и интерактивни образователни ресурси. [6]

Заключение

Използването на комуникационни мрежи и графови модели в образованието по география представлява съвременен и ефективен подход за анализ и прогнозиране на академичните резултати. Чрез структуриране на взаимодействията между участниците в учебния процес се получава по-дълбоко разбиране на факторите, влияещи върху успеха. Приложението на тези методи позволява ранна интервенция и подобряване на учебните стратегии. Въпреки съществуващите предизвикателства, потенциалът на графовия анализ в образованието остава значителен. Това го прави ценен инструмент за бъдещи изследвания и практическо внедряване. Изследването на комуникационни мрежи и графови модели в образованието по география показва значителен потенциал за подобряване на учебния процес. Чрез анализ на взаимодействията се получава по-цялостна картина на ученето. Това позволява по-точно разбиране на факторите за успех. Интегрирането на тези методи в образователната практика може да доведе до по-ефективно преподаване. Учителите получават инструменти за по-добро планиране и оценка. Това повишава качеството на образованието като цяло. Същевременно е важно да се отчита балансът между технологиите и педагогиката. Данните трябва да се използват като помощен инструмент, а не като единствен критерий. Това гарантира по-хуманен подход към обучението. В заключение, графовите модели представляват обещаваща посока за бъдещи изследвания и приложения. Те съчетават математика, информатика и педагогика в единна система. Това ги прави ценен инструмент за модерното образование.

Литература

1. Romero, C., & Ventura, S. (2010). Educational data mining: A review of the state of the art. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 40(6), 601–618.
2. Siemens, G. (2013). Learning analytics: The emergence of a discipline. American Behavioral Scientist, 57(10), 1380–1400.
3. Ferguson, R. (2012). Learning analytics: Drivers, developments and challenges. International Journal of Technology Enhanced Learning, 4(5–6), 304–317.
4. Dawson, S. (2006). A study of the relationship between student communication interaction and sense of community. The Internet and Higher Education, 9(3), 153–162.
5. Dawson, S. (2010). Seeing the learning community: An exploration of the development of a resource for monitoring online student networking. British Journal of Educational Technology, 41(5), 736–752.
6. Rabbany, R., Takaffoli, M., & Zaiane, O. R. (2014). Analyzing participation of students in online courses using social network analysis techniques. Educational Data Mining Conference Proceedings, 285–288.
7. Bruun, J., & Brewe, E. (2013). Talking and learning physics: Predicting future grades from network measures and Force Concept Inventory pretest scores. Physical Review Special Topics – Physics Education Research, 9(2), Article 020109.

8. Тодорова-Лазарова, В. П. (2026). Interactive methods and specific features of teaching higher mathematics. Управление и образование, 22(3), 71–79. Бургас: Бургаски държавен университет „Проф. д-р Асен Златаров“. ISSN 1312-6121.
9. Kalchev, K., & Tsankov, Ts. (2020). Use of the decision tree method in analysis of student data from surveys. Annual of Konstantin Preslavski University of Shumen, X E, Faculty of Technical Sciences, 72–75. ISSN 1311-834X.
10. Димитрова, Е. К., & Цанков, Ц. С. (2025). Интернет и мультимедийные технологии как педагогический ресурс в условиях цифровой трансформации образования. Сборник статей участников XVIII Международной научной конференции «Инновации в технологиях и образовании», том 1, филиал КузГТУ в г. Белово, 24 апреля 2025, с. 85–89. ISBN 978-5-00137-528-9.
11. Цанков, Ц. С., & Атанасов, В. Т. (2025). Компоненты цифровой реальности как предпосылки инновационных образовательных технологий в контексте генеративных машин. Сборник статей участников XVIII Международной научной конференции «Инновации в технологиях и образовании», том 1, филиал КузГТУ в г. Белово, 24 апреля 2025, с. 194–199. ISBN 978-5-00137-528-9.
12. Simeonova, I. (2025). How GDPR treats automated decision-making. Journal Scientific and Applied Research, 28(1). Shumen: Konstantin Preslavsky University Press. ISSN 1314-6289.
13. Mincheva, S., & Stoyanova, V. (2025). Research on the impact of the user experience for the success of a virtual product: Bulgarian travel agency websites. Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference, 2, 237–241.

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**, Faculty of Artillery, Air Defense and Communication and Information Systems

CONCEPT DRIFT IN STREAMING INFORMATION DATA IN INTELLIGENT ENERGY SYSTEMS

Milen S. Davidkov

Faculty of Technical Sciences, Department of Communication and Computer Engineering and Security Technologies, Konstantin Preslavsky University of Shumen, Shumen, Bulgaria, milen_davidkov@abv.bg

***Abstract**: The paper examines concept drift in streaming data within intelligent energy systems. Its main causes and forms are analyzed, along with its impact on the quality and reliability of information. The need for continuous data monitoring and adaptation of the applied models and criteria to changing conditions is substantiated.*

***Keywords**: Concept drift, Streaming data, Data quality, Intelligent energy systems, Adaptive data processing, Real-time monitoring*

КОНЦЕПТУАЛЕН ДРЕЙФ ПРИ ПОТОЧНИТЕ ИНФОРМАЦИОННИ ДАННИ В ИНТЕЛИГЕНТНИ ЕНЕРГИЙНИ СИСТЕМИ

Милен С. Давидков

Факултет по технически науки, катедра „Комуникационна и компютърна техника и технологии за сигурност", Шуменски университет „Епископ Константин Преславски", гр. Шумен, България, milen_davidkov@abv.bg

***Резюме**: В доклада се разглежда концептуалният дрейф при поточните данни в интелигентни енергийни системи. Анализирани са основните причини и форми на неговото проявление, както и влиянието му върху качеството и надеждността на информацията. Обоснована е необходимостта от непрекъснато наблюдение на данните и адаптиране на използваните модели и критерии към променящите се условия.*

***Ключови думи**: Концептуален дрейф, Поточни данни, Качество на данните, Интелигентни енергийни системи, Адаптивна обработка на данни, Наблюдение в реално време*

Въведение

Съвременните информационни и комуникационни системи все по-често работят с данни, които постъпват непрекъснато и отразяват текущото състояние на наблюдаваните процеси. Особено характерно е това за интелигентните енергийни системи, в които множество сензори, измервателни устройства и средства за управление генерират значителни количества поточни информационни данни.

При работата на такива системи характеристиките на наблюдаваните процеси невинаги остават постоянни. Промени в натоварването, режимите на работа, състоянието на оборудването и външните условия могат да доведат до изменение на характеристиките на постъпващите данни. В резултат използваните модели и

предварително определените критерии за тяхното оценяване могат постепенно да престанат да съответстват на действителното състояние на системата.

Подобни изменения са свързани с явлението концептуален дрейф, което има важно значение при обработването и оценяването на поточни информационни данни. То може да настъпи внезапно или постепенно и да доведе до намаляване на точността и надеждността на използваните методи. В интелигентните енергийни системи причини за подобни изменения могат да бъдат аварии, промени в конфигурацията, включване на нови енергийни източници или постепенно изменение на характеристиките на измервателните устройства.

Поради това при управлението на качеството на поточните данни е необходимо да се отчита не само наличието на отделни грешки и отклонения, но и изменението на поведението на информационния поток във времето. Своевременното установяване на подобни промени създава възможност използваните критерии и модели да бъдат приспособени към новите условия.

Целта на настоящия доклад е да бъдат разгледани същността и причините за възникване на концептуален дрейф при поточните информационни данни, основните форми на неговото проявление и влиянието му върху качеството на информацията, както и необходимостта от адаптиране на използваните методи при работа в динамично изменяща се среда.

Същност и причини за възникване на концептуален дрейф

При обработването на поточни информационни данни често се приема, че характеристиките на наблюдавания процес остават относително постоянни във времето. В реални технически и енергийни системи това условие невинаги е изпълнено. Работните режими, натоварванията, външните условия и състоянието на оборудването могат постепенно или рязко да се изменят. В резултат данните, постъпващи в информационната система, могат да започнат да се различават от тези, върху които първоначално са били определени използваните модели и правила за обработка.

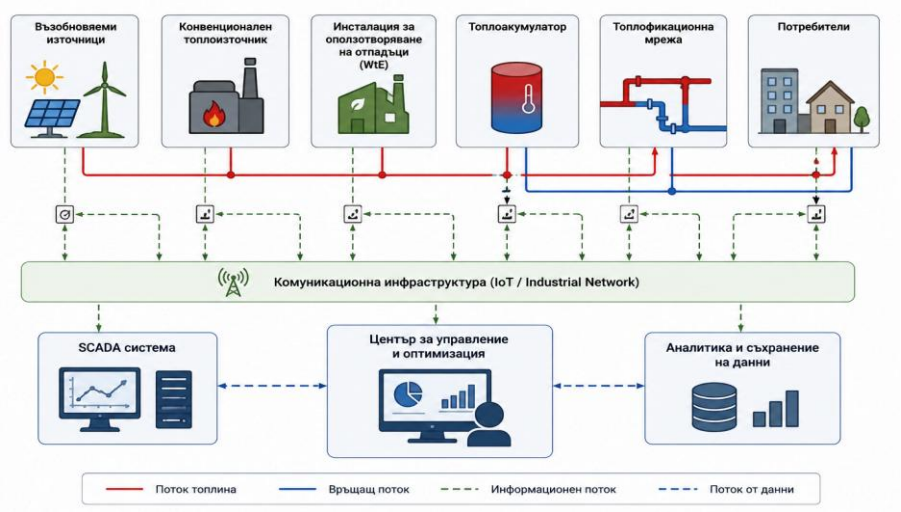
Това явление се определя като концептуален дрейф [1]. При него настъпва изменение в характеристиките на информационния поток или в зависимостите между наблюдаваните параметри. В резултат модел, който в определен момент е описвал достатъчно точно състоянието на системата, с течение на времето може да започне да дава все по-неточни оценки [3].

Концептуалният дрейф има особено значение при поточните информационни данни, тъй като те се генерират непрекъснато и отразяват текущото състояние на реалния процес [8]. Когато този процес се изменя, се изменят и статистическите характеристики на постъпващите данни. Ако системата продължи да използва непроменени предварително зададени параметри и модели, качеството на анализа постепенно може да се влоши.

Причините за възникване на концептуален дрейф могат да бъдат различни. В интелигентните енергийни системи те могат да бъдат свързани с промяна на режима на работа, въвеждане или изключване на нови енергийни източници,

изменение на потреблението, промяна на външните условия или постепенно изменение на характеристиките на измервателното оборудване.

Взаимодействието между различните енергийни източници, потребители и измервателни устройства води до формиране на множество взаимосвързани информационни потоци. Примерна структура на интегрирана интелигентна топлоенергийна система и основните информационни потоци в нея е представена на фиг. 1.



Фиг. 1. Интегрирана интелигентна топлоенергийна система и информационни потоци

Например включването на нови фотоволтаични мощности може да промени профила на натоварването в даден район. Ако използваният модел е изграден върху по-стари исторически данни, неговите прогнози постепенно могат да започнат да се различават от действителното поведение на системата. Подобен ефект може да възникне и при стареене на измервателните устройства, когато с течение на времето в измерванията започват да се появяват систематични отклонения.

Концептуален дрейф може да възникне и при по-резки изменения. Авария, повреда на оборудване, внезапно превключване на конфигурацията или прекъсване на електрозахранването могат за кратко време да променят нормалното поведение на наблюдавания процес. В този случай предварително използваните граници, зависимости или модели могат вече да не съответстват на новото състояние на системата.

Следователно концептуалният дрейф не трябва да се разглежда само като статистическо изменение на данните. При техническите системи той често

отразява реална промяна в състоянието или режима на работа на наблюдавания обект. Това налага използването на подходи, които могат не само да обработват постъпващите данни, но и да установяват настъпилите изменения и да приспособяват използваните модели към новите условия.

Основни видове концептуален дрейф при поточните информационни данни

Концептуалният дрейф може да се проявява по различен начин в зависимост от характера и скоростта на настъпващите изменения. Разграничаването на отделните видове е важно, тъй като начинът на изменение на информационния поток определя и възможностите за неговото своевременно откриване и последваща адаптация.

Внезапният дрейф се характеризира с бърза промяна на наблюдавания процес [4]. За сравнително кратък период досегашното поведение се заменя с ново и използваният до този момент модел може да престане да описва правилно постъпващите данни. В енергийните системи подобна промяна може да възникне при авария, повреда на оборудване, превключване на конфигурацията или прекъсване на електрозахранването.

При този вид дрейф съществено значение има времето за реакция. Ако промяната не бъде установена достатъчно бързо, системата може да продължи да обработва новите данни според условия, характерни за предишния режим. Това може да доведе до неправилно определяне на нормални стойности като отклонения или, обратно, до пропускане на действително възникнали проблеми.

Постепенният дрейф се развива за по-продължителен период [7]. Статистическите характеристики на информационния поток се изменят плавно, като за известно време старото и новото поведение могат да се наблюдават едновременно. Постепенно новото състояние започва да преобладава.

Характерен пример е постепенното изменение на измерванията вследствие на стареене на сензор или измервателно устройство. Първоначално отклоненията могат да бъдат малки и да останат незабелязани, но с течение на времето тяхното натрупване може да окаже съществено влияние върху качеството на получаваните данни. Подобни изменения могат да възникнат и при постепенно изменение на потреблението или на режима на работа на техническата система.

При поточните данни могат да се наблюдават и периодични или повтарящи се изменения, при които различни режими на работа се сменят в определени периоди или системата се връща към вече наблюдавано състояние. Такова поведение е характерно за процеси, зависещи от времето на денонощието, сезона, метеорологичните условия или характера на потреблението. В тези случаи връщането към вече наблюдаван режим не трябва непременно да се приема като възникване на грешка.

От практическа гледна точка отделните видове дрейф могат да се различават значително по продължителност и интензивност. Рязката промяна обикновено се открива по-лесно, тъй като води до ясно изменение на наблюдаваните стойности.

Постепенната промяна е по-трудна за установяване, защото всяко отделно изменение може да бъде малко и да остава в допустимите граници.

Поради това определянето на вида на концептуалния дрейф има пряко значение за избора на подход за неговото откриване. Необходимо е да се отчита не само текущата стойност на наблюдавания параметър, но и изменението на характеристиките на информационния поток във времето. По този начин могат да бъдат разграничени единичните случайни отклонения от по-трайна промяна в поведението на наблюдавания процес. За обобщаване на разгледаните форми на концептуален дрейф и техните характерни проявления при поточните информационни данни основните им особености са систематизирани в табл. 1.

Табл. 1. Сравнителна характеристика на основните видове концептуален дрейф

Вид концептуален дрейф	**Характер на изменението**	**Типична причина в енергийна система**	**Особености при откриване**
Внезапен	Рязка промяна за кратък период	Авария, повреда, превключване на конфигурацията	Относително лесно откриване поради ясно изразената промяна
Постепенен	Плавно изменение за продължителен период	Стареене на сензори, изменение на натоварването	По-трудно откриване поради малките последователни изменения
Периодичен	Изменения, свързани с определени периоди	Денонощни, сезонни или метеорологични изменения	Необходимо е разграничаване между нормална периодичност и аномалия
Повтарящ се	Връщане към вече наблюдаван режим	Повторно възникване на характерен работен режим	Необходимо е разпознаване на вече известни състояния

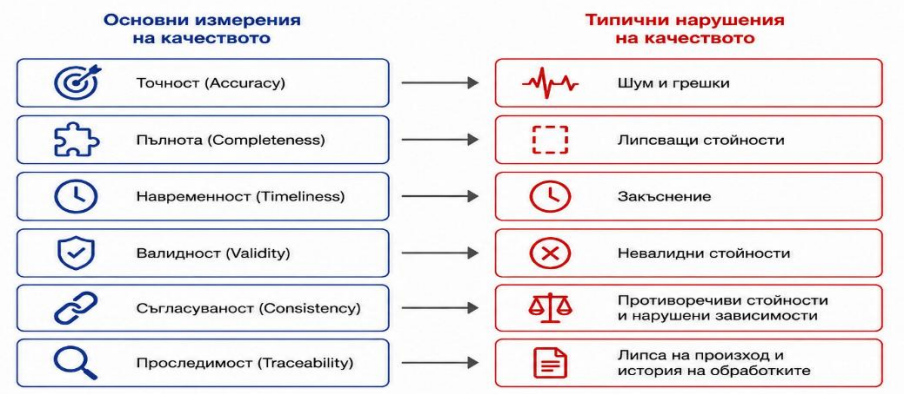
Влияние на концептуалния дрейф върху качеството на данните и необходимост от адаптация

Появата на концептуален дрейф оказва пряко влияние върху надеждността на обработката на поточните информационни данни. Основният проблем е, че използваните методи и модели обикновено са изградени въз основа на определени характеристики на наблюдавания процес. Когато тези характеристики се променят, предварително определените зависимости и критерии постепенно могат да престанат да отговарят на действителното състояние на системата.

В резултат е възможно данни, които съответстват на новия нормален режим на работа, да бъдат определени като отклоняващи се. Възможна е и обратната ситуация – действително възникнали отклонения да останат неразпознати, ако използваният модел вече не описва достатъчно точно текущото поведение на процеса. Това е особено важно при системи, в които получената информация се използва непосредствено за наблюдение, прогнозиране или управление.

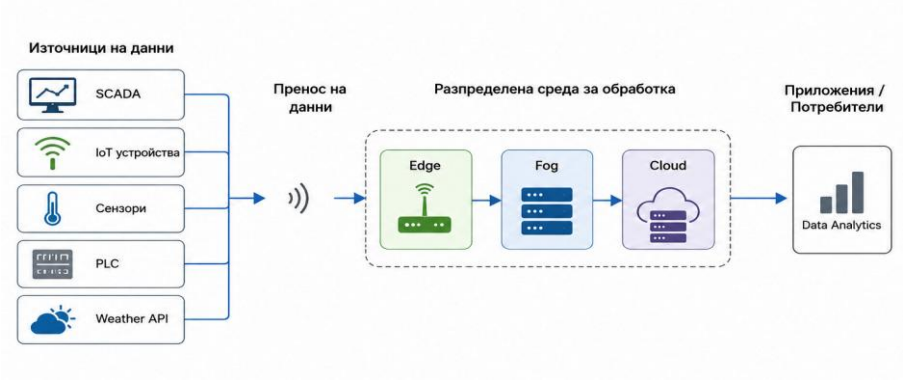
Влиянието на концептуалния дрейф може да се прояви в различни характеристики на качеството на поточните информационни данни. Промените в

поведението на наблюдавания процес могат да доведат до отклонения в точността, пълнотата, навременността и съгласуваността на постъпващата информация [13], [14]. Основните измерения на качеството и характерните нарушения при поточните данни са представени на фиг. 2.



Фиг. 2. Основни измерения и типични нарушения на качеството на поточните данни

При интелигентните енергийни системи проблемът се усложнява от големия брой източници на информация [10]. Сензори, интелигентни електромери и други измервателни устройства непрекъснато генерират поточни данни, които се предават през комуникационната инфраструктура към системите за обработка и управление [11], [15]. Промяната в характеристиките дори на част от тези източници може да повлияе върху общата оценка за състоянието на наблюдавания процес. Обобщена схема на постъпването на данни от различни източници и предаването им към разпределена среда за обработка е представена на фиг. 3.



Фиг. 3. Поток от данни от разнородни източници към разпределена среда за обработка

Използването само на предварително зададени постоянни граници и критерии не винаги е достатъчно при подобна динамична среда. Те могат да бъдат подходящи при относително стабилен режим, но при изменение на характеристиките на потока тяхната ефективност намалява. Направеният анализ показва, че класическите статистически методи са удобни за първичен контрол поради сравнително ниската си изчислителна сложност, но по-трудно установяват постепенно възникващи изменения, характерни за концептуалния дрейф. В [17] е представаена една гледна точка на проблемите с информационна сигурност на данните в мобилните устройства.

Поради това е необходимо наблюдението на качеството да се извършва непрекъснато [2]. Освен проверка на отделните постъпващи стойности трябва да се следи изменението на характеристиките на информационния поток за определен период. Устойчивата промяна на средните стойности, разсейването, честотата на отклоненията или други наблюдавани показатели може да бъде признак, че системата преминава към различен режим на работа [9].

След установяване на такава промяна е необходимо използваните критерии и модели да могат да бъдат приспособени към новите условия [5]. Адаптацията може да включва актуализиране на допустими граници, промяна на параметри, използване на по-нови наблюдения или повторно настройване на използвания модел [6]. Целта е системата да продължи да оценява правилно постъпващата информация, без всяко изменение на работния режим да бъде приемано автоматично като грешка.

Това определя необходимостта от адаптивно управление на качеството на поточните информационни данни [16]. При него оценяването на качеството, откриването на измененията и приспособяването към тях се разглеждат като свързани процеси. Тази необходимост е изведена като основание за модел, който обединява непрекъснат мониторинг, количествено оценяване на показателите за

качество, автоматично откриване на концептуален дрейф и адаптация към изменящите се условия.

По този начин отчитането на концептуалния дрейф позволява управлението на качеството да не се основава единствено на предварително зададени и неизменни критерии. Системата трябва да отчита динамиката на наблюдавания процес и своевременно да приспособява начина, по който постъпващите данни се оценяват и използват. Това е особено важно при интелигентните енергийни системи, където работните режими и информационните потоци могат да се изменят непрекъснато [12].

Заключение

Концептуалният дрейф е характерно явление при обработването на поточни информационни данни в динамично изменящи се системи. Той възниква при промяна в характеристиките на наблюдавания процес и може да доведе до несъответствие между текущо постъпващите данни и използваните модели и критерии за тяхното оценяване.

Разгледаните видове концептуален дрейф показват, че измененията могат да настъпват както рязко, така и постепенно. Особено затруднение представляват плавните изменения, тъй като те могат да останат незабелязани за по-продължителен период и постепенно да влошат надеждността на получаваните резултати. В интелигентните енергийни системи подобни изменения могат да бъдат предизвикани от промени в натоварването, режимите на работа, състоянието на оборудването и включването на нови енергийни източници.

Установено е, че използването единствено на постоянни предварително зададени критерии не е достатъчно при непрекъснато изменящи се информационни потоци. Необходимо е да се следят не само отделните постъпващи стойности, но и изменението на характеристиките на данните във времето. Това позволява да се разграничат случайните отклонения от трайните промени в поведението на наблюдавания процес.

Поради това управлението на качеството на поточните информационни данни трябва да включва възможности за своевременно откриване на концептуален дрейф и адаптиране на използваните критерии и модели. Съчетаването на непрекъснато наблюдение, оценяване на качеството и адаптация към настъпващите изменения създава условия за по-надеждно използване на поточната информация при анализа и управлението на интелигентни енергийни системи. Тази необходимост е изведена и като основа за последващото разработване на адаптивен модел в дисертационния труд.

Литература

1. Gama, J., Žliobaitė, I., Bifet, A., Pechenizkiy, M., & Bouchachia, A. (2014). A survey on concept drift adaptation. ACM Computing Surveys, 46(4), Article 44, 1–37. https://doi.org/10.1145/2523813

2. Bifet, A., & Gavaldà, R. (2007). Learning from time-changing data with adaptive windowing. Proceedings of the 2007 SIAM International Conference on Data Mining, 443–448. https://doi.org/10.1137/1.9781611972771.42
3. Lu, J., Liu, A., Dong, F., Gu, F., Gama, J., & Zhang, G. (2019). Learning under concept drift: A review. IEEE Transactions on Knowledge and Data Engineering, 31(12), 2346–2363. https://doi.org/10.1109/TKDE.2018.2876857
4. Widmer, G., & Kubat, M. (1996). Learning in the presence of concept drift and hidden contexts. Machine Learning, 23, 69–101.
5. Bifet, A., Holmes, G., Kirkby, R., & Pfahringer, B. (2010). MOA: Massive Online Analysis. Journal of Machine Learning Research, 11, 1601–1604.
6. Bifet, A., Holmes, G., & Pfahringer, B. (2010). Leveraging bagging for evolving data streams. In Machine Learning and Knowledge Discovery in Databases, Lecture Notes in Computer Science, 6321 (pp. 135–150). Springer.
7. Ditzler, G., Roveri, M., Alippi, C., & Polikar, R. (2015). Learning in nonstationary environments: A survey. IEEE Computational Intelligence Magazine, 10(4), 12–25. https://doi.org/10.1109/MCI.2015.2471196
8. Žliobaitė, I. (2010). Learning under concept drift: An overview.
9. Wang, H., & Abraham, Z. (2015). Concept drift detection for streaming data. Proceedings of the International Joint Conference on Neural Networks (IJCNN), 1–9. https://doi.org/10.1109/IJCNN.2015.7280398
10. Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Smart grid – The new and improved power grid: A survey. IEEE Communications Surveys & Tutorials, 14(4), 944–980. https://doi.org/10.1109/SURV.2011.101911.00087
11. Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: Communication technologies and standards. IEEE Transactions on Industrial Informatics, 7(4), 529–539.
12. Gopstein, A., Nguyen, C., O'Fallon, C., Hastings, N., & Wollman, D. A. (2021). NIST framework and roadmap for smart grid interoperability standards, Release 4.0. NIST Special Publication 1108r4. National Institute of Standards and Technology.
13. Denev, D., & Tsankov, Ts. (2022). A survey of data quality and processing of information in innovative smart devices. Proceedings of the International Conference Automatics and Informatics (ICAI 2022), 1–4.
14. Denev, D., & Tsankov, Ts. (2022). A survey of data quality in digital processing of acoustic signals. Proceedings of the International Conference on Communications, Information, Electronic and Energy Systems (CIEES), 1–4.
15. Denev, D., & Tsankov, Ts. (2022). Design and implementation of a field level of an industrial communication network for the needs of the industry. Proceedings of the 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST 2022), 1–4.
16. Denev, D., & Nikolova, S. (2025). A novel algorithm for industrial network reliability estimation and AI-based system optimization. Proceedings of the XXXIII National Conference with International Participation TELECOM, 1–4.

17. Stoyanova, V. (2019). Problems with information security on mobile devices. Industry 4.0, 4(4), 200-202.

ASSESSMENT AND IMPROVEMENT OF STREAMING INFORMATION DATA QUALITY MILEN S. DAVIDKOV[1], TSVETOSLAV S. TSANKOV[2]

Faculty of Technical Sciences, Department of Communication and Computer Engineering and Security Technologies, Konstantin Preslavsky University of Shumen, Shumen, Bulgaria,
[1]milen_davidkov@abv.bg, [2]c.cankov@shu.bg

***Abstract**: The paper examines the main characteristics and indicators related to the quality of streaming information data. Approaches for assessing the accuracy, completeness, timeliness, validity, and consistency of incoming information are presented. Methods for detecting missing, invalid, and anomalous values, as well as the use of time windows in data stream processing, are considered. Basic approaches for improving data quality through filtering, recovery of missing values, and smoothing of random fluctuations are discussed. The application of these approaches provides a basis for more reliable use of streaming data in subsequent analysis, control, and decision-making.*

***Keywords**: Data streams, Data quality, Data processing*

ОЦЕНЯВАНЕ И ПОВИШАВАНЕ НА КАЧЕСТВОТО НА ПОТОЧНИТЕ ИНФОРМАЦИОННИ ДАННИ

Милен С. Давидков[1], Цветослав С. Цанков[2]

Факултет по технически науки, катедра „Комуникационна и компютърна техника и технологии за сигурност", Шуменски университет „Епископ Константин Преславски", гр. Шумен, България, [1]milen_davidkov@abv.bg, [2]c.cankov@shu.bg

***Резюме**: В доклада са разгледани основни характеристики и показатели за качеството на поточните информационни данни. Представени са подходи за оценяване на точността, пълнотата, навременността, валидността и съгласуваността на постъпващата информация. Разгледани са методи за установяване на липсващи, недопустими и отклоняващи се стойности, както и използването на времеви прозорци при обработката на информационни потоци. Представени са основни възможности за повишаване на качеството чрез филтриране, възстановяване на липсващи данни и изглаждане на случайни изменения. Прилагането на тези подходи създава условия за по-надеждно използване на поточните данни при последващ анализ, управление и вземане на решения.*

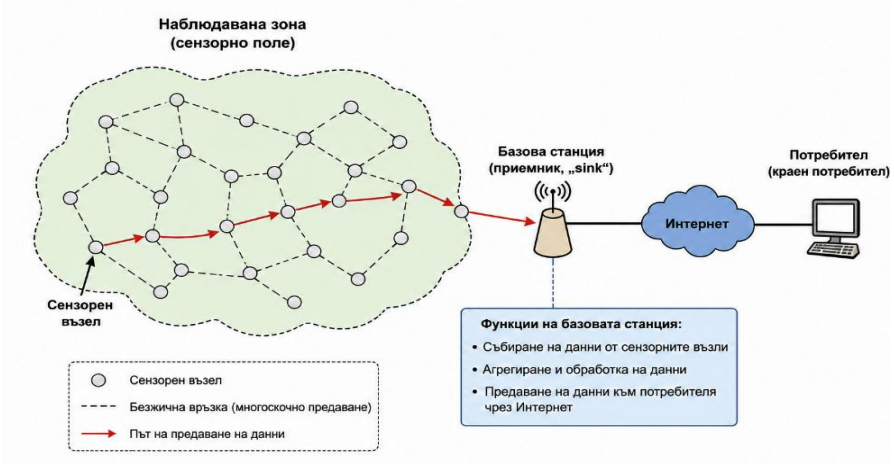
***Ключови думи**: Потоци от данни, Качество на данните, Обработка на данни*

Въведение

Съвременните информационни и комуникационни системи работят с непрекъснато постъпващи данни от различни източници. Такива данни се формират при работата на сензорни мрежи, комуникационни устройства, системи за наблюдение и различни автоматизирани технически средства [9, 14]. В много случаи получената информация трябва да бъде обработена непосредствено след

нейното постъпване, което поставя определени изисквания към нейната точност, пълнота и надеждност.

При предаването и обработката на поточни информационни данни могат да възникнат различни отклонения. Те могат да бъдат свързани с липсващи стойности, грешки при измерването, прекъсване на комуникацията или поява на стойности, които значително се различават от останалите. Подобни проблеми могат да окажат влияние върху последващия анализ и върху решенията, които се вземат въз основа на получената информация (фиг. 1). Когато поточните данни се използват при автоматизирано вземане на решения, следва да се осигурят прозрачност на обработката, защита на личните данни и възможност за човешка намеса [13].



Фиг. 1: Примерна структура на безжична сензорна мрежа и предаване на поточни информационни данни

Поради това е необходимо качеството на постъпващите данни да бъде оценявано още в процеса на тяхното получаване и обработване. Целта на настоящия доклад е да бъдат разгледани основни подходи за установяване на отклонения и грешки в поточните информационни данни, както и някои практически методи за тяхното филтриране, коригиране и повишаване на качеството.

Основни характеристики и показатели за качество на поточните информационни данни

Качеството на поточните информационни данни има съществено значение за работата на съвременните интелигентни системи. За разлика от традиционните информационни масиви, поточните данни постъпват непрекъснато и се използват

непосредствено при наблюдението, анализа и управлението на технологичните процеси [2]. Поради това тяхното качество трябва да бъде оценявано още в процеса на постъпване и обработване, а не само след натрупването им в информационната система. В [15] е представена една гледна точка на проблемите с информационна сигурност на данните в мобилните устройства.

Особеност на поточните данни е тяхната силна зависимост от времето [11]. Една измерена стойност може да бъде правилна, но ако постъпи със значително закъснение, тя вече да не отразява текущото състояние на наблюдавания процес. По тази причина при оценяване на качеството трябва да се отчита не само числовата стойност, но и моментът на възникване на събитието, времето на приемане, произходът на информацията и техническото състояние на нейния източник. Поточният запис именно поради това се разглежда като информационен обект, съдържащ стойност и допълнителен контекст.

Качеството на поточните информационни данни може да бъде разглеждано чрез няколко взаимно свързани показателя. Сред основните са точност, пълнота, навременност, валидност, съгласуваност, уникалност и проследимост [1]. Тези показатели позволяват да се установи доколко постъпващата информация е подходяща за последваща обработка и използване при вземане на управленски решения. Същите характеристики са заложени и в жизнения цикъл на данните.

Точността характеризира степента, в която получената стойност съответства на действителното състояние на наблюдавания обект или процес. Върху нея могат да влияят измервателният шум, грешки при калибриране, техническото състояние на датчиците и извършените преобразувания на данните.

Пълнотата показва дали всички необходими данни са налични. При поточната обработка липсващите записи могат да нарушат последователността на наблюдавания процес и да затруднят правилното определяне на неговото текущо състояние [8].

Навременността определя дали информацията постъпва в рамките на времето, в което тя все още може да бъде използвана за съответната задача [11]. Този показател е особено важен при системите за управление в реално време, където закъснението може да промени практическата стойност на получената информация. Допустимото закъснение зависи от конкретното приложение – една и съща стойност може да бъде достатъчно навременна за отчетна задача, но неприемлива за защитна функция.

Валидността характеризира съответствието на данните с предварително определени правила, формати и допустими диапазони. Проверката може да включва типа на данните, наличието на задължителни полета, идентификатора на източника, времевия маркер и допустимите граници на измерваната величина.

Съгласуваността показва дали отделните данни не си противоречат и дали съответстват на известните зависимости между наблюдаваните параметри. Това е особено важно в техническите и енергийните системи, където отделните величини често са свързани чрез физически или технологични зависимости.

Уникалността е свързана с откриването на повторно постъпили или дублирани записи [6]. Дублирането може да възникне при комуникационни прекъсвания,

повторно предаване на съобщения или неправилна работа на отделни компоненти на системата.

Проследимостта позволява да бъде установен произходът на информационния запис и извършените върху него обработки. Това означава да бъде запазена информация дали стойността е първично измерена, филтрирана, коригирана, възстановена или прогнозирана. В поточните системи метаданните дават възможност да бъде проследен жизненият цикъл на конкретния запис и обработките, през които той е преминал.

Разглеждането на тези показатели поотделно не е достатъчно за получаване на цялостна оценка [7]. Един запис например може да бъде точен и валиден, но да е получен твърде късно. Друг може да бъде навременен, но да произхожда от устройство с установено техническо нарушение. Поради това качеството на поточните информационни данни следва да се определя чрез съвместното оценяване на няколко характеристики, като се отчита и конкретното предназначение на информацията.

Особено важно е, че различните информационни потоци нямат еднаква критичност. Данните могат да се използват за аварийна защита, оперативно регулиране, оптимизация, прогнозиране, диагностика, техническа поддръжка или архивиране. Следователно едно и също нарушение може да има различно значение в зависимост от предназначението на конкретния поток.

По този начин качеството на поточните информационни данни представлява комплексна характеристика, която не може да бъде сведена единствено до точността на измерената стойност. То трябва да отчита както самите данни, така и тяхната времева актуалност, произход, съгласуваност и пригодност за конкретната задача. Това създава необходимост от използването на подходящи методи за оценяване на качеството в реално време, които ще бъдат разгледани в следващата част на доклада.

Методи за оценяване на качеството на поточните информационни данни

Оценяването на качеството на поточните информационни данни е важна част от тяхната обработка, тъй като получаваната информация постъпва непрекъснато и трябва да бъде анализирана в момента на нейното получаване. За разлика от данните, които се съхраняват предварително и могат да бъдат проверявани многократно, при информационните потоци времето за извършване на проверка е ограничено. Поради тази причина използваните методи трябва да позволяват бързо установяване на липсващи, неточни или необичайни стойности.

Един от основните подходи е извършването на проверка за допустимост на постъпващите стойности. При този метод за отделните параметри предварително се определят допустими граници. Всяка новопостъпила стойност се сравнява с тях и при излизане извън зададения диапазон се отчита възможно отклонение. Този подход е сравнително лесен за прилагане и е подходящ за системи, при които са известни нормалните работни граници на наблюдаваните параметри.

Например, ако от даден измервателен елемент се получава последователност от стойности $x_1, x_2, \ldots, x_n$, за всяка стойност може да бъде извършена проверка:

$$x_{min} \leq x_i \leq x_{max},$$

където x_{min} и x_{max} са предварително зададените минимална и максимална допустима стойност. Когато условието не е изпълнено, получената стойност може да бъде отбелязана за допълнителна проверка.

Друг показател е пълнотата на информационния поток. При непрекъснатото предаване на информация е възможно част от данните да не достигнат до системата поради прекъсване на комуникацията, техническа неизправност или други смущения [12]. Пълнотата може да бъде оценена чрез отношението между броя на действително получените и очакваните данни за определен период:

$$K_p = \frac{N_p}{N_o},$$

където Np е броят на получените стойности, а No – броят на очакваните стойности. При стойност на Kp, близка до 1, информационният поток може да се приеме за достатъчно пълен. Намаляването на този коефициент показва наличие на липсващи данни.

При поточните данни значение има и последователността на получаваната информация. Рязката промяна между две съседни стойности невинаги означава реална промяна на наблюдавания процес [10]. Тя може да бъде резултат от грешка при измерване, предаване или обработване на данните. Един сравнително прост начин за установяване на подобни случаи е проследяването на разликата между последователни стойности [3]:

$$\Delta x_i = |x_i - x_{i-1}|$$

Когато тази разлика надвиши предварително определена допустима стойност, съответният елемент от потока може да бъде разглеждан като възможно отклонение.

Освен отделните стойности може да се наблюдава и поведението на данните за определен времеви интервал [4]. За тази цел потокът се разделя на последователни времеви прозорци, в рамките на които се определят характерни показатели – средна стойност, минимална и максимална стойност, брой получени данни и наличие на отклонения. По този начин не е необходимо да се съхранява и анализира целият информационен поток, а се обработва ограничена част от него [2].

Например средната стойност за прозорец, съдържащ n наблюдения, може да бъде определена чрез:

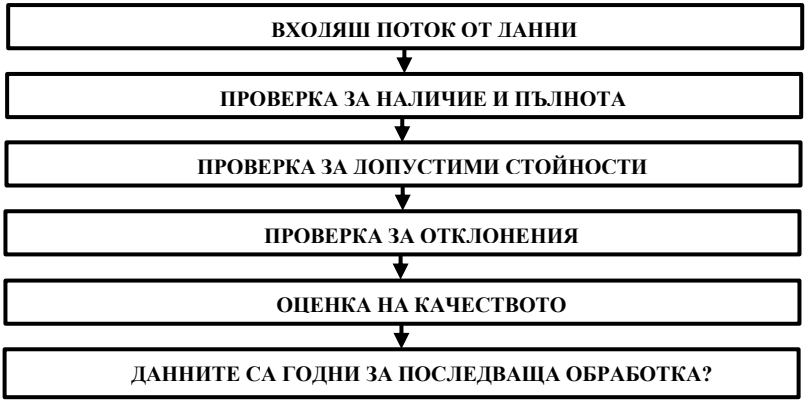
$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i.$$

Сравняването на получените средни стойности за последователни времеви прозорци позволява да се проследяват измененията в поведението на информационния поток и да се установяват по-трайни отклонения.

При практическото оценяване на качеството обикновено не е достатъчно използването само на един показател. Една стойност например може да се намира в

допустимите граници, но да е получена със значително закъснение или да е част от поток с голям брой липсващи данни. Поради това е целесъобразно качеството да се определя чрез съвместно разглеждане на няколко показателя, характеризиращи различни свойства на постъпващата информация.

Така оценяването може да се извършва последователно – първо се проверява дали данните са получени, след това дали попадат в допустимите граници и накрая дали тяхното изменение съответства на нормалното поведение на наблюдавания процес. Получената оценка може да се използва при последващата обработка на информационния поток и при вземането на решение дали конкретните данни могат да бъдат използвани непосредствено или трябва да бъдат подложени на допълнителна проверка. Основните етапи при оценяването на качеството на поточните информационни данни могат да бъдат представени обобщено чрез последователна проверка на постъпващата информация (фиг. 2) [2].



Фиг. 2: Основни етапи при оценяване на качеството на поточните информационни данни

Обработка и повишаване на качеството на поточните информационни данни

Установяването на отклонения и грешки в информационния поток е само първият етап от работата с данните. След извършване на оценката е необходимо да се предприемат действия за ограничаване на влиянието на неточните, липсващите или несъответстващите стойности. Целта е към следващите етапи на обработка да бъдат предадени данни с достатъчно качество и надеждност.

Един от най-простите подходи е филтрирането на недопустими стойности. Когато дадена стойност излиза извън предварително определените граници, тя може да бъде отхвърлена или обозначена като съмнителна. Изборът между тези два подхода зависи от характера на наблюдавания процес. Не всяка необичайна

стойност представлява грешка, тъй като тя може да показва действително настъпила промяна в състоянието на системата [10].

Друг често срещан проблем е наличието на липсващи данни. При поточната обработка липсата на отделни стойности може да бъде резултат от прекъсване на връзката, загуба при предаването или неизправност на източника. Когато броят на липсващите стойности е малък, те могат да бъдат приблизително възстановени въз основа на съседните данни [8].

При две известни стойности x_{i-1} и x_{i+1} една проста оценка на липсващата стойност може да бъде:

$$x_i = \frac{x_{i-1} + x_{i+1}}{2}$$

Този начин е приложим при сравнително плавно изменение на наблюдавания параметър. При процеси с резки изменения подобно заместване трябва да се използва внимателно, тъй като може да доведе до изкривяване на действителното състояние.

За ограничаване на влиянието на случайните колебания може да се използва и изглаждане на данните. Един от лесно приложимите методи е плъзгащата средна стойност [5]. При нея всяка нова оценка се формира от определен брой последователни стойности:

$$\bar{x_i} = \frac{1}{m}\sum_{j=0}^{m-1} x_{i-j},$$

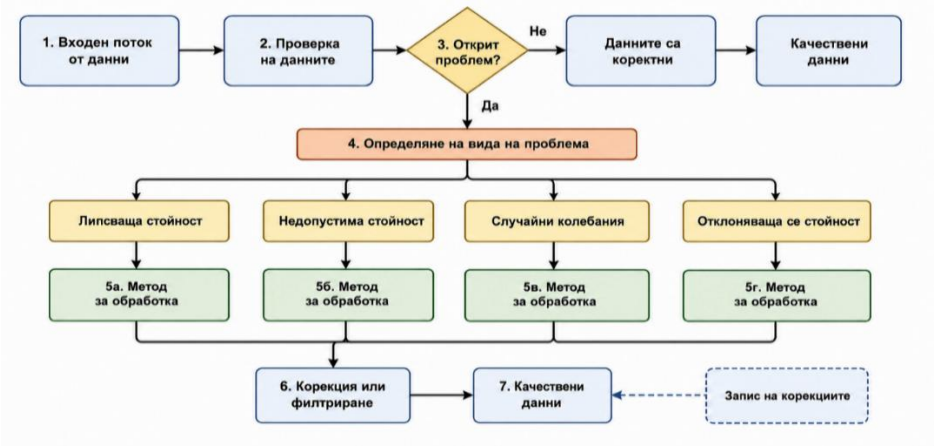
където m е броят на стойностите, включени в разглеждания прозорец.

По този начин влиянието на единичните случайни изменения се намалява и по-ясно се проследява общата тенденция в информационния поток. Увеличаването на размера на прозореца води до по-силно изглаждане, но едновременно с това може да забави отчитането на реално настъпили промени [5].

Особено значение има и обработката на отклоняващите се стойности [3]. При установяване на значително отклонение системата трябва да определи дали стойността да бъде запазена, коригирана или изключена от последващата обработка. Автоматичното премахване на всяка необичайна стойност не винаги е подходящо, защото по този начин може да бъде загубена информация за реално възникнало събитие.

Затова при поточните информационни данни е целесъобразно да се запазва информация и за извършените корекции. Това позволява да се различават първоначално получените данни от стойностите, които са били променени в процеса на обработка.

Процесът на повишаване на качеството може условно да бъде представен чрез последователността: входни данни → проверка → откриване на проблем → избор на метод за обработка → корекция или филтриране → качествени данни (фиг. 3) [3].



Фиг. 3: Основни действия при обработка и повишаване на качеството на поточните информационни данни

По този начин оценяването на качеството и обработката на данните представляват свързани процеси. Оценяването показва наличието на проблем в информационния поток, а последващата обработка има за задача да ограничи неговото влияние. Това създава основа за по-надеждно използване на поточните данни при анализ, управление и вземане на решения.

Заключение

Качеството на поточните информационни данни има важно значение за надеждната работа на съвременните информационни и комуникационни системи. Наличието на липсващи, неточни или отклоняващи се стойности може да затрудни обработката на информацията и да доведе до неправилна оценка на наблюдавания процес.

Разгледаните подходи показват, че установяването на проблеми в информационния поток трябва да бъде свързано с последваща обработка на откритите отклонения. Използването на проверки за допустими граници, анализ на последователни стойности, възстановяване на липсващи данни, филтриране и изглаждане позволява да се ограничи влиянието на случайните грешки и смущения.

При избора на конкретен метод трябва да се отчита характерът на наблюдавания процес, тъй като необичайната стойност невинаги представлява грешка, а може да показва действително настъпила промяна. Поради това обработката на поточните данни трябва да осигурява баланс между отстраняването на неточната информация и запазването на данните, които носят информация за реални събития. По този начин се създават условия за по-надежден последващ анализ и използване на получената информация.

Литература

1. Muthukrishnan, S. (2005). Data streams: Algorithms and applications. Foundations and Trends in Theoretical Computer Science, 1(2), 117–236.
2. Babcock, B., Babu, S., Datar, M., Motwani, R., & Widom, J. (2002). Models and issues in data stream systems. Proceedings of the 21st ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS), 1–16.
3. Aggarwal, C. C. (Ed.). (2007). Data streams: Models and algorithms. New York: Springer.
4. Garofalakis, M., Gehrke, J., & Rastogi, R. (Eds.). (2016). Data stream management: Processing high-speed data streams. Berlin, Heidelberg: Springer-Verlag. ISBN 978-3-540-28608-0.
5. Datar, M., Gionis, A., Indyk, P., & Motwani, R. (2002). Maintaining stream statistics over sliding windows. SIAM Journal on Computing, 31(6), 1794–1813. https://doi.org/10.1137/S0097539701398363
6. Cormode, G., & Muthukrishnan, S. (2005). An improved data stream summary: The Count-Min Sketch and its applications. Journal of Algorithms, 55(1), 58–75.
7. Leskovec, J., Rajaraman, A., & Ullman, J. D. (2020). Mining of massive datasets (3rd ed.). Cambridge: Cambridge University Press.
8. Gama, J. (2010). Knowledge discovery from data streams. Boca Raton: Chapman & Hall/CRC.
9. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. Computer Networks, 38(4), 393–422. https://doi.org/10.1016/S1389-1286(01)00302-4
10. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), Article 15.
11. Stonebraker, M., Çetintemel, U., & Zdonik, S. (2005). The 8 requirements of real-time stream processing. ACM SIGMOD Record, 34(4), 42–47.
12. Arasu, A., Babcock, B., Babu, S., Cieslewicz, J., Datar, M., Ito, K., Motwani, R., Srivastava, U., & Widom, J. (2016). STREAM: The Stanford data stream management system. In M. Garofalakis, J. Gehrke, & R. Rastogi (Eds.), Data stream management: Processing high-speed data streams. Berlin, Heidelberg: Springer.
13. Simeonova, I. (2025). How GDPR treats automated decision-making. Journal Scientific and Applied Research, 28(1), 164–175. Shumen: Konstantin Preslavsky University Press. ISSN 1314-6289.
14. Stefanova, A. (2025). Geodesy 4.0: Geodesy transformation via new technologies. Proceedings of International Scientific Conference on Architecture and Civil Engineering ArCivE 2025, Vol. 5–2025, 311–317. ISSN 2535-0781.
15. Stoyanova, V. (2019). Problems with information security on mobile devices. Industry 4.0, 4(4), 200-202.

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

HYBRID APPROACH TO NETWORK TRAFFIC ANOMALY DETECTION USING WIRESHARK, CISCO PACKET TRACER AND IDS

Dimitar R. Iliev[1], Ekaterina M. Hristova[2]

Faculty of Technical Sciences, Department of Communication and Computer Engineering and Security Technologies, Konstantin Preslavsky University of Shumen, Shumen, Bulgaria, [1]dimitar25_8000@abv.bg, [2]ekaterinamkonstantinova@gmail.com

***Abstract**: A hybrid approach to network traffic anomaly detection is presented, combining packet analysis with Wireshark, simulation-based verification of network configurations with Cisco Packet Tracer, and intrusion detection system logic. The roles of NIDS and HIDS and the strengths and limitations of signature-based and anomaly-based detection are systematized. A combined indicator is proposed, incorporating signature matching, timing deviation, packet intensity, failed TCP sessions and changes in address mappings. The approach is applied to illustrative HTTP, DNS, TCP SYN, Z-Wave and Zigbee traffic data. A sequential process for simulation, capture, assessment and retesting of protective measures is developed.*

***Keywords**: Network traffic, Wireshark, Cisco Packet Tracer, IDS, Anomaly detection*

ХИБРИДЕН ПОДХОД ЗА ОТКРИВАНЕ НА АНОМАЛИИ В МРЕЖОВИЯ ТРАФИК ЧРЕЗ WIRESHARK, CISCO PACKET TRACER И IDS

Димитър Р. Илиев[1], Екатерина М. Христова[2]

Факултет по технически науки, катедра „Комуникационна и компютърна техника и технологии за сигурност“, Шуменски университет „Епископ Константин Преславски“, гр. Шумен, България, [1]dimitar25_8000@abv.bg, [2]ekaterinamkonstantinova@gmail.com

***Резюме**: Представен е хибриден подход за откриване на аномалии в мрежовия трафик, който обединява пакетен анализ с Wireshark, симулационна проверка на мрежовата конфигурация с Cisco Packet Tracer и логиката на системите за откриване на проникванията. Систематизирани са ролите на NIDS и HIDS, както и предимствата и ограниченията на сигнатурния и аномалийния анализ. Предложен е комбиниран показател, включващ сигнатурно съвпадение, отклонение на времевите характеристики, интензивност на пакетите, неуспешни TCP сесии и промени в адресните съответствия. Подходът е приложен към илюстративни данни за HTTP, DNS, TCP SYN, Z-Wave и Zigbee трафик. Разработен е последователен процес за симулация, улавяне, оценяване и повторно тестване на защитните мерки.*

***Ключови думи**: Мрежов трафик, Wireshark, Cisco Packet Tracer, IDS, Откриване на аномалии*

Въведение

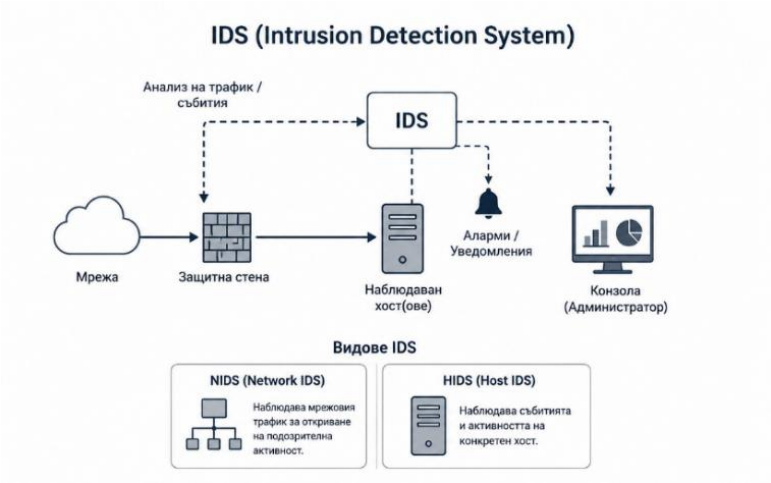
Наблюдението на мрежовия трафик е основен източник на информация за работоспособността и сигурността на комуникационните системи. Нарушенията

могат да се проявят като необичаен брой пакети, промяна на използваните протоколи, многократни неуспешни връзки, несъответствие между IP и MAC адреси или нетипично време за отговор. Самостоятелният преглед на пакетите предоставя подробна информация, но при голям обем от данни е необходимо автоматизирано наблюдение и оценяване на мрежовата активност [5].

Wireshark позволява детайлно улавяне и филтриране на реален трафик, а Cisco Packet Tracer предоставя контролирана среда за изграждане на топологии и проверка на VLAN, ACL и други защитни настройки [1, 2]. Системата за откриване на проникванията (IDS) допълва двата инструмента чрез правила за автоматизирано откриване на подозрителна активност и генериране на предупреждения. Целта на доклада е да предложи обща методика, която свързва тези три функции и може да се използва при анализ, обучение и предварително тестване на защити.

Системи за откриване на проникванията

Системата за откриване на проникванията наблюдава събитията в мрежата или в крайното устройство и открива признаци за нарушения на политиката за сигурност. NIDS анализира пакети и потоци в реално време от стратегически точки в мрежата и може едновременно да наблюдава множество устройства [6]. HIDS работи върху конкретен компютър или сървър и използва системни журнали, файлови промени, процеси и локални събития [3]. Двата типа са допълващи се: NIDS има широка видимост, докато HIDS вижда последствията вътре в системата.



Фиг. 1: Основни компоненти и разположение на IDS система

Сигнатурен и аномалиен анализ

Сигнатурният анализ сравнява наблюдаваните пакети и събития с предварително дефинирани правила и известни шаблони, като този подход е реализиран и в системи за откриване на проникванията като Snort [7]. Той осигурява висока точност при разпознаването на известни атаки и обикновено генерира по-малко фалшиви положителни резултати, но не може да открива нови техники за атака, преди за тях да бъде създадено съответно правило. Аномалийният анализ изгражда профил на нормалното поведение и регистрира съществени отклонения. Така могат да бъдат открити непознати атаки, но промени в легитимното натоварване също могат да задействат предупреждение.

Таблица 1: Сравнение на подходите за откриване

Метод	Силна страна	Ограничение	Подходящи данни
Сигнатурен	точно разпознаване на известни модели	зависимост от актуални правила	полета на пакети, последователности
Аномалиен	открива непознати отклонения	фалшиви аларми при нов нормален режим	интензивност, времена, разпределения
Хибриден	съчетава обяснимост и адаптивност	изисква настройване и валидиране	пакети, потоци, журнали и контекст

Хибридният подход първо проверява еднозначните сигнатури, а след това оценява отклоненията на останалия трафик. Това позволява известните инциденти да се обработват бързо, а съмнителните, но неизвестни модели да се насочват към допълнителен анализ.

Пакетен анализ с Wireshark

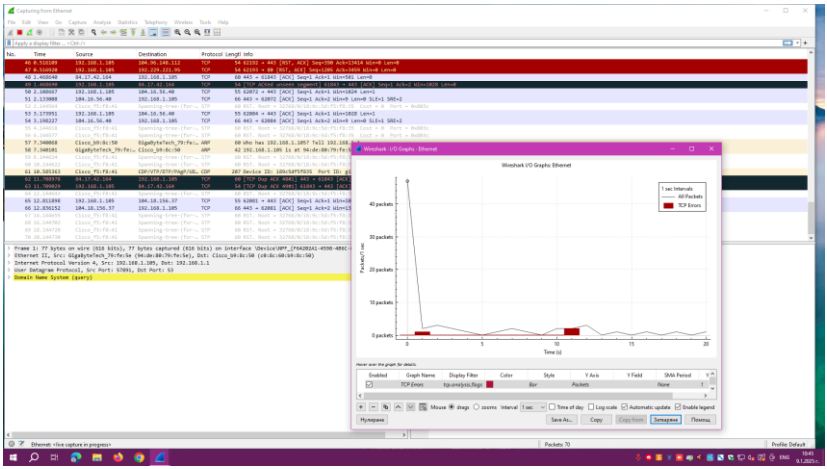
Wireshark предоставя времеви маркер, адреси, портове, протоколни полета и съдържание за всеки уловен пакет. Филтрите за визуализация (display filters) ограничават показваните записи според IP адрес, TCP/UDP порт, флагове или използван протокол. При диагностиката могат да се проследят повторни предавания, липсващи потвърждения, необичайни DNS заявки и множество SYN пакети без успешно завършване на връзката [1, 4]. Анализът на криптиран трафик е възможен само когато са налични подходящите сесийни тайни или ключов материал; самото наличие на сертификат не е достатъчно във всички конфигурации.

Времеви характеристики

Времето между два последователни пакета се определя чрез $\Delta t_i = t_{i+1} - t_i$. При правилно съпоставени заявка и отговор закъснението се определя като $\Delta t = t_{\text{отговор}} - t_{\text{заявка}}$, при което $\Delta t \geq 0$. Получаването на отрицателна стойност показва неправилно съпоставяне на пакетите или грешка във времевите маркери и не трябва да се коригира чрез използване на абсолютна стойност.

Таблица 2: Илюстративни времеви данни, адаптирани от [1]

Тип	Източник	Дестинация	Заявка, ms	Отговор, ms	Δt, ms
HTTP	192.168.1.2	192.168.1.11	100	150	50
Z-Wave шлюз	192.168.1.5	8.8.8.4	200	270	70
DNS	192.168.1.3	8.8.4.4	320	340	20
Zigbee шлюз	192.168.1.4	192.168.1.20	500	650	150
TCP SYN	192.168.1.7	192.168.1.12	800	900	100



Фиг. 2: Улавяне и времеви анализ на пакети с Wireshark [1]

Средната стойност е 78 ms, медианата е 70 ms, а максималното наблюдавано закъснение е 150 ms. Само по тези пет записа не може да се направи статистически надежден извод за аномалия. Те показват начина на изчисление и необходимостта всяка стойност да се сравнява с базова линия за съответната услуга, час и тип трафик.

Симулационна проверка с Cisco Packet Tracer

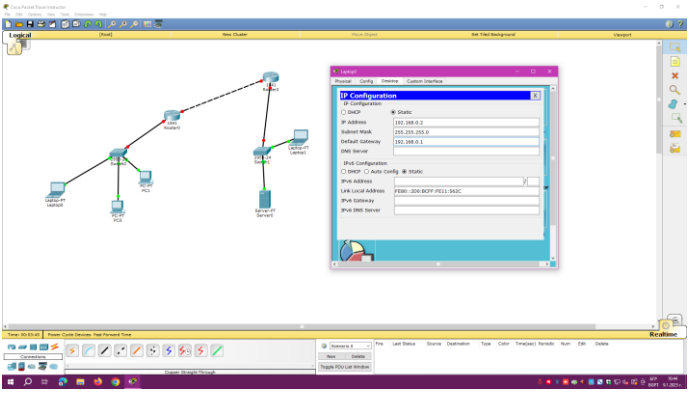
Cisco Packet Tracer позволява топологията, адресирането, VLAN сегментацията, маршрутизацията и ACL правилата да бъдат изследвани без въздействие върху производствена мрежа [2]. Контролираният сценарий започва с описание на нормален обмен, след което се въвежда конкретно отклонение. Получените пакети и събития се сравняват с очакваното поведение и се формулира правило за откриване.

Сценарий за ARP spoofing

Протоколът ARP установява съответствието между мрежовия IP адрес и физическия MAC адрес в локалната мрежа [9]. При ARP spoofing нападателят

изпраща фалшиви ARP съобщения, чрез които подменя тези съответствия. Индикатори за атаката са промяна на MAC адреса, свързан с вече известен IP адрес, свързване на няколко IP адреса с един и същ неочакван MAC адрес, получаване на непоискани ARP отговори и чести промени в ARP таблицата. В контролирана лаборатория се записва нормалното състояние, въвежда се подправен ARP трафик и се проверява дали правилата откриват промяната.

VLAN ограничава областта на разпространение, но сама по себе си не проверява достоверността на ARP. Dynamic ARP Inspection използва доверена база от съответствия, а port security ограничава допустимите MAC адреси на порт. След активиране на мерките е необходимо повторно изпитване, защото прекалено строгото правило може да блокира легитимни устройства.



Фиг. 3: Симулационна топология и конфигуриране на устройство в Cisco Packet Tracer [1]

Таблица 3: Процес за симулиране, откриване и проверка на защитата

Етап	Действие	Проверка
1	създаване на базова топология	валидни IP/MAC съответствия
2	симулиране на отклонение	поява на непоискани ARP отговори
3	улавяне и филтриране	arp display filter и сравнение на таблиците
4	прилагане на защита	Dynamic ARP Inspection, DHCP snooping, port security
5	повторно изпитване	блокиране на невалидните съобщения и запазена свързаност

За ограничаване на атаки с подправен изходен IP адрес може допълнително да се прилага входящо филтриране (ingress filtering), при което се отхвърлят пакети с адреси, несъответстващи на мрежата, от която постъпват [8].

Предложен хибриден показател и алгоритъм

За автоматизирано приоритизиране се предлага комбиниран показател H в интервала [0,1]. Той не заменя решението на анализатора, а обединява няколко независими признака:

$$H = 0{,}40S + 0{,}20T + 0{,}15P + 0{,}15C + 0{,}10A$$

S е сигнатурно съвпадение; T е нормализирано отклонение на времето за отговор; P е отклонение на пакетната интензивност; C е дял на неуспешните или незавършени TCP сесии; A е оценка за промяна в адресните съответствия. При наличие на потвърдено сигнатурно съвпадение S приема стойност 1, а при липса – 0. Компонентът C се определя като отношение между броя на неуспешните или незавършените TCP сесии и общия брой наблюдавани сесии. Стойностите на T, P и A се нормализират спрямо предварително определени прагове за съответната мрежа, като резултатите се ограничават в интервала [0,1].

Последователност на обработване

Първо се определя наблюдаваният сегмент и се събира нормален трафик за достатъчно представителен период. След това се извличат времеви, обемни и протоколни признаци. Известните сигнатури се проверяват преди аномалийния модел. Ако H премине съответния праг, събитието се свързва с информация от HIDS, защитната стена и журналите на приложението. Накрая мрежовата топология и защитните настройки се моделират в Cisco Packet Tracer, а пълният сценарий с реален или генериран трафик се възпроизвежда в подходяща изолирана лабораторна среда. След прилагането на защитната мярка се проверява дали тя намалява стойността на показателя, без да прекъсва легитимната услуга.

Праговете са начални и трябва да се калибрират. Мрежа с периодични пикове, VoIP, видео или промишлени протоколи има различен нормален профил. Намаляването на фалшивите аларми изисква отделни базови линии по услуга и време, както и потвърждение от повече от един източник.

Таблица 4: Предложени прагове за първоначално лабораторно калибриране

H	Интерпретация	Действие
0,00–0,29	обичайно поведение	запис и периодично наблюдение
0,30–0,59	отклонение с ограничена увереност	корелация с други източници и кратко засилено наблюдение
0,60–0,79	вероятен инцидент	предупреждение, анализ на потока и проверка на хоста
0,80–1,00	висока увереност или критично отклонение	незабавна реакция според утвърден план

Ограничения

Представените времеви стойности са малък илюстративен набор и не доказват точност на класификатор. Packet Tracer моделира само поддържаните функции и не възпроизвежда напълно натоварването, закъсненията и поведението на реални устройства. Поради това методиката трябва да бъде проверена с по-големи PCAP

набори, ясно означени нормални и атакуващи периоди и показатели precision, recall и F1.

Заключение

Съвместното използване на Wireshark, Cisco Packet Tracer и логиката на системите за откриване на проникванията създава последователна връзка между наблюдението, анализа и проверката на мрежовата защита. Wireshark осигурява подробни пакетни доказателства, симулационната среда позволява безопасно възпроизвеждане на сценарии, а IDS организира автоматизираното откриване. NIDS и HIDS предоставят различна видимост и постигат по-надежден резултат, когато събитията им се корелират.

Предложеният показател H комбинира сигнатурни и аномалийни признаци и създава основа за приоритизиране на събитията. Неговите тегла и прагове не са универсални и трябва да се валидират експериментално. Основният принос на доклада е интегрираната методика: базова линия, улавяне на трафик, извличане на признаци, хибридна оценка, симулационно възпроизвеждане, прилагане на защита и повторно изпитване.

Бъдещата работа трябва да включи автоматизирано извличане на признаци от PCAP файлове, сравнение на сигнатурен, аномалиен и хибриден вариант върху един и същ набор и оценка на точността при променящ се легитимен трафик. Това ще позволи методиката да премине от концептуален модел към възпроизводим експеримент.

Литература

1. Tsankov, Ts., & Hatib, I. (2024). Analyse network traffic and improve security with Wireshark and Cisco Packet Tracer. Annual of Konstantin Preslavsky University of Shumen, XIV E, 74–81. https://doi.org/10.46687/YT24CEC
2. Denev, D., & Tsankov, Ts. (2023). Use of Cisco Packet Tracer in evaluation of communication networks. Proceedings of the XVI International Scientific Conference "Innovations in Technologies and Education", 163–171.
3. Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS) (NIST Special Publication 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94
4. Denev, D. (2023). Surveillance with Wireshark and its use in communication networks. Annual of Konstantin Preslavsky University of Shumen, XIII E, 104–109.
5. Bejtlich, R. (2013). The practice of network security monitoring. No Starch Press.
6. Paxson, V. (1999). Bro: A system for detecting network intruders in real-time. Computer Networks, 31(23–24), 2435–2463. https://doi.org/10.1016/S1389-1286(99)00112-7
7. Roesch, M. (1999). Snort: Lightweight intrusion detection for networks. Proceedings of the 13th USENIX Conference on System Administration (LISA '99), 229–238.

8. Ferguson, P., & Senie, D. (2000). Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing (RFC 2827). Internet Engineering Task Force. https://doi.org/10.17487/RFC2827
9. Plummer, D. C. (1982). An Ethernet address resolution protocol (RFC 826). Internet Engineering Task Force. https://doi.org/10.17487/RFC0826

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

DECISION-MAKING MODEL FOR ADAPTIVE ACCESS CONTROL IN A UNIVERSITY INFORMATION SYSTEM

Radostin H. Lefterov

Technical University of Gabrovo Dept. of Mathematics, Informatics and Natural Sciences
Gabrovo, Bulgaria, rikitab97@gmail.com

***Abstract**: Modern university information systems require access control mechanisms that consider not only predefined user permissions but also the dynamic conditions under which access requests are made. This paper presents a model for adaptive decision-making in access control within a university information system. The proposed model employs a sequential evaluation of user roles, attributes, contextual information, SIEM and EDR data, as well as risk assessment to determine the final access decision. The paper describes the main factors influencing the decision-making process, presents a conceptual model of its operation, and discusses illustrative application scenarios. In addition, the advantages and limitations of the proposed approach are outlined together with directions for future experimental evaluation and practical implementation.*

***Keywords**: Adaptive access control; decision-making; university information system; risk assessment; RBAC; ABAC; SIEM; EDR; cybersecurity.*

МОДЕЛ ЗА ВЗЕМАНЕ НА РЕШЕНИЕ ПРИ АДАПТИВЕН КОНТРОЛ НА ДОСТЪПА В УНИВЕРСИТЕТСКА ИНФОРМАЦИОННА СИСТЕМА

Радостин Х. Лефтеров

Технически университет – Габрово,
катедра „Математика, информатика и природни науки“,
гр. Габрово, България
rikitab97@gmail.com

***Резюме**: Съвременните университетски информационни системи изискват механизми за контрол на достъпа, които да отчитат не само предварително зададените права на потребителите, но и динамичните условия, при които се осъществява достъпът. В настоящата работа е представен модел за адаптивно вземане на решение при контрол на достъпа в университетска информационна система. Моделът използва последователна оценка на ролята на потребителя, неговите атрибути, контекстната информация, данните от SIEM и EDR, както и оценка на риска при формиране на крайното решение. Представени са основните фактори, влияещи върху процеса на вземане на решение, концептуален модел на неговата работа и примерни сценарии за приложение. Разгледани са също предимствата и ограниченията на предложения подход, както и насоки за неговото бъдещо експериментално изследване и практическо приложение.*

***Ключови думи**: адаптивен контрол на достъпа; вземане на решение; университетска информационна система; оценка на риска; RBAC; ABAC; SIEM; EDR; киберсигурност.*

Въведение

В съвременните университетски информационни системи достъпът до ресурси се осъществява от различни категории потребители, използващи множество устройства и комуникационни среди. Наред с традиционния достъп от вътрешната университетска мрежа, все по-често се използват дистанционни връзки, мобилни устройства и облачни услуги, което създава динамична среда с повишени изисквания към сигурността [1].

При подобни условия вземането на решение за предоставяне на достъп не може да се основава единствено на предварително зададени права или на ролята на потребителя. Необходимо е да бъдат отчетени и допълнителни фактори, като характеристиките на заявката, използваното устройство, контекстът на достъпа и наличието на признаци за потенциален риск. Това налага прилагането на по-гъвкав подход, при който крайното решение се формира след анализ на информация от няколко различни източника [2,3].

Настоящата статия предлага модел за адаптивно вземане на решение при контрол на достъпа в университетска информационна система. Моделът използва последователна оценка на ролята на потребителя, неговите атрибути, контекстната информация и резултатите от наблюдението на средата, като въз основа на тях определя подходящото действие при всяка заявка за достъп. Основната цел е да бъде представена логиката за формиране на крайното решение и възможността то да се адаптира според текущото ниво на риск.

Фактори, влияещи върху вземането на решение

След постъпване на заявка за достъп е необходимо да бъде събрана достатъчно информация, въз основа на която системата да определи дали заявката може да бъде изпълнена. При предложения модел решението не се формира непосредствено след проверка на потребителското удостоверяване, а се основава на последователен анализ на няколко групи фактори. Всеки от тях предоставя различна информация за заявката и допринася за изграждането на по-пълна оценка на текущата ситуация.

Първата група фактори е свързана с потребителя. Проверява се неговата роля в университетската информационна система, както и атрибутите, които определят допустимия обхват на достъп. Към тях могат да принадлежат заеманата длъжност, факултетът, катедрата, преподаваните дисциплини или други характеристики, използвани при определяне на правата [4,5].

Наред с информацията за потребителя се анализира и контекстът, при който е подадена заявката. От значение са времето на достъп, използваното устройство, мрежата, местоположението и други условия, които могат да окажат влияние върху нивото на доверие [3,6]. При наличие на необичайни характеристики системата не прекратява автоматично заявката, а отчита тези фактори при последващата оценка.

Допълнителна информация може да бъде получена от средствата за наблюдение на събитията и защитата на крайните устройства. Данните от SIEM подпомагат откриването на съмнителна активност в информационната среда, а EDR предоставя сведения за състоянието на устройството, от което се осъществява

достъпът. Така оценката на риска не зависи само от състоянието на устройството или само от регистрираните събития, а отчита информацията и от двата източника [7,8].

Модел за адаптивно вземане на решение

Решението за предоставяне на достъп се формира чрез последователна обработка на информацията, получена от различни източници. Вместо всички проверки да имат еднаква тежест или да се разглеждат независимо една от друга, предложеният модел използва поетапна оценка, при която резултатът от всяка стъпка допринася за изграждането на крайната оценка. Крайният резултат следователно не зависи от една отделна проверка.

Процесът започва с удостоверяване на потребителя и проверка на неговите базови права за достъп. Ако те не са изпълнени, заявката се прекратява още на този етап. При успешно преминаване се анализират атрибутите на потребителя и характеристиките на заявения ресурс. Следващата стъпка включва оценка на контекстната информация, като се разглеждат параметри, свързани с използваното устройство, мрежовата среда, времето на достъп и местоположението.

След приключване на основните проверки моделът използва наличната информация от средствата за наблюдение на събитията и защитата на крайните устройства. Получените данни не водят автоматично до отказ на заявката, а участват при определяне на текущото ниво на риск. Крайното решение се взема след обединяване на всички резултати, което позволява една и съща заявка да бъде оценена по различен начин при промяна на условията, при които е направена.

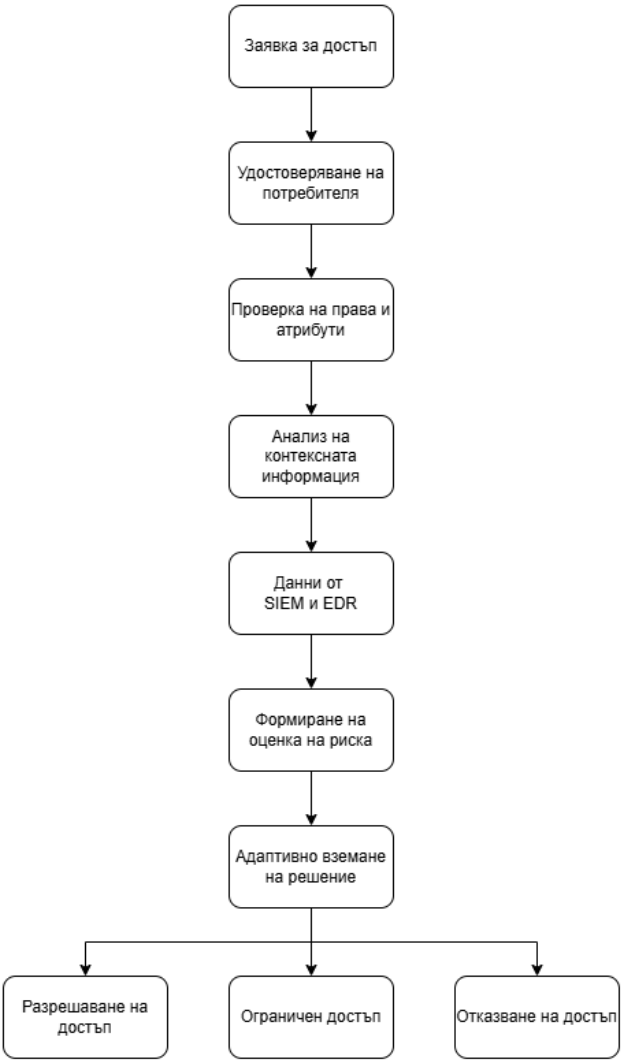
Особеност на модела е, че наличието на отделно отклонение не определя предварително крайния резултат. Различните фактори се разглеждат в контекста на цялата заявка, тъй като тяхното значение може да се променя според конкретната ситуация [3,6]. Достъп от външна мрежа например може да бъде нормален за потребител, който често работи дистанционно, но същото обстоятелство придобива по-голямо значение, ако е съчетано с непознато устройство или необичайна активност. Това позволява оценката да се променя според текущите условия, без да е необходимо основните права на потребителя да бъдат променяни при всяка нова ситуация.

Обобщената последователност от постъпването на заявката до определянето на подходящо действие е представена на фиг. 1.

Представеният модел проследява последователността на обработване на заявката за достъп – от нейното постъпване до определянето на крайното действие. Процесът започва със „Заявка за достъп", след което чрез „Удостоверяване на потребителя" се проверява самоличността на заявителя. При неуспешно удостоверяване обработването на заявката се прекратява, а при успешно се преминава към следващите проверки.

В блока „Проверка на права и атрибути" се установява дали ролята на потребителя позволява достъп до заявения ресурс и дали са изпълнени необходимите атрибутни условия. Следва „Анализ на контекстната информация", при който се отчитат използваното устройство, мрежовата среда, времето на

достъп, местоположението и други налични параметри. Целта е да бъдат установени условия, които могат да повлияят върху оценката на заявката.



Фиг. 6: Концептуален модел за адаптивно вземане на решение при контрол на достъпа

Блокът „Данни от SIEM и EDR“ допълва наличната информация със сведения за регистрирани събития, подозрителна активност и състоянието на крайното устройство. Резултатите от извършените проверки се обединяват при „Формиране на оценка на риска“, където се определя доколко конкретната заявка може да представлява риск за информационната система.

На базата на получената оценка блокът „Адаптивно вземане на решение“ определя подходящото действие. Решението не зависи само от предварително зададените права, а и от условията, при които се извършва достъпът, както и от установените отклонения.

Последните блокове представят възможните резултати – „Разрешаване на достъп“, „Ограничен достъп“ и „Отказване на достъп“. При нисък риск заявката може да бъде изпълнена в пълен обем, при наличие на определени отклонения достъпът може да бъде ограничен, а при високо ниво на риск заявката се отказва.

При определяне на нивото на риск отделните фактори не следва да се разглеждат изолирано. Например използването на непознато устройство само по себе си не е достатъчно основание за отказ на достъп. Ако обаче то е съчетано с необичайно местоположение, нетипичен часови диапазон или регистрирани събития за сигурност, общата оценка може да бъде повишена. Натрупването на няколко отклонения следователно оказва по-съществено влияние върху крайното решение в сравнение с наличието само на един необичаен параметър [9].

Формиране на крайното решение

След преминаване през отделните етапи на оценяване системата разполага с достатъчно информация, за да определи начина, по който да обработи заявката за достъп. Вместо да използва предварително зададено правило, основано само на един показател, предложеният модел съчетава резултатите от всички извършени проверки и формира крайно решение, съобразено с текущото състояние на заявката.

При наличие на ниско ниво на риск достъпът може да бъде предоставен без допълнителни ограничения. Ако бъдат установени фактори, които пораждат съмнения, но не представляват непосредствена заплаха, моделът може да приложи ограничен достъп или да изиска допълнително удостоверяване на потребителя [6,9]. По този начин се намалява вероятността легитимна заявка да бъде необосновано отказана, като едновременно с това се повишава нивото на защита.

При високо ниво на риск заявката не се изпълнява. В зависимост от характера на установените отклонения системата може да откаже достъп или да предприеме блокиране на заявката, когато съществуват признаци за потенциална компрометация. Независимо от взетото решение информацията за обработената заявка се записва в журнала, което позволява последващ анализ и проследяване на извършените действия.

Посочените нива не представляват фиксирани стойности, приложими еднакво във всяка университетска информационна система. Границите между тях могат да бъдат определени според използваните ресурси, изискванията за сигурност и политиките на конкретната организация. Например достъпът до общодостъпни

учебни материали може да допуска по-ниски ограничения, докато работата с административни или лични данни предполага по-строги критерии при определяне на допустимия риск.

Таблица 1: Примерни решения според оценените ниво на риск

Ниво на риск	Примерно решение
Ниско	Разрешаване на достъпа
Умерено	Ограничен достъп
Повишено	Допълнително удостоверяване
Високо	Отказ на заявката
Критично	Блокиране и запис в журнал

Примерно приложение

За да бъде илюстриран начинът на работа на предложения модел, могат да бъдат разгледани две примерни ситуации, характерни за университетска информационна система. Те имат демонстрационен характер и не представляват резултат от експериментално изследване.

В първата ситуация преподавател осъществява достъп до системата за управление на обучението чрез университетската мрежа и служебно устройство. След удостоверяване на самоличността му се потвърждава, че притежава необходимите права за работа с учебните дисциплини, които води. Контекстната информация не показва отклонения, а данните от SIEM и EDR не регистрират подозрителна активност. При тези условия моделът определя ниско ниво на риск и заявката се изпълнява без допълнителни ограничения.

Във втората ситуация студент подава заявка за достъп до системата от непознато устройство чрез външна мрежа в необичаен часови диапазон. Независимо че удостоверяването е успешно и потребителят разполага с необходимите права, анализът на контекстната информация отчита няколко фактора, които повишават нивото на риск. Ако към тях се добавят и данни за необичайна активност, получени от SIEM или EDR, моделът може да изисква допълнително удостоверяване или да ограничи достъпа до приключване на проверката. Ако същият потребител осъществи достъп от разпознато устройство и обичайна мрежова среда, при липса на други отклонения оценката на риска може да бъде по-ниска, независимо че основните му права остават непроменени.

Представените примери показват, че крайното решение не се определя единствено от ролята на потребителя. То се формира след съвместен анализ на информацията, получена от различни източници, което позволява моделът да се адаптира към конкретните условия, при които се извършва всяка заявка за достъп.

Предимства и ограничения

Предложеният модел съчетава информация от различни източници при формиране на решението за достъп, което позволява по-гъвкава оценка в сравнение с традиционните подходи, основани само на предварително зададени права. Отчитането на ролята на потребителя, неговите атрибути, контекстната информация и текущото ниво на риск създава възможност решенията да бъдат съобразени с конкретната ситуация, без да се променят основните политики за контрол на достъпа.

Наред с предимствата следва да бъдат отчетени и някои ограничения. Практическото приложение на модела изисква наличие на актуална информация за потребителите, устройствата и използваната среда, както и интеграция между отделните средства за защита. Ефективността на взетото решение зависи от качеството на наличните данни и от коректното функциониране на системите, които ги предоставят. Представеният модел има концептуален характер и неговата практическа приложимост следва да бъде потвърдена чрез експериментална реализация в реална университетска информационна система.

Заключение

В статията е представен модел за вземане на решение при адаптивен контрол на достъпа в университетска информационна система. При формирането на крайното решение се отчитат не само предварително зададените права, но и атрибутите на потребителя, контекстът на заявката, информацията от средствата за наблюдение и текущото ниво на риск. Това дава възможност достъпът да бъде оценяван според конкретната ситуация, без да се налага промяна на основните потребителски права при всяко отклонение от обичайните условия.

Съществена особеност на модела е възможността за избор между различни действия – разрешаване, ограничаване на достъпа, допълнително удостоверяване, отказ или блокиране. Решението зависи от съвкупността от установените фактори, а не от наличието на единичен необичаен параметър. Така се създава по-гъвкав механизъм за реакция при промяна на условията, в които се използва университетската информационна система.

Следващ етап от разработката е експерименталната реализация на модела в тестова среда. Практическото изследване ще позволи да бъдат определени подходящи граници между нивата на риск, да се оцени влиянието на отделните фактори върху крайното решение и да се проследи времето за обработване на заявките. Получените резултати могат да послужат за последващо настройване на модела и оценка на възможностите за прилагането му в реална университетска информационна система.

Литература

1. Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. Computers & Security, 86, 350–357. DOI: 10.1016/j.cose.2019.07.003.

2. Farhadi Ghalati, N., Estrada-Jimenez, L. A., Nikghadam-Hojjati, S., & Barata, J. (2025). *A Systematic Review of Access Control Models: Background, Existing Research, and Challenges.* IEEE Access, 13, 17777–17806. DOI: 10.1109/ACCESS.2025.3533145.
3. Kayes, A. S. M., Han, J., Rahayu, W., Dillon, T., Islam, M. S., & Colman, A. (2019). *A Policy Model and Framework for Context-Aware Access Control to Information Resources.* The Computer Journal, 62(5), 670–705. DOI: 10.1093/comjnl/bxy065.
4. Ferraiolo, D., Kuhn, D., & Chandramouli, R. (2006). *Role-Based Access Control, Second Edition.* Artech House, Norwood, MA.
5. Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2019). *Guide to Attribute Based Access Control (ABAC) Definition and Considerations.* NIST Special Publication 800-162. DOI: 10.6028/NIST.SP.800-162.
6. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture.* NIST Special Publication 800-207. DOI: 10.6028/NIST.SP.800-207.
7. Kent, K., & Souppaya, M. (2006). *Guide to Computer Security Log Management.* NIST Special Publication 800-92. National Institute of Standards and Technology DOI: 10.6028/NIST.SP.800-92.
8. Cybersecurity and Infrastructure Security Agency (CISA). (2023). Continuous Diagnostics and Mitigation (CDM) Technical Capabilities, Volume 2, Version 2.5.
9. Atlam, H. F., Azad, M. A., Alassafi, M. O., Alshdadi, A. A., & Alenezi, A. (2020). *Risk-Based Access Control Model: A Systematic Literature Review.* Future Internet, 12(6), 103. DOI: 10.3390/fi12060103.

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

CONCEPTUAL MODEL AND MULTILAYER ARCHITECTURE FOR REAL-TIME STREAMING DATA QUALITY MANAGEMENT

Svetlana M. Davidkova[1], Milen S. Davidkov[2]

Konstantin Preslavsky University of Shumen, Shumen, Bulgaria
[1]2443041056@shu.bg, [2]milen_davidkov@abv.bg

***Abstract**: A conceptual model for continuous real-time streaming data quality management is presented. Data quality is treated as a dynamic state dependent on the measurement source, communication environment, context, and processing history. The proposed multilayer architecture includes source-level validation, stream normalization, comprehensive quality assessment, and decision logic. The model allows the quality assessment process to be adapted when the characteristics of the incoming data change. It supports distributed deployment in an Edge–Fog–Cloud environment and provides traceability throughout the lifecycle of each information record. An integrated thermal energy system is used as the application context*.

***Keywords**: Streaming data, Data quality, Edge–Fog–Cloud, Data traceability*

КОНЦЕПТУАЛЕН МОДЕЛ И МНОГОСЛОЙНА АРХИТЕКТУРА ЗА УПРАВЛЕНИЕ НА КАЧЕСТВОТО НА ПОТОЧНИ ИНФОРМАЦИОННИ ДАННИ В РЕАЛНО ВРЕМЕ

Светлана М. Давидкова[1], Милен С. Давидков[2]

Шуменски университет „Епископ Константин Преславски", гр. Шумен, България,
[1]2443041056@shu.bg, [2]milen_davidkov@abv.bg

***Резюме**: Представен е концептуален модел за непрекъснато управление на качеството на поточни информационни данни в реално време. Качеството се разглежда като динамично състояние, зависещо от измервателния източник, комуникационната среда, контекста и последователността на извършените обработки. Предложена е многослойна архитектура, включваща първична проверка, поточна нормализация, комплексно оценяване и управленска логика. Моделът позволява адаптиране на оценяването при промяна в характеристиките на постъпващите данни. Предвидена е разпределена реализация в Edge–Fog–Cloud среда и проследяване на жизнения цикъл на всеки информационен запис. Като приложен контекст е използвана интегрирана топлоенергийна система.*

***Ключови думи**: Поточни данни, Качество на данните, Edge–Fog–Cloud, Проследимост на данните*

Въведение

Разпространението на IoT, SCADA и кибер-физичните системи измества управлението на данни от периодична обработка на натрупани масиви към непрекъснат анализ на събития. При този режим закъснелият, непълният или непроследимият информационен запис може да бъде формално коректен, но

практически непригоден за използване при управлението. Това налага качеството на поточните данни да се оценява не само след тяхното съхраняване, а още при постъпването и обработката им. Анализът на характеристиките, методите за оценяване и влиянието на концептуалния дрейф показва необходимостта от адаптивен подход, който отчита измененията на данните във времето. Целта на настоящото изследване е да се разработят концептуален модел и многослойна архитектура за оценяване на качеството през целия жизнен цикъл на информационния запис и за обвързване на получената оценка с допустимото управленско действие.

Методология на изследването

Методологията на изследването съчетава системен анализ, функционално разлагане и структурно описание на информационния запис. Въз основа на установените особености на поточните данни са изведени изисквания за непрекъснатост на оценяването, многомерност, адаптивност, проследимост и интеграция с управлението.

Разработването на модела преминава през последователно определяне на неговите основни принципи, функционални слоеве и връзки между тях. Архитектурните функции са разпределени между периферни, междинни и централни изчислителни нива според времевата критичност на обработката и необходимия изчислителен ресурс. По този начин се осигурява връзка между оценяването на качеството на данните и избора на подходящо управленско действие.

Разработен модел и анализ

Концептуални основи на предложения модел

Разработването на адаптивен модел за управление на качеството на поточните информационни данни изисква съчетаване на методи от областта на информационните системи, поточната обработка на данни, статистическия анализ и управлението на кибер-физични системи. При изграждането на модела трябва да се отчита и възможността характеристиките на постъпващите данни да се изменят във времето вследствие на промени в наблюдавания процес или поява на концептуален дрейф [5]. За разлика от моделите, при които качеството се оценява върху предварително натрупани информационни масиви, в предложения модел то се разглежда като динамична характеристика. Нейната текуща стойност зависи от състоянието на наблюдавания процес, точността на измервателната инфраструктура, условията в комуникационната среда и приложените методи за обработка [1–3]. Това позволява оценката да се актуализира при промяна на условията и да отразява действителната пригодност на данните за последващо използване при управлението.

Основната концепция се основава на разбирането, че всяко измерване представлява не само числова стойност, а информационен запис с определени характеристики. Освен измерената величина той съдържа данни за нейния произход, момента на възникване, начина на предаване, използвания измервателен

канал и историята на извършените обработки. По този начин качеството не се оценява единствено въз основа на стойността на измерването, а се отчита целият жизнен цикъл на информационния запис. Това позволява да се установи на кой етап е възникнало евентуално отклонение и как то влияе върху пригодността на данните за използване.

Предложеният модел е разработен така, че да не зависи от конкретна приложна област. Това позволява използването му при различни поточни информационни системи. В настоящия доклад приложението на модела се разглежда в контекста на интелигентна интегрирана топлоенергийна система, предназначена за отопление и битово горещо водоснабдяване на малко населено място.

В системата се комбинират възобновяеми и конвенционални източници на топлинна енергия, електрическа енергия, акумулиращи съоръжения и инсталация за плазмено оползотворяване на отпадъци. Съвместното им управление изисква надеждна и своевременна информация за текущото състояние на отделните елементи. Поради това управлението на качеството на поточните данни се разглежда като част от цялостното интелигентно управление на системата.

При част от традиционните SCADA системи проверката на информацията се извършва основно след постъпването ѝ в централен сървър. Разпределянето на отделни функции между различни нива на промишлената комуникационна мрежа създава възможност част от обработката да бъде извършвана по-близо до източника на данните [4, 7]. В предложения модел оценяването на качеството се разглежда като непрекъснат процес, който започва още при генерирането на измерването. По този начин записи с липсващи атрибути, недопустими стойности или неправилни времеви маркери могат да бъдат установени в периферията на системата, преди да достигнат до централните аналитични модули.

Основни принципи при изграждането на модела

Концептуалният модел е разработен въз основа на няколко основни принципа, които определят неговата архитектура и начина му на функциониране.

Първият принцип е непрекъснатото оценяване на качеството. Всяко новопостъпило измерване преминава през предварително определена последователност от проверки и оценки. Те се извършват в рамките на допустимото за системата време и позволяват отклоненията да бъдат установени възможно най-близо до момента на тяхното възникване.

Вторият принцип е многомерното описание на качеството. Вместо използването само на един общ показател, качеството се разглежда като съвкупност от взаимно свързани характеристики – точност, пълнота, навременност, валидност, съгласуваност, проследимост и надеждност [1, 2, 6, 8]. Всяка характеристика отразява различна страна на пригодността на данните за използване. Съвместното им оценяване позволява да се определи по-точно текущото състояние на информационния поток.

Третият принцип е адаптивността. Част от параметрите и критериите на модела могат да бъдат актуализирани при установено изменение на характеристиките на наблюдавания процес. Необходимостта от такава промяна се определя въз основа на наблюденията върху поточните данни и установяването на

концептуален дрейф. По този начин моделът може да се приспособява както към внезапни, така и към постепенни изменения в натоварването, работните режими и конфигурацията на енергийната система.

Четвъртият принцип е проследимостта на информацията. За всеки информационен запис се съхранява първоначално получената стойност, а последващите корекции, филтрирания и възстановявания се регистрират като отделни версии. Към тях се добавя информация за момента и начина на извършената обработка. Това позволява да бъдат проследени произходът на данните и последователността на приложените операции.

Петият принцип е интеграцията между оценяването на качеството и управлението. В предложения модел получената оценка не се използва единствено за статистически анализ, а участва при вземането на управленски решения. В зависимост от качеството и надеждността на постъпилите данни се избира подходящ режим на работа на интелигентната топлоенергийна система.

Архитектура на концептуалния модел

Предложеният модел е структуриран като многослойна архитектура. Всеки слой изпълнява определени функции и обменя информация със свързаните компоненти на системата. Разделянето на функциите позволява проверките и обработките да бъдат изпълнявани на различни изчислителни нива според тяхната времева критичност. Архитектурата включва четири основни функционални слоя (фиг. 1).



Фиг. 1: Многослойна архитектура на предложения адаптивен модел за управление на качеството на поточните информационни данни

Първият слой осъществява първична проверка и обработка на измерванията непосредствено при техния източник. Проверяват се форматът на данните, наличието на задължителните атрибути, допустимият диапазон на измерваната величина и коректността на времевия маркер. Когато измервателното устройство предоставя диагностична информация, се отчита и неговото текущо техническо състояние. Установените отклонения се регистрират и записът се маркира за последваща обработка.

Вторият слой извършва поточната обработка и нормализацията на данните. На този етап записите се преобразуват в унифициран формат, а измерванията от различните източници се подреждат и синхронизират според техните времеви маркери. Закъснелите записи се установяват и обработват съгласно предварително зададени правила. След това данните се подготвят за последващо оценяване и анализ.

Третият слой извършва комплексно оценяване на качеството. При него се обединяват оценките за точност, пълнота, навременност, валидност, съгласуваност, проследимост и надеждност. Отчитат се също установените аномалии и текущото състояние на наблюдаваната система. Общата оценка за качеството на информационния запис се определя чрез претегляне на отделните показатели:

$$Q = \sum_{i=1}^{n} w_i \, q_i, \qquad \sum_{i=1}^{n} w_i = 1, \qquad w_i \geq 0$$

където q_i е нормализираната оценка по съответния показател за качество, w_i е неговият тегловен коефициент, а n е броят на използваните показатели. Стойностите на q_i са в интервала от 0 до 1, като по-високата стойност съответства на по-високо качество. Тегловните коефициенти са неотрицателни и сборът им е равен на 1. Те се определят според предназначението и изискванията на конкретната система.

Четвъртият слой реализира управленската логика. Получената оценка за качество се сравнява с предварително определени допустими граници. В зависимост от резултата информационният запис може да бъде използван непосредствено или да бъде маркиран за допълнителна проверка. При недостатъчно качество за управлението могат да бъдат използвани данни от резервен източник, без първоначалният запис да бъде изтриван или променян. При липса на надеждна заместваща информация системата може да премине в предварително определен безопасен режим на работа.

Основните функции на отделните слоеве и възможните реакции при установяване на проблеми с качеството на данните са обобщени в табл. 1.

Представените слоеве са функционални и не е задължително да съответстват на отделни физически устройства. В зависимост от мащаба и конфигурацията на системата няколко функции могат да бъдат изпълнявани в общ изчислителен възел.

Предложената архитектура позволява моделът да бъде реализиран в разпределена Edge–Fog–Cloud среда [4, 9]. Проверките с висока времева критичност се извършват на Edge ниво, в близост до измервателните устройства.

Нормализацията и синхронизацията на данните се изпълняват на междинното Fog ниво, а по-сложните аналитични операции и дългосрочното съхранение се извършват в централната Cloud платформа.

Таблица 1: Основни функции и реакции на слоевете в предложения модел

Функционален слой	**Основна функция**	**Типична реакция**
Периферен (Edge)	Проверка на формата, диапазоните и времевите маркери	Маркиране и отделяне на некоректните записи
Поточен (Fog)	Нормализация, синхронизация и обработка на закъснели записи	Буфериране, времево подреждане и маркиране
Аналитичен	Комплексно оценяване на качеството и откриване на аномалии	Формиране на обща оценка за качество
Управленски	Избор на действие според качеството и текущия контекст	Нормален, резервен или безопасен режим на работа

Това разпределение може да намали закъснението и обема на предаваните към централната платформа данни. Локалната обработка позволява част от основните проверки да продължат и при временно прекъсване на отделни комуникационни връзки.

Научен принос и ограничения

Научният принос на изследването се състои в разработването на концептуален модел, който обединява непрекъснатото оценяване на качеството на поточните информационни данни, адаптирането към измененията в техните характеристики и избора на съответна управленска реакция. Предложено е функционално разпределение на отделните дейности между периферно, междинно и централно изчислително ниво.

Ограничение на настоящото изследване е неговият концептуален характер. Стойностите на тегловните коефициенти, допустимите граници и правилата за избор на управленска реакция трябва да бъдат определени и проверени за конкретната измервателна и технологична среда. Експерименталната проверка на модела е предвидена като следващ етап на изследването.

Заключение

В доклада е представен концептуален модел за непрекъснато управление на качеството на поточните информационни данни в реално време. При него оценяването на качеството не се разглежда само като последваща контролна процедура, а като част от процеса на вземане на управленски решения.

Разделянето на функциите между периферно, междинно и централно изчислително ниво създава възможност проверките с висока времева критичност да се извършват близо до източника на данните, а по-сложните анализи – в централната платформа. Проследяването на извършените обработки запазва връзката между първоначално получената стойност и нейните последващи версии.

Следващият етап на изследването включва създаване на прототип, определяне на параметрите за конкретната топлоенергийна система и количествено сравнение с централизирана архитектура за обработка на данни.

Литература

1. Batini C., Cappiello C., Francalanci C., Maurino A. Methodologies for Data Quality Assessment and Improvement. ACM Computing Surveys, Vol. 41, No. 3, 2009, Article 16, pp. 1–52. DOI: 10.1145/1541880.1541883.
2. Denev D., Tsankov Ts. A Survey of Data Quality and Processing of Information in Innovative Smart Devices. 2022 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 2022, pp. 311–315. DOI: 10.1109/ICAI55857.2022.9960040.
3. Cai L., Zhu Y. The Challenges of Data Quality and Data Quality Assessment in the Big Data Era. Data Science Journal, Vol. 14, 2015, Article 2, pp. 1–10. DOI: 10.5334/dsj-2015-002.
4. Denev D. R., Tsankov Ts. S. Design and Implementation of a Field Level of an Industrial Communication Network for the Needs of the Industry. Proceedings of the 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST 2022), Ohrid, North Macedonia, 2022, pp. 1–4. DOI: 10.1109/ICEST55168.2022.9828607.
5. Gama J., Žliobaitė I., Bifet A., Pechenizkiy M., Bouchachia A. A Survey on Concept Drift Adaptation. ACM Computing Surveys, Vol. 46, No. 4, 2014, Article 44, pp. 1–37. DOI: 10.1145/2523813.
6. ISO/IEC 25012:2008. Software Engineering — Software Product Quality Requirements and Evaluation (SQuaRE) — Data Quality Model. International Organization for Standardization, Geneva, 2008.
7. Denev D., Tsankov Ts. Communication-Based Dynamic Packet Optimization for Visual PLC Monitoring. Proceedings of the Annual University Scientific Conference of Vasil Levski National Military University, 2022, pp. 1259–1266. ISSN 2367-7481.
8. Wang R. Y., Strong D. M. Beyond Accuracy: What Data Quality Means to Data Consumers. Journal of Management Information Systems, Vol. 12, No. 4, 1996, pp. 5–33. DOI: 10.1080/07421222.1996.11518099.
9. Shi W., Cao J., Zhang Q., Li Y., Xu L. Edge Computing: Vision and Challenges. IEEE Internet of Things Journal, Vol. 3, No. 5, 2016, pp. 637–646. DOI: 10.1109/JIOT.2016.2579198.

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**, Faculty of Artillery, Air Defense and Communication and Information Systems

REAL TIME HIGH ORDER QUADRATURE AMPLITUDE MODULATION IMPLEMENTED VIA SOFTWARE-DEFINED RADIO: FUNDAMENTAL STRUCTURE, EMPIRICAL CHARACTERIZATION, AND MILITARY APPLICATION

Ivan I. Ivanov

Joint Forces Command, Sofia, Bulgaria
i.i.ivanov@armf.bg

Abstract: *This paper presents the fundamental structure and empirical characterization of 64-QAM and 256-QAM modulation schemes implemented using a software-defined radio (SDR) based on the USRP B210 transceiver platform. Geometric and energy related relationships governing the heightened sensitivity of dense signal constellations (minimum Euclidean distance, required Es/N0 ratio, and peak to average power ratio PAPR. These relationships are validated through direct real time measurements using the developed transceiver. Operational advantages associated with the controlled use of high order modulation in military applications are discussed, and directions for future research are outlined.*

Keywords: *software-defined radio, quadrature amplitude modulation, high order modulation, PAPR, military communications.*

ВИСОКОРЕДОВА КВАДРАТУРНА АМПЛИТУДНА МОДУЛАЦИЯ В РЕАЛНО ВРЕМЕ РЕАЛИЗИРАНА НА БАЗАТА НА СОФТУЕРНО ДЕФИНИРАНО РАДИО: ФУНДАМЕНТАЛНА СТРУКТУРА, ЕМПИРИЧНА ХАРАКТЕРИЗАЦИЯ И ВОЕННО ПРИЛОЖЕНИЕ

Иван И. Иванов

Съвместно командване на силите, София, България
i.i.ivanov@armf.bg

Резюме: *Представени са фундаменталната структура и емпиричната характеризация на 64- и 256-QAM модулации, реализирани със софтуерно дефинирано радио (SDR) на базата на приемо-предавателна платформа USRP B210. Изведени са геометричните и енергийните зависимости, обуславящи повишената чувствителност на плътните сигнални съзвездия (минимално Евклидово разстояние, изисквано съотношение Es/N0, отношение пикова към средна мощност – PAPR). Тези зависимости са потвърдени чрез директни измервания в реално време с разработения трансивър. Обсъдени са оперативните предимства при контролирано използване на висок ред модулация във военната сфера и са дефинирани насоки за бъдещи изследвания.*

Ключови думи: *софтуерно дефинирано радио, квадратурна амплитудна модулация, висок ред модулация, PAPR, военни комуникации.*

Увод

Софтуерно дефинираното радио (SDR) премества функциите на аналоговите физически компоненти в софтуерни алгоритми, изпълнявани от програмируеми изчислителни устройства [1]. Това прави физическия слой преконфигуруем без необходимост от хардуерни промени. Наличните в литературата SDR реализации на адаптивна модулация върху обща изчислителна платформа обикновено се ограничават до BPSK, QPSK и 8-PSK, като изборът на модулационна схема се управлява в реално време въз основа на оценка на съотношението сигнал/шум [2]. Тази архитектура е експериментално потвърдена върху платформа USRP B210, която се използва и в настоящата разработка. По-ранни реализации на SDR модеми, документирани при π/4-DQPSK модем [3] и неговото разширение с пространствено разнесено приемане [4], също не надхвърлят рамките на QPSK фамилията. Официалният пакетен модем в средата GNU Radio, явяваща се най-широко използваната SDR платформа с отворен код, по подобен начин спира до QPSK [5].

Литературно проучване не открива адаптивен трансивър с една носеща честота, обхващащ нива до 64-/256-QAM, с характеризирана в реално време приемна верига (синхронизация, автоматично регулиране на усилването, демапиране) върху общодостъпен SDR хардуер. Този преглед е ограничен по обхват и не претендира за глобално отсъствие на подобни разработки. В настоящия доклад се представя именно такъв трансивър, функциониращ върху USRP B210 с непрекъснато работеща в реално време приемо-предавателна верига. Изследват се причините, поради които преходът отвъд 8-PSK към плътни QAM съзвездия изисква качествено различен подход, какви са практическите ползи от това и каква е емпиричната цена.

Основните приноси на доклада са:

- Извеждане на фундаменталната структура на приемо-предавателната верига въз основа на класическата литература за QAM и адаптивни трансивъри [7, 8], приложена конкретно за прехода отвъд 8-PSK;
- Количествен анализ на геометричната и енергийната цена при използване на плътни сигнални съзвездия;
- Емпирични измервания с реален трансивър USRP B210, потвърждаващи теоретичните зависимости;
- Анализ на приложимостта във военното дело и дефиниране на насоки за бъдещи изследвания.

1 Военно приложение

Софтуерно дефинираните радиосистеми се разглеждат в специализираната българска военна литература като ефективно средство за гъвкаво и енергийно ефективно използване на радиочестотния спектър [10], като изрично са анализирани предимствата и предизвикателствата при оперативното им разгръщане [11]. Разширението на възможностите конкретно към 64-/256-QAM добавя количествено измерение към тази обща оценка, подкрепено от теоретичната и емпиричната основа, развити в Раздели 2–5.

Военните радиокомуникационни мрежи функционират в строго регулирани и споделени честотни ленти [10]. Учетворената спектрална ефективност на 256-QAM спрямо QPSK (Раздел 3, Таблица 1) директно намалява необходимата честотна лента за дадена скорост на предаване. Това е съществено предимство при честотен дефицит, какъвто обикновено възниква в полеви условия.

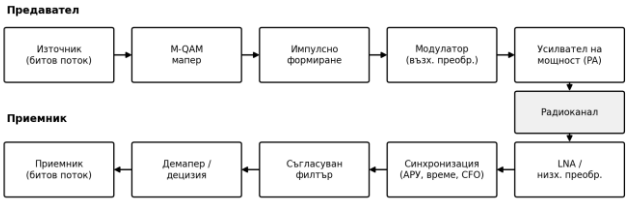
Резултатите, изведени по-долу в Раздел 5, сочат към дефинирането на конкретна оперативна политика: целесъобразно е 256-QAM да се активира само при потвърден стабилен радиоканал (например при къси и фиксирани линии – команден пункт в защитена позиция или релейна връзка при пряка видимост). Тази схема не е подходяща като постоянна работна точка за мобилни тактически възли с динамично променящ се канал, за които 64-QAM предлага по-устойчив компромис между скорост на трансфер и праг на срив на линка.

Стесняването на разстоянието d_{min} при повишаване на реда на модулация (Раздел 3) означава, че за прекъсване на връзката при 256-QAM е необходима пропорционално по-ниска мощност на радиоелектронно подавяне (РЕП) в сравнение със същия линк, работещ на QPSK [10]. Поради тази уязвимост, съзнателното ограничаване на модулационния ред до нивото, строго необходимо за изпълнение на конкретната задача (вместо автоматично избиране на най-високия достъпен ред), се явява директна практическа мярка за защита на комуникациите.

2 Фундаментална структура на приемо-предавателната верига

Класическата структура на цифров M-QAM приемо-предавател се състои от [6, 7, 8]:

- **Предавателна верига:** картографиране на битовия поток в комплексни символи (M-QAM мапер), импулсно формиране (филтрация), честотно преобразуване нагоре (up-conversion) и усилване на мощността.
- **Приемна верига:** честотно преобразуване надолу (down-conversion), съгласувана филтрация, блокове за синхронизация – автоматично регулиране на усилването (АРУ/AGC), времева синхронизация (timing) и възстановяване на носещата честота (CFO) – и демапиране за вземане на решение. На Фигура 1 е представена тази обща структура, която е инвариантна спрямо конкретния ред на модулация M.



Фигура 1: Фундаментална структура на M-QAM приемо-предавателна верига.

Изборът на параметъра M рефлектира върху два взаимно свързани, но качествено различни аспекта на веригата:

- Увеличаването на размера на съзвездието в мапера/демапера (M точки вместо 4) изисква по-фина и сложна решаваща логика при демапиране.
- Изискванията към аналоговите блокове (усилвател на мощност (PA), аналогово-цифров преобразувател (АЦП)) стават количествено много по-строги с нарастването на M по причини, изведени в Раздел 3. Това прави прехода от 8-PSK (постоянна амплитуда, само фазова модулация) към M-QAM (променлива амплитуда и фаза) различен скок, а не просто разширение на броя точки в съзвездието.

3 Предимства на модулациите от висок ред

Спектралната ефективност на M-QAM, изразена в брой битове на символ, се определя като [7]:

$$\eta = \log_2 M \tag{1}$$

При 64-QAM (η=6) и 256-QAM (η=8), спрямо базовия QPSK (η=2), теоретичният капацитет на канала при еднаква заета честотна лента нараства съответно 3 и 4 пъти. Тази директна практическа полза е основният мотив за прехода към по-високи редове на модулация.

Цената на това увеличение обаче е двустранна. От гледна точка на надеждността при липса на кодиране, изискваното съотношение E_s/N_0 за постигане на целева вероятност за грешка нараства значително с увеличаването на M (Таблица 1). В същото време, минималното Евклидово разстояние между съседни точки в съзвездието при нормирана средна енергия на символа E_s, намалява по формулата [7]:

$$d_{min} = \sqrt{(6E_s/(M-1))} \tag{2}$$

От гледна точка на хардуерната реализация, отношението пикова към средна мощност (PAPR) на M-QAM сигнала нараства с увеличаването на M, тъй като по-широкото разпределение на амплитудите увеличава вероятността за поява на високи мигновени пикове в мощността [9]. При работа на предавателния усилвател (PA) близо до зоната на насищане, по-високият PAPR налага по-голямо занижение на изходната мощност. Това е необходимо, за да се избегнат нелинейни изкривявания, към които плътните сигнални съзвездия са изключително чувствителни.

Таблица 1: Теоретични зависимости от реда на модулация M.

Модулация	η (bit/symbol)	d_min (отн. към QPSK)	Изискван Es/N0
QPSK	2	1.00×	13.5 dB
16-QAM	4	0.45×	20.5 dB
64-QAM	6	0.22×	26.5 dB
256-QAM	8	0.11×	32.5 dB

4 Експериментална реализация и изметвания

Експерименталните измервания са проведени с разработената SDR система на базата на USRP B210, поддържаща четиристепенна адаптивна модулация (с възможност за ръчно управление QPSK/16-/64-/256-QAM), импулсно формиране (филтър с характеристика корен квадратен от повдигнат косинус – RRC, с коефициент на заобляне $\beta = 0.35$) и скорост на отчитане 5.0 MS/s. Приемната верига изчислява непрекъснато показателите за качество на връзката за всеки обработен блок, оценките за конкретните радиочестотни (RF) деградации на сигнала, пропускателната способност и стабилността на приемния процес. Пълният набор от измервани параметри е представен в Таблица 2.

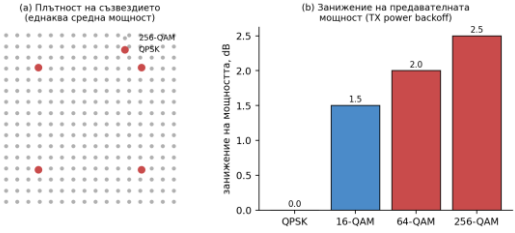
Таблица 2: Стойности, измервани в реално време от реализирания трансивър.

Стойност	Описание
MER (dB)	Modulation Error Ratio (коефициент на грешка на модулацията), изчислен въз основа на отклонението на приетите символи спрямо идеалните референтни точки.
EVM (%)	Error Vector Magnitude (вектор на грешката), алтернативно представяне на MER.
Суров BER	Некодирана честота на битовите грешки, измерена спрямо известна псевдослучайна последователност (PRBS).
BER след FEC	Декодирана честота на битова грешка, когато е активна схема за корекция на грешки (извън обхвата на настоящия доклад).
CFO (Hz)	Остатъчно отместване на носещата честота (Carrier Frequency Offset) след процеса на синхронизация.
RMS фазова грешка (°)	Средноквадратично отклонение на фазата на приетите символи спрямо номиналната.
IQ дисбаланс (dB)	Амплитудно и фазово разминаване между синфазния (I) и квадратурния (Q) клон на приемника.
SNR по спектър (dB)	Оценка на съотношението сигнал/шум, изчислена директно от честотния спектър на приетия сигнал.

Стойност	Описание
PAPR (dB)	Измерено отношение пикова към средна мощност на генерирания сигнал за съответната модулация.
Модулационна скорост (Mbps)	Теоретичен капацитет на физическия слой при съответния модулационен ред и символна скорост.
Реална скорост (Mbps)	Действително предаден полезен товар (throughput), изключвайки служебните и запълващите (filler) блокове.
AGC gain	Текущ коефициент на усилване, прилаган от блока за автоматично регулиране на усилването преди демапиране.
RX overflows / timeouts	Брой препълвания на приемния буфер и пропуснати отчети – индикатор за изчислителната натовареност на приемника в реално време.

За детайлно характеризиране на поведението на физическия слой, независимо от влиянието на конкретни кодове за корекция на грешки (FEC), от общия масив данни бяха анализирани следните ключови показатели:

1. Оценката на необходимото занижение на предавателната мощност за поддържане на извънлентовите излъчвания в допустимите граници;
2. Стойността на постигнатият коефициент MER при директна връзка на близко разстояние (line-of-sight с разнесени антени), определящ горната граница на качеството за дадената хардуерна конфигурация.



Фигура 2: (a) относителна плътност на съзвездията при еднаква средна мощност; (b) измерено занижение на предавателната мощност по модулация.

На Фигура 2(b) е изобразен измереният необходим TX backoff за различните видове модулации. При QPSK той е 0 dB (поради сравнително постоянната обвивка на сигнала PAPR не оказва негативно влияние), като се наблюдава монотонно нарастване до 2.5 dB при 256-QAM. Тази тенденция потвърждава теоретичните очаквания от Раздел 3 – по-плътните съзвездия изискват по-голям линеен резерв спрямо точката на насищане на усилвателя, което е за сметка на средната изходна мощност.

Таблица 3: Постигнато MER при директно (близко) антенно разположение и реален марж.

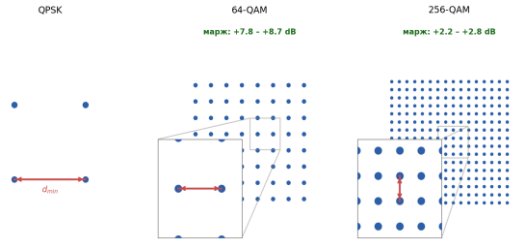
Модулация	Изискван праг (Табл. 1)	Постигнато MER	Марж
64-QAM	26.5 dB	≈34.3–35.2 dB	+7.8 – +8.7 dB
256-QAM	32.5 dB	≈34.7–35.3 dB	+2.2 – +2.8 dB

Данните в Таблица 3 показват, че и двата реда модулации осигуряват положителен запас спрямо теоретичния праг на чувствителност, но с качествено различна ширина. Докато при 64-QAM е налице стабилен резерв от 7.8–8.7 dB, то при 256-QAM този марж се свива до едва 2.2–2.8 dB. Това е директно експериментално доказателство за тесния толеранс към шумове, породен от геометричните особености на констелацията. Тези количествени граници са специфични за изследвания хардуер (USRP B210) и конкретните параметри на сигнала.

5 Анализ на резултатите

На Фигура 3 е представена визуално геометрията от Раздел 3, съпоставена с измерените маржове от Таблица 3. Свиването на практическия марж при прехода от 64-QAM (≈9 dB) към 256-QAM (≈3 dB в най-добрия случай) е пряко следствие от намаляването на минималното Евклидово разстояние d_{min}. Докато при 64-QAM се запазва 0.22× от разстоянието, характерно за QPSK, при 256-QAM то намалява наполовина до 0.11×. Това линейно сгъстяване на точките в съзвездието рязко повишава уязвимостта на системата към хардуерни и канални смущения, което се материализира в драстичен спад на енергийния запас с около 6 dB.

Тази зависимост демонстрира строга съгласуваност по посока и мащаб, като стойностите на маржа намаляват монотонно с нарастването на модулационния ред M. Разликата между двата измерени маржа (≈6 dB) съответства адекватно на теоретичното нарастване на изисквания SNR праг между двата реда модулация (32.5 - 26.5 = 6 dB, съгласно Таблица 1).



Фигура 3: Минимално Евклидово разстояние при QPSK, 64-QAM и 256-QAM (еднаква средна мощност) и съответният измерен марж над теоретичния праг.

Практическото следствие от този анализ налага ясно разграничение между двете схеми. Модулацията 64-QAM осигурява трикратна спектрална ефективност спрямо QPSK, поддържана от солиден енергиен резерв (7.8–8.7 dB) при реални условия. От друга страна, 256-QAM предлага четирикратно увеличение на капацитета, но работи с осезаемо по-тесен, но все пак стабилно положителен резерв (марж от 2.2–2.8 dB), постижим единствено при радиолинии, близки до идеалните. Следователно изборът на модулация трябва да се базира на прецизен компромис, съобразен с конкретната хардуерна платформа и динамиката на радиоканала, както бе обсъдено в Раздел 1, а не на максималистичния принцип „възможно най-висок ред".

Въз основа на ограниченията на настоящото изследване се дефинират някои основни насоки за бъдеща работа:

- Разширяване на обхвата на измерванията извън лабораторна геометрия на къси разстояния, за да се оцени влиянието на реалното многолъчево разпространение и фадинг върху стабилността на 256-QAM;
- Интегриране на алгоритми за шумоустойчиво кодиране (FEC), които съзнателно бяха изключени от настоящата работа, тъй като кодовата защита директно променя ефективния праг на срив на системата;
- Реализиране и сравнителен анализ с налични адаптивни BPSK/QPSK/8-PSK системи [2] върху идентична хардуерна платформа за получаване на директна оценка на компромиса между диапазон на адаптация и реална пропускателна способност.
- Комбиниране на адаптивна високоредова QAM с установени схеми за многостанционен достъп, изследвани самостоятелно в по-ранна българска литература [12].

Заключение

В настоящата работа бяха изведени фундаменталните геометрични и енергийни зависимости при високоредови модулации (намаляване на минималното Евклидово разстояние и нарастване на PAPR с реда на модулация), като същите бяха потвърдени експериментално чрез SDR трансивър на базата на USRP B210. Измереното необходимо занижение на предавателната мощност нараства монотонно от 0 до 2.5 dB, а разликата между маржовете на 64-QAM и 256-QAM (≈6 dB) съвпада почти точно с разликата в теоретичните им прагове, потвърждавайки че постигнатото MER на двата реда е практически еднакво и цялата разлика идва от геометрията, не от остатъчна деградация.

За целите на военните комуникации тези резултати обосновават необходимостта от **динамично и ситуационно (адаптивно)** ангажиране на високите редове модулация. То трябва да бъде строго съобразено с високата чувствителност на плътните сигнални съзвездия към средства за радиоелектронно подавяне (РЕП). Учетворената спектрална ефективност на 256-QAM остава съществено предимство при типичния за тактическите мрежи честотен дефицит, но само при контролирано използване в защитени физически линкове. Изведените

количествени резултати са ограничени до изследваната хардуерна конфигурация на реално работещата в базова лента приемо-предавателна SDR верига.

Литература

1. Mitola, J. (1995). The software radio architecture. IEEE Communications Magazine, 33(5), 26–38.
2. 2. Gummineni, M., & Polipalli, T. R. (2023). Real Time Implementation of Automatic Digital Modulation-Based SNR Estimation Using SDR Platforms. Wireless Personal Communications. doi:10.1007/s11277-023-10681-0
3. 3. Ivanov, I. (2023). Modeling, Simulation and Implementation of π/4-DQPSK Modem on SDR. Proc. XXXII International Scientific Conference Electronics (ET 2023), IEEE, 1–5. doi:10.1109/ET59121.2023.10278732
4. 4. Ivanov, I., & Angelov, M. (2024). Design and Implementation of Software-Defined π/4-DQPSK Modem with Receive Antenna Diversity. Environment. Technology. Resources, 3, 101–104. doi:10.17770/etr2024vol3.8108
5. 5. GNU Radio Project. (2026). QPSK Mod and Demod; Packet Communications. GNU Radio Wiki. (accessed 28 August 2026).
6. 6. Ivanov, I. P. (2025). Software-Defined Radio Communication Systems [in Bulgarian]. Defence Institute, Sofia. ISBN 978-619-90024-8-3.
7. 7. Hanzo, L., Ng, S. X., Keller, T., & Webb, W. (2004). Quadrature Amplitude Modulation: From Basics to Adaptive Trellis-Coded, Turbo-Equalised and Space-Time Coded OFDM, CDMA and MC-CDMA Systems (2nd ed.). Wiley-IEEE Press.
8. 8. Hanzo, L., Wong, C. H., & Yee, M. S. (2002). Adaptive Wireless Transceivers: Turbo-Coded, Turbo-Equalized and Space-Time Coded TDMA, CDMA and OFDM Systems. Wiley-IEEE Press.
9. 9. Salman, M. B., & Guvensen, G. M. (2021). An Efficient QAM Detector via Nonlinear Post-Distortion Based on FDE Bank Under PA Impairments. IEEE Transactions on Communications, 69(9), 5947–5961.
10. 10. Неделчев, М. (2023). Изследване на възможности за изграждане на софтуерно дефинирана радиосистема за динамичен достъп до честотните ресурси. Автореферат на дисертация, Национален военен университет „Васил Левски“, Факултет „Артилерия, ПВО и КИС“, Шумен.
11. 11. Неделчев, М., Богданов, Р. (2019). Софтуерно дефинирани радиосистеми с военно предназначение – предимства и предизвикателства. Списание СІО, ISSN 1312-5605.
12. 12. Съслеков, Е., & Ангелов, М. (2001). Performance of time division duplex CDMA mobile communication. Известия на Технически университет – Пловдив „Технически науки“, 7, 201–206.

SHUMENTECH AS A REGIONAL HUB FOR DUAL-USE TECHNOLOGIES AND DEFENSE INNOVATION IN BULGARIA'S NATIONAL SECURITY SYSTEM

Vladislav Milkov Genoff[1], Hristo Atanasov Hristov[2]

[1] Department "Computer Systems and Technologies", "Artillery, Air Defense and CIS" Faculty, "Vasil Levski" National Military University, Shumen, Shumen, Bulgaria, e-mail: vgenov70@gmail.com

[2] Shumen Municipality, Shumen, Bulgaria, e-mail: hristov.2023@abv.bg

***Abstract**: This paper examines how the future ShumenTech Technology Park can practically perform the role of a regional hub for dual-use technologies and defense innovation. A conceptual-functional model is proposed, linking identified technological needs with research and development, prototyping, testing, pilot deployment and technology transfer through collaboration among SiT (Shumen Institute of Technology), universities, industry, Shumen Municipality and competent state institutions. Six priority technological areas are examined, together with their potential contribution to technological sovereignty, regional innovation capacity, Bulgaria's technological and economic security and, more broadly, national security.*

***Keywords:** ShumenTech, dual-use technologies, defense innovation, robotics, technology transfer, technological sovereignty, national security*

ШУМЕНТЕХ КАТО РЕГИОНАЛЕН ЦЕНТЪР ЗА ТЕХНОЛОГИИ С ДВОЙНА УПОТРЕБА И ОТБРАНИТЕЛНИ ИНОВАЦИИ В СИСТЕМАТА ЗА НАЦИОНАЛНА СИГУРНОСТ НА БЪЛГАРИЯ

Владислав Милков Генов[1], Христо Атанасов Христов[2]

[1] Катедра „Компютърни системи и технологии", Факултет „Артилерия, ПВО и КИС", Национален военен университет „Васил Левски", Шумен, Шумен, България, e-mail: vgenov70@gmail.com

[2] Община Шумен, Шумен, България, e-mail: hristov.2023@abv.bg

***Резюме**: Настоящият доклад разглежда как бъдещият технологичен парк ШуменТех може практически да изпълнява ролята на регионален център за технологии с двойна употреба и отбранителни иновации. Предлага се концептуално-функционален модел, който свързва идентифицираните технологични потребности с научноизследователска и развойна дейност, прототипиране, изпитване, пилотно внедряване и технологичен трансфер чрез взаимодействие между SiT (Shumen Institute of Technology), университети, индустрия, Община Шумен и компетентни държавни структури. Разглеждат се шест приоритетни технологични направления и техният потенциал за принос към технологичния суверенитет, регионалния иновационен капацитет, технологичната и икономическата сигурност на България и, в по-широк план, към националната сигурност.*

***Ключови думи:** ШуменТех, технологии с двойна употреба, отбранителни иновации, роботика, технологичен трансфер, технологичен суверенитет, национална сигурност*

Въведение

Развитието на изкуствения интелект (ИИ), автономните системи, роботиката и комуникационните технологии ускорява сближаването между гражданските разработки и приложенията в областта на сигурността и отбраната. Научно-технологичната стратегия на НАТО също поставя акцент върху ускореното внедряване на нововъзникващи технологии и тяхната роля за отбранителните способности и устойчивостта [8].

В предходно изследване бъдещият технологичен парк ШуменТех е разгледан като регионален иновационен център с потенциален принос към технологичната и икономическата сигурност на България чрез взаимодействие между образование, наука, индустрия, иновации и сигурност [1]. Настоящият доклад продължава тази научна линия, като премества фокуса от обосноваването на стратегическата роля на ШуменТех към въпроса как тази роля може да бъде реализирана практически чрез развитие и трансфер на технологии с двойна употреба и отбранителни иновации.

Научният проблем е как наличните образователни, научни, инженерни и индустриални компетентности да бъдат свързани в устойчив механизъм от технологична потребност до изпитано и приложимо решение. Механизми като Ускорителя на НАТО за отбранителни иновации за Северния Атлантик (DIANA) и Схемата на ЕС за отбранителни иновации (EUDIS) показват значението на връзката между иноватори, изпитвателна инфраструктура, технологично съзряване и крайни потребители [3], [4].

Целта на настоящия доклад е да се разработи и обоснове концептуално-функционален модел на бъдещия технологичен парк ШуменТех като регионален център за технологии с двойна употреба и отбранителни иновации, който чрез взаимодействие между образование, наука, индустрия, местна власт и държавни структури да осигурява среда за научноизследователска и развойна дейност, прототипиране, изпитване и технологичен трансфер на решения, приложими в гражданския сектор и в областта на сигурността и отбраната.

Основният изследователски въпрос е: как може бъдещият технологичен парк ШуменТех да бъде структуриран като регионален център за технологии с двойна употреба и отбранителни иновации, така че да осигурява ефективен преход от идентифицирана технологична потребност през научноизследователска и развойна дейност, прототипиране и изпитване до пилотно внедряване и практическо приложение в гражданския сектор и в областта на сигурността и отбраната?

Формулирана е хипотезата, че ако ШуменТех бъде развит чрез интегриран модел, който обединява приоритетни технологии с двойна употреба, научноизследователска и развойна инфраструктура и устойчив механизъм за взаимодействие между SiT, университетите, индустрията, Община Шумен и компетентните държавни структури, той може да съкрати пътя от технологична потребност до прототип, изпитване и пилотно внедряване и по този начин да допринася практически за отбранителните иновации, технологичния суверенитет и националната сигурност на България.

Изследването последователно разглежда теоретичната рамка, предлага концептуално-функционален модел с шест технологични направления, оценява ги по предварително определена система от критерии и анализира възможностите за интегрирана регионална технологична среда.

1. Технологии с двойна употреба и регионални отбранителни иновации

1.1. Технологии с двойна употреба

Технологиите с двойна употреба свързват гражданското технологично развитие с приложенията в областта на сигурността и отбраната. В Регламент (ЕС) 2021/821 изделията с двойна употреба са определени като изделия, включително софтуер и технологии, които могат да бъдат използвани както за граждански, така и за военни цели [2]. Макар определението да е формулирано в контекста на контрола на износа, то ясно установява основната характеристика на двойната употреба — възможността една и съща технологична основа да намира приложение в различни функционални среди.

В настоящото изследване понятието се използва в по-широк иновационен смисъл. Не е необходимо дадена технология да е разработена първоначално за военни цели, за да има значение за сигурността и отбраната. ИИ, роботиката, автономните системи, сензориката, комуникациите, киберсигурността и енергийните технологии могат да произхождат от граждански или индустриални приложения и впоследствие да се адаптират за наблюдение, защита на критична инфраструктура, устойчивост, логистика, ситуационна осведоменост или работа в опасна среда. Подобна логика следва и DIANA, която подпомага развитието, изпитването и валидирането на решения с двойна употреба [3].

Под регионални отбранителни иновации тук се разбира способността на регионална екосистема да идентифицира потребности, да мобилизира компетентности и да подпомага разработването, изпитването и трансфера на решения с приложение в областта на сигурността и отбраната, като използва взаимодействието с гражданската икономика.

1.2. Проблемът на технологичния трансфер

Наличието на научни знания, инженерни компетентности и технологични идеи **не гарантира практическо приложение**. Между идентифицирането на технологична потребност и внедряването на работещо решение стоят етапи на научноизследователска и развойна дейност, прототипиране, изпитване, валидиране, демонстрация и пилотно внедряване. Прекъсването на тази последователност може да остави перспективни разработки на ниво лабораторен резултат или прототип, без да достигнат до реален краен потребител.

Механизми като DIANA и EUDIS адресират именно този преход чрез достъп до изпитвателни среди, технологично съзряване, демонстрация и мащабиране [3], [4]. През 2026 г. по европейската програма AGILE за гъвкави и бързи отбранителни иновации е постигнато политическо споразумение с цел ускоряване на разработването, изпитването и внедряването на иновативни отбранителни решения; очаква се програмата да започне да функционира през 2027 г. [5].

Следователно основният проблем за регионален център като ШуменТех не е единствено какви технологии да бъдат развивани, а **как да бъде организиран устойчив процес**, който свързва реалната потребност с необходимите компетентности, разработването на решение, неговото изпитване и последващия технологичен трансфер. Върху решаването на този проблем е изграден предложеният по-долу концептуално-функционален модел.

2. Концептуален модел на ШуменТех за технологии с двойна употреба и отбранителни иновации

Предходното изследване разглежда ШуменТех като регионален иновационен център с потенциален принос към технологичната и икономическата сигурност и технологичния суверенитет на България [1]. Настоящият модел надгражда тази постановка чрез технологии с двойна употреба и технологичен трансфер.

Моделът организира иновационната среда около процес от идентифицирана потребност до проверено и приложимо решение, а не около изолирани лаборатории. Подобна процесна логика се наблюдава и при DIANA и EUDIS [3], [4].

2.1. Приоритетни технологични направления

В рамките на модела са определени шест **взаимосвързани направления**: роботика и роботизирани системи; безпилотни и автономни системи; изкуствен интелект и анализ на данни; киберсигурност и защита на индустриални системи; вградени системи, сензорика и комуникации; интелигентни енергийни системи и енергийна устойчивост. Подборът им се основава на потенциала за двойна употреба и технологична конвергенция и е съобразен със съответните приоритети в съвременните отбранителни и научно-технологични програми [3], [8].

Роботиката и роботизираните системи обхващат индустриални и колаборативни роботи, мобилни роботи, манипулатори, автономни наземни платформи, машинно зрение и системи за инспекция, логистика и работа в опасна среда. Хуманоидните (антропоморфни) платформи се разглеждат като биомиметична подкатегория, а не като самостоятелен инженерен дял, което е съвместимо с таксономиите на мобилната роботика [6]. Те са подходящи за задачи, изискващи мобилност и манипулация в среда, създадена за човека; публикации, свързани с DARPA Robotics Challenge, демонстрират такава приложимост при бедствия [7].

Безпилотните и автономните системи обхващат автономни платформи, навигация, управление, комуникации и сензорни полезни товари. Изкуственият интелект и анализът на данни осигуряват машинно зрение, разпознаване, прогнозна аналитика и автономно управление. Киберсигурността защитава свързаните информационни, индустриални и кибер-физични системи, при нарастващи европейски изисквания за киберустойчивост [9].

Вградените системи, сензориката и комуникациите осигуряват основата за физически прототипи, специализиран хардуер, интернет на нещата и обмен на данни. Интелигентните енергийни системи включват локално производство и

съхранение на енергия, управление на потреблението, микромрежи и резервираност. Шестте направления образуват обща технологична база, конфигурирана според конкретната задача.

2.2. Заинтересовани страни и модел за технологичен трансфер

Основните заинтересовани страни са SiT (Shumen Institute of Technology / Шуменски технологичен институт), университети и други образователни институции, индустриални компании, Община Шумен и компетентни държавни структури. При конкретни разработки могат да се включват научни организации, стартиращи предприятия, инвеститори, предприятия от отбранителната индустрия и оператори на критична инфраструктура.

Взаимодействието се разглежда като функционална иновационна мрежа: потребителите формулират потребностите; научните и образователните организации осигуряват знания и кадри; SiT и ШуменТех координират изследванията, разработването, прототипирането и изпитването; Община Шумен участва като регионален и институционален партньор; държавните структури се включват при задачи, свързани със сигурност, отбрана, критична инфраструктура или регулаторни изисквания.



Фигура 1. Концептуално-функционален модел на ШуменТех за развитие и технологичен трансфер на решения с двойна употреба.

Предложеният процес включва осем взаимно свързани етапа: идентифициране на технологична потребност, формулиране на технологична задача, научноизследователска и развойна дейност, прототипиране, изпитване и валидиране, пилотно внедряване, технологичен трансфер и мащабиране, както и практическо приложение. Ключова характеристика е обратната връзка между етапите: резултатите от изпитването могат да наложат промяна на прототипа, а

пилотното внедряване — прецизиране на изискванията. По този начин моделът се интерпретира като итеративен процес за намаляване на технологичния риск, а технологичният трансфер — като структурна функция, а не като последваща дейност след приключване на разработката.

3. Методика за оценка на предложения модел

За оценяване на приложимостта на определените технологични направления в рамките на концептуалния модел на ШуменТех се използва сравнителен подход, основан на система от предварително определени критерии. Оценява се не абсолютната значимост на технологията, а степента на съответствие с модела на ШуменТех.

Определени са шест критерия: K1 — стратегическа значимост; K2 — потенциал за двойна употреба; K3 — регионален капацитет, включващ наличието или реалистичната възможност за развитие на човешки ресурси, научни и образователни компетентности, индустриални партньорства и инфраструктура; K4 — принос към технологичния суверенитет; K5 — реализуемост на прототипирането и пилотното внедряване; K6 — потенциал за технологичен трансфер и мащабиране.

Всеки критерий се оценява по петстепенна скала: 1 — много ниска, 2 — ниска, 3 — средна, 4 — висока и 5 — много висока степен на съответствие. На настоящия концептуален етап шестте критерия се приемат с еднаква тежест. Така се избягва въвеждането на авторски определени различни тегла без предварително проведена формална експертна процедура.

$$S_j = \sum_{i=1}^{6} w_i \, x_{ij}$$

$$w_1 = w_2 = \ldots = w_6 = 1/6, \quad j = [1{:}6], \quad S_j = \frac{\sum_{i=1}^{6} x_{ij}}{6},$$

където x_{ij} е оценката на технологично направление j по критерий i, w_i е теглото на съответния критерий, а S_j е интегралната оценка на направлението. Получената стойност е в диапазона от 1 до 5.

Оценяването има характер на авторски аналитичен и концептуален анализ, основан на научна литература, официални документи и информация за регионалния капацитет. То не представлява представително експертно изследване; необходима е последваща независима валидация. Методиката оценява предпоставките за приложимост на модела, но не измерва пряко времето за преминаване от технологична потребност до пилотно внедряване. Технологичната зрялост следва да се оценява при конкретни прототипи и пилотни разработки.

4. Резултати и обсъждане

Прилагането на разработената методика към шестте приоритетни технологични направления води до резултатите в Таблица 1. Оценката характеризира не абсолютната значимост на съответната технология, а степента на съответствие с предложения функционален модел на ШуменТех.

Таблица 1. Сравнителна оценка на приоритетните технологични направления по избраните критерии

№	Направление	K1	K2	K3	K4	K5	K6	S_j
1	Роботика	4	5	4	4	4	5	**4,33**
2	Безпилотни системи	5	5	4	5	4	5	**4,67**
3	ИИ и анализ на данни	5	5	4	5	5	5	**4,83**
4	Киберсигурност	5	5	4	5	4	5	**4,67**
5	Вградени системи	4	5	5	5	5	5	**4,83**
6	Енергийни системи	4	5	3	4	3	4	**3,83**

Резултатите показват висока степен на съответствие на всички направления. Различията се определят главно от регионалния капацитет и реализуемостта на прототипирането и пилотното внедряване; по-ниска стойност на S_j не означава по-ниска стратегическа значимост.

Най-висока оценка S_j = 4,83 получават изкуственият интелект и анализът на данни и вградените системи, сензориката и комуникациите, поради хоризонталната им приложимост. Безпилотните и автономните системи и киберсигурността достигат S_j = 4,67, а роботиката — S_j = 4,33. При по-сложните роботизирани платформи необходимата интеграция на механика, електроника, управление, сензорика, комуникации и ИИ увеличава инфраструктурните изисквания.

Интелигентните енергийни системи получават S_j = 3,83, което отразява по-ограничена доказана регионална научноизследователска база и по-високи капиталови и регулаторни изисквания. Регионалният компонент се подкрепя от актуални образователни направления в НВУ „Васил Левски“ [10], документирана специализирана лабораторна и учебна база в Шуменския университет [11] и индустриална среда в областта на електрониката, информационните и комуникационните технологии, комуникационната техника и машиностроенето [12], [13], [14].

По-съществения резултат е, че шестте направления не следва да се разглеждат като шест независими структури. Анализът очертава интегрирана технологична архитектура, в която вградените системи, сензориката, комуникациите и изкуственият интелект формират базов технологичен слой; роботиката и автономните системи използват този слой при изграждането на приложни платформи; киберсигурността осигурява хоризонтална защита; а интелигентните енергийни решения повишават устойчивостта и автономността. Следователно ШуменТех следва да се развива като споделена среда за научноизследователска и развойна дейност, прототипиране и изпитване, а не като набор от изолирани лаборатории.

5. Приложни сценарии

Практическата приложимост на модела е илюстрирана с два примерни сценария, които не представляват конкретни проекти, а показват комбинирането на направленията и двойната употреба на обща технологична база.

5.1. Защита и устойчивост на индустриална инфраструктура

Първият сценарий е свързан с наблюдение, защита и повишаване на устойчивостта на индустриална инфраструктура. Технологичната потребност може да възникне при необходимост от ранно откриване на технически отклонения, наблюдение на труднодостъпни участъци, повишаване на киберустойчивостта или осигуряване на непрекъсваемост на критични процеси.

В рамките на модела могат да бъдат интегрирани сензорни и вградени системи за събиране на данни, алгоритми с изкуствен интелект за откриване на аномалии, роботизирани платформи за дистанционна инспекция, средства за защита на индустриални системи за управление и контрол и решения за локално управление и резервиране на енергийните ресурси. Разработката може първоначално да бъде проверена в лабораторна среда и след това да премине към ограничен пилотен проект в партньорство с индустриално предприятие. Същите базови компетентности могат да бъдат използвани и при защита на обекти и системи със значение за националната сигурност.

5.2. Наблюдение и реакция при кризисна и опасна среда

Вторият сценарий разглежда технологична потребност при природно бедствие, промишлена авария или друга среда, при която непосредственото човешко присъствие е затруднено или създава повишен риск. Безпилотни летателни апарати могат да осигуряват наблюдение на по-голяма територия, а мобилни роботизирани системи — инспекция в труднодостъпни или рискови зони. Сензорните системи и комуникационната инфраструктура осигуряват събирането и предаването на данни, а алгоритми за изкуствен интелект подпомагат тяхната обработка и откриването на обекти, събития или отклонения.

В рамките на направлението „Роботика и роботизирани системи“ могат да бъдат разглеждани и хуманоидни (антропоморфни) платформи, когато характеристиките на средата изискват придвижване и манипулация в пространства, първоначално проектирани за човек [7]. Те не представляват отделно направление, а специализиран вариант на роботизирана платформа, интегриращ механика, сензорика, управление и изкуствен интелект. От гледна точка на технологичния трансфер същата технологична основа може да бъде адаптирана за гражданска защита, индустриална инспекция, критична инфраструктура и приложения в областта на сигурността и отбраната.

И двата сценария показват, че стойността на модела произтича от комбинирането на технологиите около конкретна потребност и от общия процес на научноизследователска и развойна дейност, прототипиране, изпитване, пилотно внедряване и трансфер.

Заключение и бъдеща работа

Изследването надгражда предходно разглеждане на ШуменТех като регионален иновационен център с потенциален принос към технологичната и икономическата сигурност на България [1], като предлага практически модел за развитие, изпитване и трансфер на технологии с двойна употреба чрез взаимодействие между образователни и научни институции, индустрията, местната власт и държавните структури.

Сравнителната оценка по избраните критерии показва висока степен на съответствие на шестте направления. Важен резултат е взаимосвързаната технологична архитектура и възможността обща технологична основа да се адаптира към граждански и индустриални приложения, както и към приложения в областта на сигурността и отбраната.

Концептуалните резултати са в подкрепа на формулираната хипотеза, според която интегриран модел, обединяващ приоритетни технологии с двойна употреба, научноизследователска и развойна инфраструктура и устойчив механизъм за взаимодействие между SiT, университетите, индустрията, Община Шумен и компетентните държавни структури, може да създаде условия за по-кратък преход от технологична потребност до прототип, изпитване и пилотно внедряване. Настоящата методика не измерва пряко този времеви ефект и той следва да бъде проверен чрез пилотно приложение. В този смисъл ШуменТех може да бъде разглеждан не само като физическа инфраструктура, а като регионален механизъм за създаване, валидиране и трансфер на технологични решения с потенциален принос към отбранителните иновации, технологичния суверенитет и националната сигурност на България.

Основно ограничение на изследването е концептуалният характер на оценката и липсата на представително експертно проучване. Бъдеща работа следва да включва експертна валидация, детайлна лабораторна архитектура, избор на първи пилотен проект, изграждане на технологичен демонстратор и проверка на модела в реална среда.

Литература

1. Генов, В., & Матеева, Ц. (2026). Ролята на бъдещия технологичен парк ШуменТех като регионален иновационен център за технологичната и икономическата сигурност на България. Сборник доклади от научна конференция „Актуални проблеми на сигурността“, 7–8 май 2026 г., стр. 1229-1236. Велико Търново: Издателски комплекс на НВУ „Васил Левски“. ISSN 2367-7473.
2. Европейски парламент и Съвет на Европейския съюз. (2021). Регламент (ЕС) 2021/821 на Европейския парламент и на Съвета от 20 май 2021 година за въвеждане на режим на Съюза за контрол на износа, брокерската дейност, техническата помощ, транзита и трансфера на изделия с двойна употреба (преработен текст). Официален вестник на

Европейския съюз, L 206, стр. 1–461. https://eur-lex.europa.eu/eli/reg/2021/821/oj?locale=bg. [viewed 2026-09-04]

3. NATO. (2026, July 1). Defence Innovation Accelerator for the North Atlantic (DIANA). Retrieved from https://www.nato.int/en/about-us/organization/nato-structure/defence-innovation-accelerator-for-the-north-atlantic-diana. [viewed 2026-09-04]
4. European Commission, Directorate-General for Defence Industry and Space. (2026, March 15). EU Defence Innovation Scheme (EUDIS) Factsheet 2026. Retrieved from https://eudis.europa.eu/factsheet_en. [viewed 2026-09-04]
5. European Commission, Directorate-General for Defence Industry and Space. (2026, July 16). Commission welcomes political agreement on the Programme for agile and rapid defence innovation (AGILE). Retrieved from https://defence-industry-space.ec.europa.eu/commission-welcomes-political-agreement-programme-agile-and-rapid-defence-innovation-agile-2026-07-16_en. [viewed 2026-09-04]
6. Jahn, U., Heß, D., Stampa, M., Sutorma, A., Röhrig, C., Schulz, P., & Wolff, C. (2020). A taxonomy for mobile robots: Types, applications, capabilities, implementations, requirements, and challenges. Robotics, 9(4), 109. https://doi.org/10.3390/robotics9040109
7. DeDonato, M., Dimitrov, V., Du, R., Giovacchini, R., Knoedler, K., Long, X., Polido, F., Gennert, M. A., Padır, T., Feng, S., Moriguchi, H., Whitman, E., Xinjilefu, X., & Atkeson, C. G. (2015). Human-in-the-loop control of a humanoid robot for disaster response: A report from the DARPA Robotics Challenge Trials. Journal of Field Robotics, 32(2), p. 275–292. https://doi.org/10.1002/rob.21567
8. NATO. (2025). NATO Science & Technology Strategy. Retrieved from https://www.nato.int/content/dam/nato/webready/documents/sto/STO-strategy-2025.pdf. [viewed 2026-09-04]
9. Европейски парламент и Съвет на Европейския съюз. (2022). Директива (ЕС) 2022/2555 от 14 декември 2022 година относно мерки за високо общо ниво на киберсигурност в Съюза (Директива МИС 2). Официален вестник на Европейския съюз, L 333, стр. 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=bg. [viewed 2026-09-04]
10. Национален военен университет „Васил Левски“. (б.д.). Граждански специалности ОКС „Магистър“. https://www.nvu.bg/bg/специалности-магистри. [viewed 2026-09-04]
11. Шуменски университет „Епископ Константин Преславски“. (2018, 10 септември). Президентът на Република България разгледа три учебни зали. https://www.shu.bg/news-events/news/prezidentat-na-republika-balgariya-razgleda-tri-uchebni-zali/. [viewed 2026-09-04]
12. Община Шумен. (2026, 12 май). Кметът проф. Христо Христов: Шумен става икономическият център на Североизтока, разширяваме Индустриалния парк. https://www.shumen.bg/bg/novini/kmetat-prof-hristo-hristov-shumen-stava-ikonomicheskiyat-tsentar-na-severoiztoka-

razshiryavame-industrialniya-park (https://www.24chasa.bg/mneniya/article/20462871). [viewed 2026-09-04]

13. Община Шумен. (2026, 7 май). Шумен развива стратегическа платформа за дългосрочен икономически растеж и иновации. https://www.shumen.bg/bg/novini/shumen-razviva-strategicheska-platforma-za-dalgosrochen-ikonomicheski-rastezh-i-inovatsii/. [viewed 2026-09-04]
14. Община Шумен. (2026, 27 юли). Вицепремиерът и министър на икономиката, инвестициите и индустрията Александър Пулев и кметът на Шумен обсъдиха развитието на технологичен парк. https://www.shumen.bg/bg/novini/vitsepremierat-i-ministar-na-ikonomikata-investitsiite-i-industriyata-aleksandar-pulev-i-kmetat-na-shumen-obsadiha-razvitieto-na-tehnologichen-park. [viewed 2026-09-04]

APPLICATION OF SATELLITE COMMUNICATION SYSTEMS IN AIR DEFENSE

Yoana A. Pashkuleva

Air Defense Department, Artillery, Air Defense, Communication and Information Systems Faculty, National Military University „Vasil Levski", Shumen, Bulgaria
pashkulevaioana@gmail.com

Abstract: *This paper examines the critical role and practical application of satellite communication systems (SATCOM) within the architecture of modern network-centric air and missile defense systems. The integration of geographically dispersed sensors, radar complexes, and command posts to establish a Recognized Air Picture (RAP) is thoroughly analyzed. Special emphasis is placed on the operational advantages of Low Earth Orbit (LEO) satellite constellations for Beyond-Line-of-Sight (BLOS) command and control, as well as the coordination of mobile tactical air defense teams. Drawing on lessons learned from recent military conflicts (including the deployment of Link 16 protocols via satellite), the study identifies the primary vulnerabilities of the space segment, specifically electronic warfare (jamming and spoofing) and anti-satellite weapons (ASAT). Methods for enhancing communication resiliency are proposed, and future trends regarding the deployment of edge-computing artificial intelligence (AI) for orbital target filtering are outlined.*

Keywords: *satellite communications, SATCOM, air defense, network-centric operations, LEO constellations, BLOS control, electronic warfare, ASAT.*

ПРИЛОЖЕНИЕ НА САТЕЛИТНИТЕ КОМУНИКАЦИОННИ СИСТЕМИ В ПРОТИВОВЪЗДУШНАТА ОТБРАНА

Йоана А. Пашкулева

Катедра „Противовъздушна отбрана", факултет „Артилерия, противовъздушна отбрана, комуникационни и информационни системи", гр. Шумен към Национален военен университет „Васил Левски", България
pashkulevaioana@gmail.com

Резюме*: Настоящият доклад изследва критичната роля и практическото приложение на сателитните комуникационни системи (SATCOM) в структурата на съвременната мрежово-центрична противовъздушна (ПВО) и противоракетна отбрана (ПРО). Анализирана е интеграцията на географски разпръснати сензори, радарни комплекси и командни пунктове за изграждане на Единна картина на въздушната обстановка (RAP). Специално внимание е отделено на оперативните предимства на нискоорбиталните спътникови съзвездия (LEO) за управление извън линията на пряка видимост (BLOS) и координация на мобилни тактически групи. На базата на поуките от съвременните военни конфликти (включително прилагането на протоколи от типа Link 16 през сателит), са идентифицирани основните уязвимости на космическия сегмент, свързани с радиоелектронната борба (заглушаване и измама) и противоспътниковите оръжия (ASAT). Предложени са методи за повишаване на устойчивостта на връзките и са очертани*

бъдещите тенденции за внедряване на бордови изкуствен интелект (ИИ) за филтриране на целите в орбита.

Ключови думи: *сателитни комуникации, SATCOM, ПВО, мрежово-центрични операции, LEO съзвездия, BLOS управление, радиоелектронна борба, ASAT.*

1. Въведение

В съвременните високоинтензивни мрежово-центрирани военни конфликти системите за противовъздушна отбрана (ПВО) и противоракетна отбрана (ПРО) са изправени пред нови предизвикателства. Нисколетящите крилати ракети, маневриращите хиперзвукови комплекси и масивните рояци от автономни безпилотни летателни апарати изискват време за реакция и вземане на оперативни решения в рамките на няколко секунди, а понякога дори по-кратко. В тази динамична среда сателитните комуникационни системи (SatCom) се превръщат в жизненоважна структура на бойното поле — стратегическа, оперативна и тактическа свързаност между географски разпръснати сензори, мобилни командни постове и крайни огневи средства, непрекъснатост на командването и висока бойна ефективност.

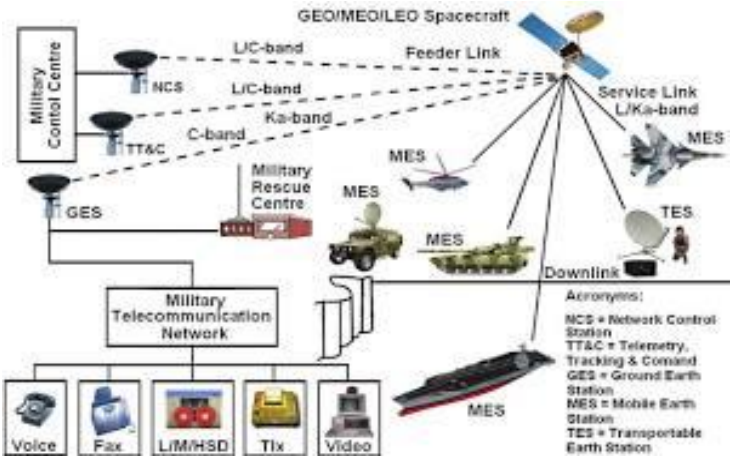
2. Архитектура на сателитния комуникационен канал в ПВО

Типичен сателитен канал в противовъздушната отбрана преминава през три основни етапа - наземна станция (радар или команден център), космически апарат (транспондер) и приемна наземна станция (система за ПВО). При симулиране на канала се вземат предвид три важни разрушителни фактора. На първо място, трябва да се има предвид, че средата на предаване не е вакуум, а има известна степен на шум в нея, второ, трябва да се вземе предвид, че системата е подложена на известни загуби от изтичане и трето, има и определени случайни смущения, които могат да бъдат генерирани по време на процеса на предаване.

2.1. Интеграция на сензори и радари в единна картина (Early Warning & C4ISR)

Основната функция на сателитните комуникации в структурата на противовъздушната отбрана е да прехвърлят радарна и телеметрична информация от отдалечени, предни или мобилни сензори към централизирани командни постове надеждно. Сателитният канал заобикаля терена, кривината на Земята и липсата на пряка видимост, които преди това ограничаваха наземните радиолинии (линии на пряка видимост). SatCom позволява пълна интеграция на данни в реално време, така че да може да се изгради RAP (т.нар. Разпозната въздушна картина). Космическите компоненти и сателитите за ранно предупреждение с високо чувствителни инфрачервени сензори откриват топлинния подпис на изстреляни балистични и крилати ракети в началната (активна) фаза на траекторията веднага след изстрелването и предават тази информация чрез сателитна връзка към наземните сили, давайки им ценно допълнително време за активиране на комплекси за противоракетна отбрана. Типичният сателитен канал в

противовъздушната отбрана преминава през три етапа: наземна станция (радар или команден център), космически апарат (транспондер) и приемаща наземна станция (SAM).[1]



Фиг. 1

2.2. Тактическо управление на огневите средства (Command and Control - C2)

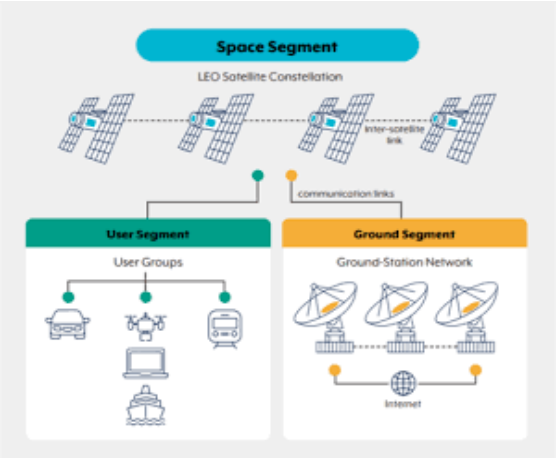
Сателитната свързаност е ключов фактор за реализиране на управление извън линията на видимост (BLOS). В тактиките за оцеляване системите за противовъздушни ракети (AAMS) и пусковите установки често са разположени далеч от основните радари и командни постове, за да се намали тяхната уязвимост към противорадарни ракети и артилерийски огън. Сателитният канал позволява сигурно предаване на команди за насочване и разрешения за стрелба от командния пост директно до отдалечената пускова установка (сигурно предаване). Това приложение е също много важно за координацията на силно разпръснати и силно мобилни малки огневи групи с преносими ПАМС или мобилни противовъздушни оръдия — чрез малки, силно мобилни сателитни терминали тези екипи получават актуални координати на целите, така че да не се случва приятелски огън върху въздушни обекти и да могат да се организират ефективни противовъздушни засади в труден терен.[1]

2.3. Приложение на съзвездия в ниска околоземна орбита (LEO Constellations)

Технологичната еволюция в космоса се е преместила от тежки GEO сателити (традиционни) към големи съзвездия от микросателити в ниска земна орбита (LEO). Военните приложения на системи като Starlink, OneWeb и специализирани мрежи на DARPA (проект Blackjack) променят архитектурата на

военните комуникации. Основните предимства на LEO съзвездията за противовъздушна отбрана са:

- Изключително ниска латентност: LEO мрежите имат забавяне на сигнала от 20–40 ms (GEO сателити >500 ms), което е необходимо за пренос на данни при прихващане на хиперзвукови цели.
- Висока пропускателна способност: Способността бързо да се прехвърлят големи обеми от радарни потоци, подробни цифрови карти и видео с висока резолюция от разузнавателни дронове.
- Оцеляване и устойчивост: Тъй като съзвездието се състои от стотици или хиляди взаимозаменяеми сателити, унищожаването (или заглушаването) на няколко от тях не унищожава работата на цялата мрежа, защото трафикът автоматично се пренасочва през съседни орбити.



Фиг. 2

2.4. Осигуряване на устойчивост и резервиране на връзките (SATCOM Resiliency)

При пълномащабни военни операции наземната комуникационна инфраструктура (подземни оптични кабелни маршрути, стационарни ретранслаторни кули и клетъчни връзки) са сред първите цели за унищожаване от конвенционални далекобойни оръжия и кибератаки. [3]Сателитните комуникации тогава са основният независим резервен канал (Failover System). Съвременните терминали за противовъздушна отбрана имат функции за автоматично превключване на трафика към сателитни ресурси веднага щом засекат влошаване или прекъсване на основната наземна връзка, така че сензорите и средствата за огън да останат в единната тактическа мрежа, дори ако регионалната инфраструктура е напълно унищожена

3. Практически примери от съвременни военни конфликти

3.1. Военно-технически изводи за практиката на ПВО

Адаптивна времева интеграция: Тъй като съществуват статистически флуктуации, цифровите приемници в противовъздушната отбрана не трябва да вземат оперативни решения, базирани на единични измервания. Необходима е дългосрочна цифрова филтрация, за да се получи надеждна оценка на канала.

Устойчивост на електронна война: Моделирането на високи нива на шум (σ = 0.5) ни позволява количествено да предвидим поведението на връзката при активно заглушаване от врага.

Компенсация на Доплер: Експериментите показват, че честотното отместване предсказуемо измества спектралния пик на сигнала (например от 1.00 kHz до приблизително 1.32 kHz), така че фазово заключени контури трябва да бъдат внедрени в реални системи за противовъздушна отбрана по подразбиране.

3.2. Поуки и опит от войната в Украйна:

Реалните бойни операции в Украйна практически показаха, че търговските и специализираните нискоорбитални сателитни мрежи са жизненоважни за оцеляването и ефективността на противовъздушната отбрана. Компактни сателитни терминали бяха използвани от мобилни огневи групи, патрулиращи с преносими зенитно-ракетни комплекси и зенитни оръдия, за да изградят децентрализирана мрежа за ранно предупреждение: те получават данни за курсове, височини и скорости (в реално време) на таблети и полеви терминали за приближаващи руски крилати ракети и дронове „Камикадзе“ (Shahed-136) — къде да заемат позиции предварително по траекторията на полета на заплахите, за да ги ангажират ефективно, дори когато основните радари на големите системи за противовъздушна отбрана са изключени, за да се защитят от вражески противорадарни ракети.

3.3. Интегрирани системи на НАТО (Link 16 през спътник):

В НАТО обменът на тактическа информация в реално време се извършва чрез тактическата мрежа Link 16. Обикновено тя работи в ултрависокочестотния (UHF) диапазон и е ограничена до пряка видимост между платформите (самолети, кораби, наземни батареи). Разработен е протоколът Satellite Link 16 / S-Link 16, който преодолява тези ограничения, така че стратегическите разузнавателни платформи (AWACS самолети за дългосрочно откриване и контрол на радара; стратегически безпилотни летателни апарати RQ-4 Global Hawk) могат директно да комуникират данни за въздушната ситуация с наземни батареи за противовъздушна отбрана на хиляди километри разстояние (Patriot, NASAMS или SAMP/T), осигурявайки глобално насочване извън хоризонта.[2]

4. Основни предизвикателства, уязвимости и противодействие

4.1. Радиоелектронна борба (РЕБ):

Въпреки всичките си големи предимства, сателитният комуникационен канал все още е много уязвим към средства за електронна война (EW). Противникът

използва два основни начина на въздействие. Първият е заглушаване. Изпращат се мощни смущаващи сигнали в честотния диапазон на сателита. Заглушаването може да бъде на възходящата връзка (приемникът на самия сателит в орбита заслепява транспондера за цял регион) и на низходящата връзка (локално насочено към наземни антени и терминали на комплекси за противовъздушна отбрана, блокиращи приемането на полезна информация). Съществува производство на фалшиви сателитни или GPS/GNSS сигнали, които заместват координатите на мобилни системи за противовъздушна отбрана или въвеждат времеви десинхронизации в цифрови приемници, така че траекториите на прихващане не могат да бъдат точно изчислени.[4]

4.2. Физически заплахи и противосателитни оръжия (ASAT)

Водещите световни сили вече официално разглеждат Космоса като самостоятелна среда за водене на бойни действия. Това излага сателитната инфраструктура на пряка опасност от противосателитни системи (Anti-Satellite – ASAT). Те включват кинетични ракети с наземно и въздушно базиране за унищожаване на сателити в ниска околоземна орбита, както и оръжия с насочена енергия (наземни лазери), способни да заслепят оптиката или да извадят от строя чувствителната бордова електроника.[4]

4.3. Технически методи за защита на връзките

За да се борят с тези заплахи, съвременните военни сателитни системи имат напреднали технологични архитектури: - **FHSS (Frequency-Hopping Spread Spectrum):** технология за бързо псевдослучайно прескачане на носещата честота хиляди пъти в секунда, така че сигналът да е изключително труден за прихващане и заглушаване от врага.[3]

- **Фазирани антенни решетки (AESA / PESA):** Наземните терминали използват адаптивно формиране на лъча — електронно насочват тесен мощен лъч директно към сателита, като софтуерно отслабват и „нулират" посоките, от които идва наземната интерференция от станции за електронна война.

- **Тежко криптиране:** Напреднали криптографски алгоритми според военните стандарти на NSA (Тип 1 криптиране), така че никой да не може да проникне в него, да подслушва или да вмъква фалшиви данни в командната верига на противовъздушната отбрана.

5. Бъдещи тенденции

Интеграция на Изкуствен интелект (ИИ) в SatCom

Основно направление в технологичното развитие е внедряването на алгоритми с Изкуствен интелект (ИИ) и машинно обучение директно на борда на спътниците (Edge Computing в орбита). Интегрираният бордови ИИ ще позволява автоматизирано филтриране на фалшиви цели, причинени от метеорологични явления или активни смущения от РЕБ, като към наземните командни пунктове на ПВО ще се предава само валидирана, пречистена и класифицирана информация за реалните заплахи. Също така ИИ софтуер в наземните терминали ще може

автономно и в реално време да открива опити за смущения и да превключва честотите или доставчиците на сателитни услуги още преди операторът да е отчел деградация на връзката.

6. Заключение

Космическото пространство вече не е просто пасивна среда за стратегическо наблюдение и разузнаване, а се е превърнало в основен и критичен гръбнак на тактическата наземна Противовъздушна отбрана. В епохата на хиперзвуковите оръжия и координираните рояци от дронове, ефективността на ПВО е правопропорционална на скоростта и сигурността на нейните комуникации. Без надеждни, високоскоростни и защитени сателитни връзки съвременната противовъздушна отбрана губи своята динамика, обсег и способност за мрежова координация, което подчертава необходимостта от постоянен национален и съюзен фокус върху развитието и защитата на военния космически капацитет.

Литература

1. Space Development Agency (SDA). Proliferated Warfighter Space Architecture (PWSA) Technical Overview and Operational Capabilities. Washington, D.C.: Department of Defense, 2023.
2. 2. NATO Standardization Office (NSO). STANAG 5516: Tactical Data Exchange - Link 16. Brussels: NATO Imagery and Data Interoperability Architecture, 2022.
3. 3. National Security Agency (NSA) & Australian Cyber Security Centre (ACSC). Joint Guidance on Low Earth Orbit (LEO) SATCOM System Risks and Mitigations. Cybersecurity Advisory, 2024.
4. 4. Center for Strategic and International Studies (CSIS). Space Threat Assessment: Counterspace Capabilities and Electronic Warfare. Washington, D.C.: CSIS Missile Defense Project, 2023.

CYBERSECURITY AND ARTIFICIAL INTELLIGENCE

CALIBRATED DIPLOMACY - A TIERED RESPONSE FRAMEWORK FOR CYBERSECURITY INCIDENTS UNDER ATTRIBUTION UNCERTAINTY

Marius Iulian Mihailescu[1], Stefania Loredana Nita[2], Valentina Marascu[1,3]
Laurentiu Bogdan Asalomia[4]

[1]Faculty of Engineering and Computer Science, Spiru Haret University, Bucharest, Romania, m.mihailescu.mi@spiruharet.ro
[2]Faculty of Information Systems and Cyber Security, Military Technical Academy "Ferdinand I", Bucharest, Romania, stefania.nita@mta.ro
[3]National Institute for Laser, Plasma and Radiation Physics Magurele, Romania; Faculty of Mathematics and Computer Science, Bucharest University, Bucharest, Romania, v.marascu.mi@spiruharet.ro
[4]Northern Marine Management Limited, Glasgow, Scotland, United Kingdom; e-mail: asalomiabogdan@yahoo.com

Abstract *International responses to state-sponsored cyberattacks continue to display an uneasy gap between what technical attribution can establish and how governments choose to act on it: existing frameworks tend to treat attribution as a binary threshold rather than a graded judgment, leaving policymakers either paralyzed by residual uncertainty or free to select a response with little visible reference to the strength of the underlying evidence. This paper develops a tiered diplomatic response framework that instead treats attribution as a graded confidence variable, mapping forensic, signals-intelligence, and behavioral indicators onto a corresponding spectrum of diplomatic instruments ranging from private démarches and Track 1.5 dialogue to public attribution, coordinated sanctions, and multilateral condemnation. The framework is formalized through a composite confidence score and tested against a comparative analysis of five incidents between 2014 and 2021 — the Sony Pictures breach, WannaCry, NotPetya, the SolarWinds compromise, and the Microsoft Exchange/Hafnium intrusion — in which attribution confidence and response intensity are shown to diverge more often, and more substantially, than existing accounts acknowledge. The comparison isolates two recurring patterns: response lag, in which accountability measures trail public attribution by months or years, and response-magnitude mismatch, in which incidents attributed with comparable confidence receive markedly different treatment. Building on these findings, the paper proposes concrete steps for institutionalizing attribution-to-response protocols within multilateral venues, directed in particular at the United Nations' newly established Global Mechanism on ICT security, offering policymakers a more calibrated and evidence-linked basis for responding to state-linked cyber incidents.*

Keywords*: cyber diplomacy, attribution, escalation management, state-sponsored cyberattacks, deterrence, international cyber norms*

Introduction

Over the past decade, state-sponsored cyber operations have moved from a specialized concern of technical incident responders to a recurring subject of head-of-state statements, treasury sanctions, and United Nations negotiations. Incidents such as the 2017 NotPetya attack and the 2020 SolarWinds compromise are now treated less as intrusions to be remediated than as foreign-policy events to be answered. Yet the two halves of that response — determining who is responsible, and deciding what to do about

it — remain governed by largely separate logics. Forensic and intelligence communities have grown comfortable describing attribution as a matter of confidence levels. Diplomatic practice, by contrast, still tends to behave as though attribution were a switch: either a government is prepared to say who did it, or it is not.

This mismatch produces two related pathologies. When attribution evidence is genuinely ambiguous, governments often default to silence or private signaling, forgoing any public response even where the underlying activity is serious. When attribution is confident, the response that follows appears to depend as much on bilateral relationships, sanctions bandwidth, and diplomatic timing as on the strength of the evidence itself. As Section 3 shows, two incidents attributed with comparable confidence and by comparable multilateral coalitions — the SolarWinds compromise and the Microsoft Exchange/Hafnium intrusion, attributed months apart in 2021 — received strikingly different treatment: one triggered same-day sanctions and expulsions, the other only a joint statement of condemnation. If confidence does not reliably predict response intensity, the signal that serious evidence produces serious consequences is considerably weaker than it appears.

This paper argues that the gap between attribution and response can be narrowed, though not eliminated, by making the relationship between them explicit. It develops a tiered response framework that formalizes attribution confidence as a composite score built from forensic, signals-intelligence, and behavioral indicators, and maps the resulting confidence tiers onto an ordered spectrum of diplomatic instruments. It tests the framework against a comparative analysis of five incidents spanning 2014 to 2021, and closes with proposals for institutionalizing attribution-to-response protocols within multilateral venues, including the United Nations' new Global Mechanism on ICT security. The contributions are threefold: a confidence-to-response mapping model integrating attribution methodology with diplomatic signaling theory; a comparative case analysis of how confidence has aligned, or failed to align, with response intensity; and policy recommendations for institutionalizing the resulting protocols.

Section 1 reviews the attribution and diplomatic-response literatures and identifies the gap between them. Section 2 presents the tiered response framework, including its formal confidence score and the resulting mapping. Section 3 applies the framework to five incidents and identifies two recurring patterns of mismatch. Section 4 translates these findings into policy recommendations directed at the UN's new Global Mechanism. Section 5 discusses the framework's limitations, and the conclusion summarizes the paper's contribution.

1 Background and Related Work

1.1 The Attribution Problem in Cyberspace

Attribution — determining who is responsible for a cyber intrusion — is frequently described as one of the hardest technical problems in the field, dependent on forensic artifacts that can be spoofed, false-flagged, or simply absent. Rid and Buchanan's influential reframing argues that this framing is itself misleading: attribution is not a single yes/no puzzle but an iterative process in which analysts move from a broad universe of possible actors toward a narrower set of plausible ones, drawing on evidence

of very different kinds and reliability (Rid & Buchanan, 2015). Three categories of indicator recur across the incidents examined here. Forensic indicators — malware code reuse, shared infrastructure, compilation artifacts — are technically verifiable but can in principle be fabricated by an adversary seeking to implicate a third party. Signals-intelligence indicators are often the most probative evidence available, but the least amenable to public disclosure, since revealing them risks exposing sources and methods. Behavioral indicators — targeting pattern, consistency with known strategic objectives, timing relative to political events — are the least individually conclusive but often what allows analysts to move from a plausible technical match to a confident attribution. No single category is sufficient on its own.

1.2 Diplomatic Instruments for Cyber Incident Response

Once attribution is made, however tentatively, states have available a wide and increasingly well-populated menu of response instruments. At the least escalatory end are private diplomatic channels: démarches delivered through an embassy, or Track 1.5 dialogues that let states signal displeasure without any public acknowledgment that an incident occurred. Further along the spectrum are public but non-attributive technical advisories, followed by formal government attribution, first unilateral and increasingly joint or multilateral. At the most escalatory end sit instruments with material consequences: criminal indictments, targeted financial sanctions, diplomatic expulsions, and coordinated multilateral sanctions regimes. Nye's account of deterrence and dissuasion in cyberspace is useful here: attribution difficulties, often treated as fatal to cyber deterrence, in fact constrain only one of several available mechanisms — punishment — while leaving denial, entanglement, and normative shaming largely intact (Nye, 2017). International lawyers have separately examined which instruments can be justified as lawful countermeasures under the law of state responsibility, a question this paper treats as adjacent rather than central to the diplomatic calibration problem it addresses.

1.3 Gaps in Existing Frameworks

What is largely missing from both literatures is an explicit bridge between them. The attribution literature offers increasingly sophisticated accounts of how confidence is built, but stops short of specifying what a given confidence level should imply for the response that follows. The response literature offers rich typologies of the instruments available to states, but treats the choice among them as a function of political will or legal permissibility, with attribution confidence entering, if at all, as a background precondition rather than a variable that scales the response. Even empirical surveys of cyber conflict behavior that treat response as a graded, comparative phenomenon rarely connect response intensity systematically back to the strength of the attribution that preceded it. The framework developed next is intended to fill that gap.

2 A Tiered Response Framework

2.1 Attribution Confidence Tiers

The framework collapses the indicators reviewed in Section 1.1 into three confidence tiers. The Contested tier describes cases in which forensic evidence is present but

disputed, uncorroborated, or actively challenged by credible technical analysts, as occurred in parts of the private security community's response to the Sony Pictures attribution in December 2014. The Presumptive tier describes cases in which forensic and behavioral indicators converge on a single plausible actor and at least one government is prepared to attribute the activity, but corroboration by independent allied governments remains partial. The High tier describes cases in which forensic, signals-intelligence, and behavioral indicators converge and the attribution is corroborated by multiple independent governments acting without coordination — the position reached by the Five Eyes governments' joint attribution of NotPetya to Russia's GRU in February 2018. These tiers are not fixed; a case can migrate from Contested to High as investigation proceeds, and several incidents in Section 3 did exactly that.

2.2 The Diplomatic Response Spectrum

The response side of the framework orders the instruments from Section 1.2 along a single escalatory spectrum: (I) private démarche or Track 1.5 signaling; (II) public, non-attributive technical advisory; (III) unilateral government attribution; (IV) joint or multilateral attribution; (V) criminal indictment; and (VI) targeted or coordinated sanctions and diplomatic expulsions. These positions are not strictly cumulative — some incidents proceed directly from silence to sanctions — but they provide a common ruler against which responses to different incidents can be compared, the analytical purpose they serve in Section 3.

2.3 The Confidence-to-Response Mapping Model

The central claim of the framework is that confidence tier and response position should be predictably related, and departures from this relationship are informative. Each incident is assigned a composite confidence score C combining a forensic score F, a signals-intelligence score S, and a behavioral score B, each normalized to [0,1] and weighted by coefficients α, β, and γ reflecting the evidentiary weight assigned by attributing governments:

$$C = \alpha F + \beta S + \gamma B \tag{1}$$

with α + β + γ = 1. Incidents scoring below 0.40 fall into the Contested tier, those between 0.40 and 0.75 fall into the Presumptive tier, and those above 0.75 fall into the High tier.

Figure 1 illustrates the resulting mapping. A Contested-tier incident should not travel past private signaling or a non-attributive advisory; a Presumptive-tier incident may reasonably proceed as far as unilateral or joint attribution; and only a High-tier incident, ideally corroborated by multiple independent parties, should be a candidate for indictments or coordinated sanctions.

The framework is agnostic about which weights a government assigns to α, β, and γ; the goal is to make the weighting explicit enough that the resulting tier, and the response that follows from it, can be compared across incidents, the task taken up next.

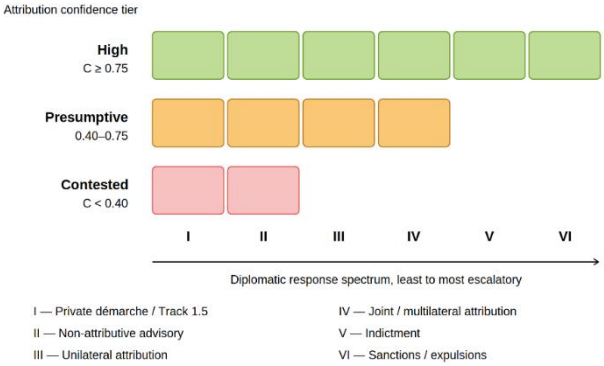


Figure 1: Confidence-to-response mapping in the tiered diplomatic framework. Source: authors.

3 Comparative Case Analysis

To test the framework against practice, this section applies it to five incidents attributed to state or state-directed actors between 2014 and 2021: the Sony Pictures breach, WannaCry, NotPetya, the SolarWinds compromise, and the Microsoft Exchange/Hafnium intrusion. The five vary along the dimensions the framework tracks: three different attributed states, attributions ranging from single-government to eight-government-plus-NATO-and-EU statements, and responses ranging from same-day sanctions to condemnation with no further action. Table 1 summarizes each case; the discussion below highlights two patterns the comparison makes visible.

Table 1: Attribution confidence and diplomatic response across five incidents, 2014–2021

Incident (year)	Attributed to	Confidence basis	Response instrument(s)	Attribution–response lag
Sony Pictures (2014)	North Korea (RGB)	High; contested by some analysts	Sanctions: 3 entities, 10 individuals	~2 weeks
WannaCry (2017)	North Korea (Lazarus / RGB)	High (5 governments)	Condemnation only; named sanctions +21 mo.	Same day / +21 months
NotPetya (2017)	Russia (GRU / Sandworm)	High (Five Eyes)	Condemnation; indictment +2.5 yr.	+8 months / +2.5 years
SolarWinds (2020)	Russia (SVR / APT29)	High (US + UK)	Sanctions + expulsions, same day as attribution	Same day
MS Exchange / Hafnium (2021)	China (MSS)	High (8 states + NATO/EU)	Condemnation only; no sanctions to date	No dedicated response

The first pattern is response lag: a substantial gap between public attribution and the deployment of instruments with material consequences. WannaCry is illustrative. The United States, joined by the United Kingdom, Australia, Canada, and New Zealand, publicly attributed the attack to North Korea's Lazarus Group in December 2017, within seven months of the attack (The White House, 2017). Yet the U.S. Treasury did not sanction Lazarus Group and its sub-units Bluenoroff and Andariel by name until September 2019 — close to two years after the attribution (U.S. Department of the Treasury, 2019). NotPetya shows a similar pattern further along the spectrum: the United Kingdom and United States attributed the attack to Russia's GRU in February 2018, but the indictment naming six specific GRU officers did not follow until October 2020 (U.S. Department of Justice, 2020). In both cases, public attribution moved quickly once confidence was established, while the material instruments further along the spectrum lagged well behind it.

The second and more striking pattern is a mismatch in response magnitude between incidents of comparable confidence. The clearest instance is the contrast between SolarWinds and Microsoft Exchange/Hafnium, attributed three months apart in 2021. Both were attributed with what the framework codes as High confidence: SolarWinds by a joint U.S.–U.K. statement corroborated by CISA, NSA, and FBI advisories, naming Russia's SVR (Cybersecurity and Infrastructure Security Agency, 2021); Exchange/Hafnium by a considerably larger coalition — the United States, the European Union, NATO, the United Kingdom, Australia, Canada, Japan, and New Zealand — naming China's Ministry of State Security and the Hafnium actor Microsoft had identified months earlier (American Journal of International Law, 2021). Despite the broader coalition, the two produced markedly different responses. SolarWinds triggered, the same day as the formal attribution, a presidential executive order, Treasury sanctions on Russian technology firms, and the expulsion of Russian diplomats. The Exchange/Hafnium attribution produced a joint statement of condemnation and an unrelated indictment of four individuals for separate hacking activity, but no sanctions tied to the Exchange intrusion itself. Under the framework, both incidents should occupy comparable positions on the response spectrum; in practice they occupied very different ones — a divergence the mapping model treats as a case requiring explanation, not noise to be discarded.

Neither pattern is fully explained by evidentiary uncertainty, which suggests attribution confidence, while necessary, is not sufficient to predict response intensity. Response lag appears partly attributable to the institutional distance between the offices that issue attribution statements and those that build criminal or financial cases, which proceed on independent, typically slower timelines. Response-magnitude mismatch appears to reflect considerations the confidence score does not capture: remaining sanctions capacity — North Korea and Russia were already subject to extensive sanctions regimes, arguably reducing the marginal deterrent value of additional measures — and competing bilateral priorities, most visibly with Exchange/Hafnium, where the broader U.S.–China economic relationship plausibly counseled against sanctions that would have been a comparatively low-cost addition to the existing Russia regime. These

are not flaws in the case for calibration; they are precisely the considerations Section 4 argues should be made explicit within an institutionalized protocol.

4 Policy Recommendations

4.1 Institutionalizing Attribution-to-Response Protocols

The case analysis suggests the mismatch between attribution and response is not primarily a technical problem to be solved with better forensics, but an institutional one: the confidence tier reached by attributing governments and the response instrument ultimately selected are decided by different offices, on different timelines, without a shared reference point connecting the two. The most direct remedy is to pre-commit, before any incident occurs, to a default mapping between confidence tier and response category similar to Section 2's — not a rigid formula that removes discretion, but a stated baseline from which departures require justification. A complementary step is a confidence-disclosure norm: when governments issue a public attribution, they would indicate, in general terms, which categories of evidence — forensic, signals-intelligence, behavioral — underpin the assessment, without disclosing specific sources or methods. This would let outside observers situate a given attribution within the tiered framework, making the confidence-to-response relationship auditable in a way it currently is not.

4.2 The UN Global Mechanism as an Implementation Venue

These proposals are more likely to gain traction as confidence-building measures within an existing multilateral process than as a freestanding initiative, and the relevant venue is currently in transition. The Open-Ended Working Group on ICT security, which ran from 2021 to 2025, concluded in July 2025 with a consensus final report establishing a new, permanent Global Mechanism on ICTs in the context of international security and advancing responsible state behaviour (United Nations, 2025). The Global Mechanism held its organizational session in March 2026 and convenes its first substantive plenary session in July 2026, with two dedicated thematic groups — one on general ICT security challenges, the other on capacity-building — beginning work later in the year. The general ICT security challenges group is a natural point of entry for the proposals above: neither requires new binding law, both are consistent with the voluntary, non-binding character of the confidence-building measures the OEWG process has favored to date, and both are pitched at the level of state practice rather than treaty text.

5 Discussion and Limitations

The framework has real limits. Assigning numerical weights to forensic, signals-intelligence, and behavioral indicators necessarily involves interpretive judgment, particularly for the signals-intelligence component, the least publicly observable of the three. The framework is also built primarily from the practice of the United States and its close allies, the states most likely to issue public attributions in the first place; whether it generalizes elsewhere, or to the binding-convention model favored by states such as Russia and China in the OEWG negotiations, is an open question. Finally, the five-incident comparison, while deliberately varied, remains a small sample of well-documented, publicly attributed cases; incidents that never receive public attribution at

all — plausibly the majority of state-sponsored activity — are invisible to this kind of analysis by construction.

Conclusion

This paper set out to address a persistent mismatch in how states respond to state-sponsored cyberattacks: the tendency to treat attribution as a binary threshold rather than a graded judgment that should scale the response that follows. It developed a tiered response framework that formalizes attribution confidence as a composite score and maps the resulting tiers onto an ordered spectrum of diplomatic instruments, and tested it against five incidents attributed between 2014 and 2021. The comparison surfaced two recurring patterns — response lag and response-magnitude mismatch — most starkly illustrated by the SolarWinds and Microsoft Exchange/Hafnium contrast. Building on this analysis, the paper proposed a default confidence-to-response mapping and a confidence-disclosure norm, directed at the United Nations' newly established Global Mechanism on ICT security, which convenes its first substantive session as this paper goes to press. Tighter coupling between attribution confidence and diplomatic response will not resolve the underlying disagreements among states about how cyberspace should be governed, but it would make the response states choose more legible, more comparable, and more credible as a source of deterrence.

References

1. American Journal of International Law. (2021). United States joins with allies, including NATO, to attribute malicious cyber activities to China. American Journal of International Law, 115(4), 715–721. https://doi.org/10.1017/ajil.2021.54
2. Cybersecurity and Infrastructure Security Agency. (2021, April 15). Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations (Alert AA20-352A). Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a
3. Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. International Security, 41(3), 44–71.
4. Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1–2), 4–37.
5. United Nations, Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. (2025). Final report (A/AC.292/2025/L.1). Retrieved from https://digitallibrary.un.org/record/4084927
6. U.S. Department of Justice, Office of Public Affairs. (2020, October 19). Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in cyberspace [Press release]. Retrieved from https://www.justice.gov/archives/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

7. U.S. Department of the Treasury. (2019, September 13). Treasury sanctions North Korean state-sponsored malicious cyber groups [Press release]. Retrieved from https://home.treasury.gov/news/press-releases/sm774
8. The White House. (2017, December 19). Press briefing on the attribution of the WannaCry malware attack to North Korea. Retrieved from https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

IMPROVING BLUE TEAM THREAT HUNTING CAPABILITIES THROUGH CYBER DEFENSE EXERCISES

Radostin S. Dimov

Cybersecurity and Information Technology Section, National Military University "Vasil Levski", Shumen, Bulgaria, rsdimov95@gmail.com

***Abstract**: Cyber defense exercises expose analysts to realistic adversarial behavior, time pressure, and coordination requirements that are difficult to reproduce through conventional classroom training. This paper proposes a methodology for using repeated cyber defense exercises as a continuous process for developing threat hunting capabilities. The approach is motivated by the participation of the Artillery, Air Defense and CIS Faculty in various exercises between 2020 and 2026, including Locked Shields, Cyber Coalition, Bulgarian Rose, and the CyberShockwave series. The proposed model defines two metrics that can be collected across different exercises: detection coverage and detection latency. A closed-cycle methodology links exercise objectives, telemetry collection, threat hunting, measurement, gap prioritization, and updated training. The model provides a structured basis for converting lessons identified during exercises into measurable and repeatable Blue Team threat hunting training.*

***Keywords:** Blue Team, Threat Hunting, Cyber Exercise, Adversary Emulation, Red Team, Cyber Range*

Introduction

Threat hunting is a proactive, analyst-driven activity used to identify malicious behavior that may not be exposed by isolated alerts or signature-based detection. It requires analysts to form hypotheses, investigate endpoint and network evidence, and correlate observations across available telemetry. The systematic review by (Mahboubi, et al., 2024) highlights the need for repeatable methodologies, appropriate data sources, and analyst expertise in practical threat hunting. These requirements make continuous hands-on training important for defensive teams.

Cyber defense exercises provide a suitable environment for such training because they expose participants to realistic adversarial behavior, incomplete information, time pressure, and coordination requirements. Cyber ranges support controlled execution of attack and defense scenarios without exposing operational systems (Yamin, Katt, & Gkioulos, 2020). Research on authentic cyber range training also shows that exercise value depends not only on scenario realism but on whether the intended learning outcomes can be evaluated systematically (Glas, Vielberth, & Pernul, 2023).

Repeated participation is especially valuable because capability development is not completed in a single event. Lessons from one exercise should influence the hunting hypotheses, telemetry requirements, analyst tasks, and training objectives used in the next. (Maennel, Ottis, & Maennel, 2017) demonstrated the value of timestamp-based measurements for evaluating technical cyber defense exercises, while (Yamin & Katt, 2022) describe cyber exercise preparation, execution, evaluation, and repetition as parts of an iterative process.

The Artillery, Air Defense and CIS Faculty (AADCF) at the National Military University "Vasil Levski" has accumulated practical experience through various cyber defense exercises between 2020 and 2026, including Locked Shields, Cyber Coalition, the CyberShockwave series, and the national Bulgarian Rose and Shadow Strike exercises. Cyber defense exercises differ substantially in technical depth, scenario structure, audience, infrastructure, and evaluation method. Some emphasize high-intensity technical defense against an active Red Team, while others focus on incident handling, information sharing, situational awareness, or national and multinational coordination. This diversity is useful for threat hunting development because analysts encounter different adversarial techniques, telemetry sources, operational constraints, and organizational procedures. Table 1 summarizes the faculty participation history in different cyber exercises.

Table 1. AADCF participation in cyber defense exercises, 2020–2026

Year	Exercise	Scope	Type
2020	Cyber Coalition 2020	NATO international	Collective
2020	CyberShockwave Embarg0 2020	International	Collective
2021	Locked Shields 2021	NATO international	Live-Fire
2021	Cyber Coalition 2021	NATO international	Collective
2021	CyberShockwave PANACEA 2021	International	Collective
2022	Locked Shields 2022	NATO international	Live-Fire
2022	Cyber Coalition 2022	NATO international	Collective
2022	CyberShockwave HYDRA 2022	International	Collective
2023	Locked Shields 2023	NATO international	Live-Fire
2023	Cyber Coalition 2023	NATO international	Collective
2024	Locked Shields 2024	NATO international	Live-Fire
2024	Cyber Coalition 2024	NATO international	Collective
2025	Cyber Coalition 2025	NATO international	Collective
2025	Bulgarian Rose 2025	National	Live-Fire
2026	Bulgarian Rose 2026	National	Live-Fire
2026	Locked Shields 2026	NATO international	Live-Fire
2026	Shadow Strike 2026	National	Live-Fire

This participation history motivates the methodology proposed in this paper. The research problem addressed in this paper is how to use observations from repeated cyber defense exercises to identify detection gaps, measure their severity, and convert them into targeted threat hunting training objectives. MITRE ATT&CK provide a common taxonomy for mapping exercise actions to categories such as reconnaissance, credential access, persistence, lateral movement, command and control, collection, and exfiltration (The MITRE Corporation, 2026). The purpose is to identify technique-specific weaknesses, track the same defensive areas over repeated training iterations, and determine whether targeted training leads to improvement. The proposed model uses two

core metrics: detection coverage and detection latency. The metrics are embedded in a closed training cycle that links exercise objectives, telemetry collection, threat hunting, measurement, gap identification, targeted training, and re-evaluation. Section 1 defines the model and mathematical formulation, and Section 2 describes how the measurements are converted into training priorities and evaluated in later exercises.

1 Closed-Cycle Threat Hunting Training Model

The proposed methodology treats each cyber defense exercise as one iteration in a continuous threat hunting training cycle. The cycle begins with the selection of exercise objectives and adversarial techniques, continues through exercise execution and telemetry collection, and then moves through threat hunting, measurement, gap identification, and updated training. The output of one iteration becomes an input to the next. Figure 1 presents the complete cycle.

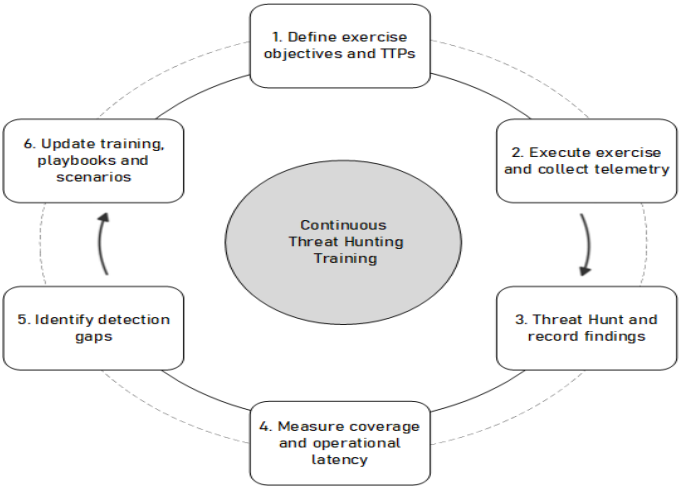


Figure 1: Closed-cycle threat hunting training model

For each exercise, the evaluation set contains adversarial actions, injects, or hunting opportunities that are relevant to the Blue Team. The exact actions do not need to be identical between exercises. Each observation is mapped to a common technique or capability category g and assigned a binary detection value $d_{e,i}$, where 1 means that the action was detected and validated and 0 means that no corresponding Blue Team finding was recorded during the defined observation period. This definition is important: an undetected action indicates absence of a recorded finding, not necessarily absence of underlying telemetry.

A compact record is sufficient for the proposed model. Table 2 lists the minimum fields. Additional exercise-specific fields can be retained locally, but they are not required for the common measurements.

Table 2. Minimum observation record for the proposed model

Field	Purpose	Required for
Exercise identifier	Associates the observation with an exercise iteration	Both metrics
Technique/category	Normalizes different injects to a common defensive area	Technique analysis
Action/inject identifier	Defines the evaluated adversarial action	Coverage
Detection status	Detected / not detected	Coverage
Action time	Time at which adversarial activity started or was executed	Latency
Detection time	Time of corresponding validated Blue Team finding	Latency
Operational intervals	Active exercise periods for each day	Latency
Evidence note	Reference to logs, case record, or analyst finding	Validation / audit

The total number of detected actions in exercise D_e is:

$$D_e = \sum_{i=1}^{N_e} d_{e,i}, \qquad d_{e,i} \in \{0,1\} \tag{1}$$

where N_e is total number of executed actions by the Red Team in exercise e.

Detection coverage C_e measures the proportion of evaluated adversarial actions for which the Blue Team records a corresponding validated finding and is calculated as:

$$C_e = \frac{D_e}{N_e} \text{x } 100\%, \tag{2}$$

Coverage therefore answers the first threat hunting question: which adversarial activities are not being identified? In some cases technique-specific value may be more useful for training than the overall exercise value. For example, high overall coverage can hide repeated weaknesses in credential access or exfiltration if the exercise contains many easily detected actions in other categories. The same measurement can be calculated for an individual technique or capability category g:

$$C_{e,g} = \frac{D_{e,g}}{N_{e,g}} \text{x } 100\%, \tag{3}$$

where $D_{e,g}$ is the detected actions in category g and $N_{e,g}$ is the total executed actions mapped to it.

Detection latency $L_{e,i}$ measures how long the Blue Team requires to identify an adversary action. It is calculated as the overlap between the interval from Red Team action to Blue Team detection.

$$L_{e,i} = t_{e,i}^{BT} - t_{e,i}^{RT}, \tag{4}$$

where $t_{e,i}^{RT}$ is the execution time of Red Team action i, and $t_{e,i}^{BT}$ is the corresponding detection time by the Blue Team.

If an activity is executed shortly before the end of an exercise day and detected during a subsequent operational period, the non-operational interval should not be interpreted as active analyst delay. For this reason, detection latency is calculated during the active exercise windows. The operational interval for exercise day can be defined as:

$$I_{e,k} = [a_{e,k}, b_{e,k}], \qquad k = 1, \dots, m_e \tag{5}$$

where $a_{e,k}, b_{e,k}$ are respectively the start and end timestamps of operational period k in exercise e. For an exercise with m_e operational days, the effective operational detection latency is:

$$L_{e,i}^{op} = \sum_{k=1}^{m_e} \max\left(0, \min\left(t_{e,i}^{BT}, b_{e,k}\right) - \max\left(t_{e,i}^{RT}, a_{e,k}\right)\right) \tag{6}$$

Undetected actions are not assigned a latency of zero or an artificial maximum value. They are represented by detection coverage and excluded from latency statistics. For the detected subset, the mean operational detection latency $\bar{L}_{e,i}^{op}$ can be calculated:

$$\bar{L}_e^{op} = \frac{1}{D_e} \sum_{i:d_{e,i}=1} L_{e,i}^{op}, \tag{7}$$

Because cyber exercise latency values can contain large outliers, the median should normally be reported together with the mean:

$$\tilde{L}_e^{op} = \text{median}\left\{L_{e,i}^{op} \mid d_{e,i} = 1\right\} \tag{8}$$

Coverage and latency therefore complement each other without being collapsed into a single score. A team may have high coverage but still detect activities too slowly, or it may respond quickly to the activities it sees while missing a substantial part of the attack sequence.

The same two metrics can be measured across repeated exercise iterations. For a technique category g evaluated in E exercises, pooled detection coverage is calculated from the total number of detected and executed actions across those exercises:

$$C_g^{(1:E)} = \frac{\sum_{e=1}^{E} D_{e,g}}{\sum_{e=1}^{E} N_{e,g}} \text{x } 100\%, \tag{9}$$

For detected actions in the same category, pooled average operational detection latency for category g across exercises 1 to E equals the sum of all operational detection

latencies for detected actions in that category, divided by the total number of detected actions in that category across all exercises:

$$\bar{L}_g^{op,1:E} = \frac{\sum_{e=1}^{E} \sum_{\substack{i \in g \\ d_{e,i}=1}} L_{e,i}^{op}}{\sum_{e=1}^{E} D_{e,g}} \tag{10}$$

2 Application and Re-evaluation

After an exercise, the proposed process does not stop with an after-action report. Coverage and operational latency are calculated for the evaluated technique categories and interpreted together. The objective is to determine whether the principal problem is missing visibility, slow investigation, or both. Figure 2 shows the resulting two-metric interpretation.

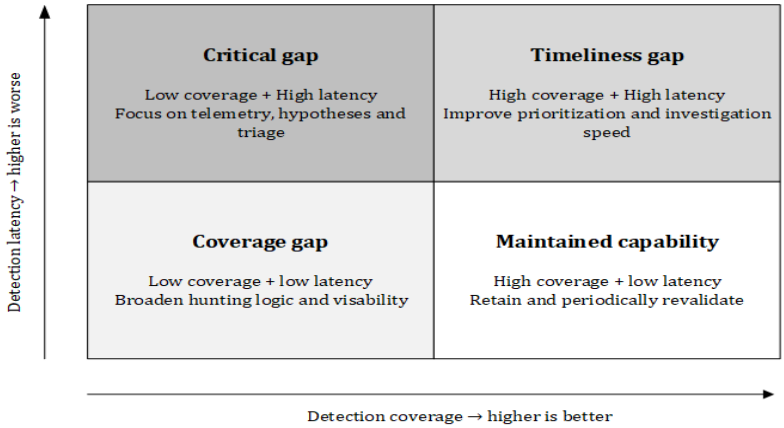


Figure 2: Interpreting detection coverage and detection latency for training prioritization

The boundaries between "high" and "low" are not universal. Before an exercise, the organization should define a target coverage C^* and an acceptable latency L^* that reflect the mission and exercise objectives. A category below the coverage target, above the latency target, or both becomes a candidate for additional training.

A low-coverage category should lead to a review of why the activity was missed. Possible causes include absent telemetry, insufficient retention, weak detection logic, lack of analyst hypotheses, or failure to correlate the available evidence. Focused adversary emulation can then reproduce the relevant techniques between major exercises so that the team can develop and validate hunting procedures in a controlled environment. Adversary-emulation platforms are particularly useful for repeatable technique execution and continuous security testing (Landauer, Mayer, Skopik, Wurzenberger, & Kern, 2024).

A high-latency category requires a different response. The activity may already be visible, but analysts may need better triage procedures, clearer escalation criteria, faster access to relevant telemetry, or more effective enrichment and correlation. Training should therefore reproduce the investigation under time constraints rather than simply create an additional alert.

The final stage of the cycle is re-evaluation. When a technique category appears again in a later exercise, the same observation rules are applied. Improvement can be expressed directly as the change in coverage and the reduction in operational latency:

$$\Delta C_g = C_{new,g} - C_{prev,g}\,, \tag{11}$$

$$\Delta \tilde{L}_g^{op} = \tilde{L}_{prev,g}^{op} - \tilde{L}_{new,g}^{op}\,, \tag{12}$$

where $C_{prev,g}$ and $C_{new,g}$ denote category-specific coverage in the previous and new evaluation iterations, while $\tilde{L}_{prev,g}^{op}$ and $\tilde{L}_{new,g}^{op}$ denote the corresponding median operational detection latencies.

Positive values for both terms indicate improvement through higher coverage and lower detection latency. The comparison should be interpreted only when the category definition, detection criteria, and observation method are sufficiently similar.

The closed cycle is completed when the re-evaluation results are used to update the next set of objectives. Categories that remain below the coverage target or above the acceptable latency target stay in the training plan. Categories that improve can receive less emphasis while new or emerging techniques are introduced. In this way, repeated participation in national and international cyber exercises becomes part of a continuous threat hunting development process.

Conclusion

Cyber defense exercises provide realistic opportunities to develop threat hunting skills, but their long-term value depends on whether observations from one event are converted into measurable objectives for the next. This paper proposed a closed-cycle methodology for using repeated cyber defense exercises as a continuous threat hunting development process.

The model uses two core metrics: detection coverage and detection latency. Coverage measures whether evaluated adversarial actions are identified, while latency measures how quickly detected activity is recognized. The latency formulation considers only active exercise periods. Both metrics can be calculated by technique category and aggregated across repeated exercises, allowing recurring visibility and timeliness weaknesses to be tracked.

The closed cycle connects exercise objectives, telemetry collection, threat hunting, gap identification, focused training, and re-evaluation. Low detection coverage indicates areas where visibility, telemetry, detection logic, or hunting hypotheses require improvement, while high detection latency indicates a need to improve triage, investigation, and correlation processes. In this way, the methodology provides a structured approach for converting lessons identified during cyber defense exercises into targeted Blue Team threat hunting training.

References

1. Glas, M., Vielberth, M., & Pernul, G. (2023). Train as you Fight: Evaluating Authentic Cybersecurity Training in Cyber Ranges. CHI '23: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, pp. 1-19. https://doi.org/10.1145/3544548.3581046
2. Landauer, M., Mayer, K., Skopik, F., Wurzenberger, M., & Kern, M. (2024). Red Team Redemption: A Structured Comparison of Open-Source Tools for Adversary Emulation. 2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 117-128. doi:10.1109/TrustCom63139.2024.00043
3. Maennel, K., Ottis, R., Maennel, O. (2017). Improving and Measuring Learning Effectiveness at Cyber Defense Exercises. In: Lipmaa, H., Mitrokotsa, A., Matulevičius, R. (eds) Secure IT Systems. NordSec 2017. Lecture Notes in Computer Science(), vol 10674. Springer, Cham. https://doi.org/10.1007/978-3-319-70290-2_8
4. Mahboubi, A., Luong, K., Aboutorab, H., Bui, H. T., Jarrad, G., Bahutair, M., Camtepe, S., Pogrebna, G., Ahmed, E., Barry, B., & Gately, H. (2024). Evolving techniques in cyber threat hunting: A systematic review. Journal of Network and Computer Applications, 232. doi:10.1016/j.jnca.2024.104004
5. The MITRE Corporation. (2026). MITRE ATT&CK. https://attack.mitre.org/
6. Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. Computers & Security, 88. https://doi.org/10.1016/j.cose.2019.101636
7. Yamin, M., & Katt, B. (2022). Modeling and executing cyber security exercise scenarios in cyber ranges. Computers & Security, 116. https://doi.org/10.1016/j.cose.2022.102635

THE ROLE OF TRUE ENTROPY IN POST-QUANTUM CYBERSECURITY

Zhaneta N. Savova*, Antoniya T. Tasheva**

** Department of Computer Systems and Technologies, Vasil Levski National Military University, Faculty of Artillery, Air Defence and Communication and Information Systems, Shumen, Bulgaria, zh.savova@mail.bg*
*** Department of Computer Systems, Technical University of Sofia, Sofia, Bulgaria, atasheva@tu-sofia.bg*

***Abstract**: True entropy is a mechanism that can mislead artificial intelligence and counter threats in cyberspace that are accelerated by quantum computing. This article introduces the concept of Entropy as a Service and explores how NIST SP 800-90 standards and entropy extraction mechanisms can be applied to the design of quantum-resistant cryptographic systems and true random number generators.*

***Keywords:** True Entropy, Entropy as a Service, EaaS, TRNG, Randomness Extraction*

Introduction

The security of all mechanisms used to protect modern cyberspace, including cryptographic key generation, establishing encrypted communications, digital signatures and certificates, session tokens and authentication, depends on the assumption that the random numbers used in their algorithms are truly unpredictable.

While the cybersecurity sector focuses on post-quantum cryptographic algorithms and threat detection using artificial intelligence, one fundamental vulnerability remains hidden at first glance. This phenomenon cannot be attributed to a vulnerability in cryptographic algorithms, nor can it be ascribed to a misconfiguration of system security or a "zero-day" exploit. The focus here is on theoretical true entropy.

Traditional cryptography relies heavily on a variety of statistical tests, such as NIST SP 800-22 [1], Dieharder [2], TestU01 [3], ENT [4], and others, to assess the degree of randomness and entropy in the generated binary sequences.

The advent of artificial intelligence (AI) in the realm of cyberattacks has led to a precipitous decline in the time it takes hackers to move from an initial breach to follow-up actions is decreasing dramatically to 29 minutes by 2025, with a minimum time of 4 minutes reported before data is extracted [5]. This underscores the critical need for high-quality, hardware-based random number generators to counter the rapid analysis and prediction of software vulnerabilities by machine learning algorithms.

The paper is organased as follows. First, the concept of Entropy as a Service is presented, along with the associated US National Institute of Standards and Technology (NIST) gold standards for generating truly random numbers. The paper then describes the EaaS architecture, which provides internet-connected devices with limited resources with secure sources of time and quantum entropy. Thirdly, the entropy extraction mechanisms that enable sources with weak randomness to be transformed into those with almost perfect randomness are compared. Finally, we conclude our paper by recommending the design of cryptographic systems that can withstand attacks by quantum computers.

1 Entropy as a Service

A significant milestone in the promotion of the Entropy as a Service (EaaS) was the project undertaken by the US NIST in 2013, which initiated work on the interoperability of entropy sources. In 2014, a novel architecture for delivering entropy over a network was presented with a view to addressing the issues surrounding the need for true entropy in virtual machines and IoT devices. Shortly thereafter, the first practical implementations emerged, offering an application programming interface (API) for generating random numbers based on quantum processes or atmospheric noise [6]. The LavaRand system, constructed in 2017, supplies an auxiliary source of entropy, which is produced by a wall of lava lamps in San Francisco [7]. The video feed from this wall is used to generate public, verifiable entropy, which contributes to the randomness that ensures the security of connections made via Cloudflare.

The NIST standards that directly affect the evolving EaaS architecture form part of the SP 800-90 series, which is widely regarded as the "gold standard" for true random number generation:

1. NIST SP 800-90A: Recommendation for Random Number Generation Using Deterministic Random Bit Generators (DRBGs) [8]. This standard describes algorithms that take an 'entropy seed' and generate long sequences of numbers that appear random.

2. NIST SP 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation [9]. This is the most critical standard for EaaS providers. It defines how physical or non-physical sources of 'noise' must be constructed and tested. Health tests are mandatory and check in real time whether the source has failed or is under external attack. Mathematical methods for assessing minimum entropy are defined to guarantee the quality of the provided data.

3. NIST SP 800-90C: Recommendation for Random Bit Generator (RBG) Constructions [10]. This standard, updated in September 2025, introduces various classes of RBG architecture and describes how components from 90A and 90B can be configured to form a complete system. Table 1 presents the main types of RBG and their characteristics.

Table 1: Main types of RBG and their characteristics

Type	Source of entropy	EaaS function
RBG1	External (Initialised once)	Receives an initial seed from an external EaaS server.
RBG2	Internal, (Reinitialised as required)	Uses a local hardware or non-physical (logical) internal source of entropy.
RBG3	Internal, continuous	Continuously extracts entropy to provide an output with 'real entropy'.
RBGC (RGB Chain)	Chain structure	Other RBG(s) on the same platform that are linked together in a chain or tree structure.

2 EaaS Architecture

Entropy as a Service (EaaS) is a new internet service architecture that provides IoT devices with secure sources of time and quantum entropy [11]. Figure 1 shows the main components of the basic EaaS architecture. These are the quantum entropy device, the EaaS server, and the Hardware Root of Trust (HRT). EaaS itself does not generate keys, but enables client systems to do so without the EaaS server having any means of obtaining information about the client.

The client system [12] runs a specialized software application capable of connecting to the local HRT device on one end and to the EaaS on the other. The application communicates with the entropy server using standard plain-text transfer protocols, such as HTTP.

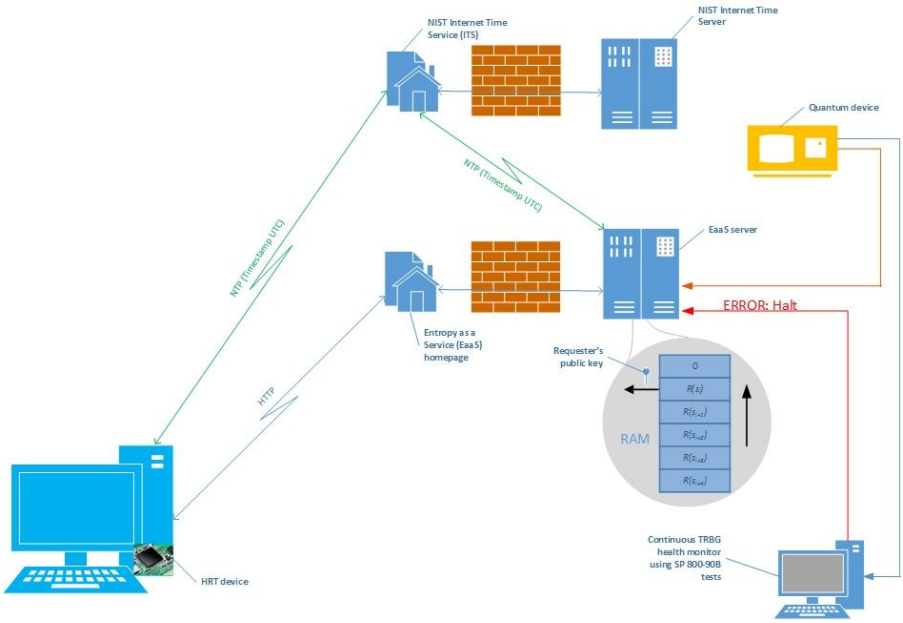


Figure 1: Basic EaaS Architecture [12]

1. The specialized application initiates the process of obtaining entropy from the EaaS server by first connecting to the HRT device and retrieving its public key.

2. The specialized application requests a timestamp from a time server via the Network Time Protocol (NTP).

3. The application then sends the HRT device's public key to the EaaS server via an HTTP GET request.

4. The EaaS server receives the applicant's public key, reads the next available random value $R(s_i)$, signs it with the EaaS private key, adds a timestamp, and sends the encrypted value back to the client.

5. The client application receives the result via HTTP and sends it to the HRT device.

6. The HRT device verifies the signature using the EaaS public key, checks the timeliness of the data via the timestamp, and decrypts the result using the client's private key. If the signature is valid, the random data is accepted, and the HRT device issues a ticket that allows the client system to later prove that it received true entropy from the EaaS.

The random data from step 6 must not be used directly to generate cryptographic keys or as a seed for a DRBG. Cryptographic entropy extraction mechanisms must be used to combine the random data from multiple remote EaaS instances with the local randomness associated with the client system and the HRT device.

It is recommended that at least two independent EaaS instances, located in different geographic regions, be used as remote sources. The data obtained from the random value generation process must be provided as the seed for a NIST-approved DRBG. This DRBG must then be used to generate cryptographic keys on the client system or in the HRT device using NIST-approved methods.

3 Entropy Extraction Mechanisms

Entropy extraction, also known as Randomness Extraction, is the process of converting a source with weak randomness (such as biometric data or software logs) into a "nearly perfect" random sequence, i.e., one with high entropy. A procedure that extracts randomness from a flawed source of random numbers by using a small additional number of truly random bits was first proposed in 1993 by Nissan and Zuckerman [13].

The main mechanisms for entropy extraction [14] are:

1. Seedless Extractors: These are simpler deterministic extractors, but they work only if the source has a specific structure (e.g., in the case of independent sources or specific mathematical properties).

Table 2: Mechanisms for Entropy Extraction

Mechanism	**How It Works**	**Strengths**	**Weaknesses**
Von Neumann extractor	Compares pairs of bits (01 → 0, 10 → 1; 00 and 11 are skipped).	Incredibly simple and fast	Works only with independent bits. Low efficiency.
Universal Hashing extractor	Applies a hash function to the source using a random seed.	Mathematically proven security. High speed	Requires a random "seed" to start with.
Trevisan's extractor	Combines error-correcting codes and hash functions.	It is theoretically optimal for extracting almost all of the entropy.	Complex to implement. Slower than hashing.
Hash-based cryptography (SHA-256)	Uses standard cryptographic hash algorithms.	Easy to integrate; available in hardware.	Mathematically, it is not a pure extractor. It relies on computational complexity.

2. Seeded Extractors: They use a small amount of truly random input (a seed) to extract a much larger amount of truly random output from a noise source.

3. Universal Hashing: A mechanism based on the Leftover Hash Lemma, which proves that hashing a source with sufficient entropy produces a nearly uniform distribution of bits.

A comparison of some specific entropy extraction mechanisms is presented in Table 2.

In theoretical studies, the Trevisan extractor offers the best performance, despite its complexity. For devices with very limited resources, the von Neumann method serves as a good first filter for removing baseline drifts. For hardware true random number generators (TRNGs), the use of Universal Hashing or SHA-256 is recommended because they are fast and cryptographically secure.

Conclusion

Entropy as a Service guarantees Internet users that attackers will not have any significant advantage that would allow them to gain access to the cryptographic keys generated locally on the client system. The implementation of the requirements of the NIST
SP 800-90 series in conjunction with the Trevisan extractor is considered the "gold standard" in the design of quantum-resistant cryptographic systems and true random number generators. To improve the speed of true random number generators, it is recommended that a universal hash extractor or SHA-256 is used.

References

1. Bassham III, Lawrence E., et al. (2010). SP 800-22 rev. 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Retrieved from: https://csrc.nist.rip/external/nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf
2. Marsaglia, George. (2008). The Marsaglia random number CDROM including the diehard battery of tests of randomness. Retrieved from: http://www.stat.fsu.edu/pub/diehard/
3. L'ecuyer, Pierre, & Richard Simard. (2007). TestU01: AC library for empirical testing of random number generators. *ACM Transactions on Mathematical Software (TOMS)* 33.4, pp. 1-40.
4. Walker (2008). ENT. A Pseudorandom Number Sequence Test Program Software and documentation. Retrieved from: https://www.fourmilab.ch/random/
5. Writer G. (February 2026). AI Arms Race Shrinks Breakout Time to 29 Minutes as Adversaries Turn GenAI on the Enterprise. IT Security Guru, Retrieved from: https://www.itsecurityguru.org/2026 /02/24/ai-arms-race-shrinks-breakout-time-to-29-minutes-as-adversaries-turn-genai-on-the-enterprise/

6. Syta, E., Jovanovic, P., Kogias, E.K., Gailly, N., Gasser, L., Khoffi, I., Fischer, M.J. & Ford, B. (2017). Scalable bias-resistant distributed randomness. In 2017 IEEE Symposium on Security and Privacy (SP), pp. 444-460. IEEE.
7. The Cloudflare Blog. November 17. (2017). LavaRand in Production: The Nitty-Gritty Technical Details. Retrieved from: https://blog.cloudflare.com/lavarand-in-production-the-nitty-gritty-technical-details/
8. Barker E.B., Kelsey J.M. (2015). Recommendation for Random Number Generation Using Deterministic Random Bit Generators. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-90Ar1. Retrieved from: https://doi.org/10.6028/NIST.SP.800-90Ar1
9. Sönmez Turan M, Barker EB, Kelsey JM, McKay KA, Baish ML, & Boyle M. (2018). Recommendation for the Entropy Sources Used for Random Bit Generation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-90B. Retrieved from: https://doi.org/10.6028/NIST.SP.800-90B
10. Barker EB, Kelsey JM, McKay K, Roginsky A, Sönmez Turan M. (2022). Recommendation for Random Bit Generator (RBG) Constructions. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-90C. Retrieved from: https://doi.org/10.6028/NIST.SP.800-90C
11. Vassilev A. & Staples R. (2016). Entropy as a Service: Unlocking Cryptography's Full Potential, in Computer, vol. 49, no. 9, pp. 98-102, doi: 10.1109/MC.2016.275.
12. NIST. Computer Security Resource Center. Created September 02, 2016. (2016). Entropy as a Service. Reference Architectures. Updated March 27, 2025. Retrieved from: https://csrc.nist.gov/Projects/ entropy-as-a-service/Architectures
13. Nisan, N., & Zuckerman D. (1993). More deterministic simulation in logspace. Proceedings of the twenty-fifth annual ACM symposium on Theory of computing.
14. Chattopadhyay, E. (2022). Recent advances in randomness extraction. Entropy 24.7, 2022: 880.

RESPONSIBLE INTELLIGENT GEOSPATIAL SYSTEMS: GEO-PRIVACY, CYBERSECURITY AND AI IN DEFENSE APPLICATIONS

Ani A. Stefanova

Faculty of Geodesy, Department of Applied Geodesy, University of Architecture, Civil Engineering and Geodesy, Sofia, Bulgaria, stefanova_fgs@uacg.bg

***Abstract**: The integration of artificial intelligence (AI), GNSS, UAV, IoT and GIS is transforming geospatial systems into intelligent infrastructures. In defense applications, these technologies support automated data acquisition, spatial analysis and decision-making, while introducing challenges related to geo-privacy, cybersecurity and responsible AI. This paper examines these challenges and proposes a conceptual framework integrating data protection, cybersecurity, transparency and human oversight.*

***Keywords**: Artificial intelligence, intelligent geospatial systems, geo-privacy, cybersecurity, GNSS, UAV, GIS, defense applications*

ОТГОВОРНИ ИНТЕЛИГЕНТНИ ГЕОПРОСТРАНСТВЕНИ СИСТЕМИ: ГЕОПОВЕРИТЕЛНОСТ, КИБЕРСИГУРНОСТ И AI В ОТБРАНИТЕЛНИ ПРИЛОЖЕНИЯ

Ани А. Стефанова

Геодезически факултет, катедра „Приложна геодезия“, Университет по архитектура, строителство и геодезия, София, България, stefanova_fgs@uacg.bg

***Резюме**: Интегрирането на изкуствения интелект (AI), GNSS, UAV, IoT и GIS трансформира геопространствените системи в интелигентни инфраструктури. В приложенията за отбраната тези технологии подпомагат автоматизираното събиране на данни, пространствения анализ и вземането на решения, но създават предизвикателства, свързани с геоповерителността, киберсигурността и отговорното използване на AI. В статията е предложена концептуална рамка, интегрираща защита на данните, киберсигурност, прозрачност и човешки контрол.*

***Ключови думи**: Изкуствен интелект, интелигентни геопространствени системи, геоповерителност, киберсигурност, GNSS, UAV, GIS, приложения за отбраната*

Въведение

През последните години развитието на изкуствения интелект (AI), глобалните навигационни спътникови системи (GNSS), безпилотните летателни апарати (UAV), технологиите на Интернет на нещата (IoT) и географските информационни системи (GIS) води до съществена трансформация на традиционните геодезически и геопространствени дейности [6]. Интегрирането на тези технологии позволява автоматизирано събиране, обработка и анализ на пространствени данни и създава основа за изграждането на интелигентни геопространствени системи.

В областта на отбраната геопространствената информация има особено значение за навигацията, ситуационната осведоменост, анализа на територията и подпомагането на вземането на решения. Едновременното използване на сензори, комуникационни мрежи, UAV, GNSS и облачни инфраструктури обаче увеличава зависимостта от цифрови технологии и поставя нови изисквания към сигурността и надеждността на геопространствените данни.

Наред с технологичните предимства възникват въпроси, свързани със защитата на информацията за местоположение, целостта и достоверността на данните, киберсигурността и отговорното използване на AI. Особено значение придобива геоповерителността (geo-privacy/location privacy), тъй като пространствените данни могат да съдържат чувствителна информация за местоположения, обекти, движения и свързани с тях дейности.

Поради това развитието на интелигентни геопространствени системи изисква не само технологична ефективност, но и интегриране на принципи за защита на данните, киберсигурност, прозрачност и човешки контрол. В този контекст концепцията за отговорна геодезия може да бъде разглеждана като основа за изграждането на надеждни и устойчиви геопространствени системи [7].

Целта на настоящата статия е да се разгледат основните аспекти на геоповерителността, киберсигурността и отговорното използване на AI при интелигентните геопространствени системи за приложения в областта на отбраната и да се предложи концептуална рамка, обединяваща тези направления.

Методологичният подход се основава на анализ и синтез на научни публикации и нормативни и методологични рамки, свързани с геоповерителността, киберсигурността, обяснимия AI и отговорното използване на интелигентни технологии. На тази основа е разработена концептуална рамка за отговорни интелигентни геопространствени системи.

Интелигентни геопространствени системи в приложенията за отбраната

В настоящото изследване под интелигентна геопространствена система се разбира интегрирана технологична среда, в която пространствени данни от различни източници се събират, обработват, анализират и представят чрез взаимосвързани цифрови технологии. За целите на настоящата работа интелигентният характер на системата се свързва с използването на автоматизирани методи за обработка и анализ, включително алгоритми на изкуствения интелект, както и с обмен на данни между различни компоненти на системата. За разлика от традиционните геодезически системи, при които отделните етапи на измерване и обработка могат да бъдат реализирани относително самостоятелно, разглежданият подход предполага по-висока степен на интеграция, автоматизация и подпомагане на анализа и вземането на решения.

Основни компоненти на такава система могат да бъдат GNSS приемници, безпилотни летателни апарати (UAV), дистанционни сензори, IoT устройства, географски информационни системи (GIS), облачни платформи и алгоритми за изкуствен интелект. Комбинирането на тези технологии позволява получаването на

пространствена информация с висока оперативна стойност и създава възможности за автоматизирана обработка на големи обеми данни.

В приложенията за отбраната интелигентните геопространствени системи могат да подпомагат навигацията, наблюдението на територии, анализа на пространствена информация, управлението на инфраструктура и ситуационната осведоменост [5], [6]. Особено значение има възможността данни от GNSS, UAV и дистанционни наблюдения да бъдат интегрирани в GIS среда, като AI подпомага откриването на пространствени промени и аномалии [2], [4], [6]. Например, при сценарий за ситуационна осведоменост получените резултати могат да бъдат подложени на експертна проверка преди използването им за подпомагане на решенията.

Разширяването на автоматизацията и свързаността обаче променя и характера на рисковете. Когато GNSS, UAV, IoT устройства, комуникационни мрежи и цифрови платформи функционират като взаимосвързана система, надеждността на крайния резултат зависи не само от точността на измерванията, но и от целостта, достъпността и защитата на данните. Поради това интелигентната геопространствена система следва да се разглежда не само като средство за повишаване на ефективността, а като значима цифрова инфраструктура, към която трябва да се прилагат изисквания за сигурност, защита на данните и контрол върху автоматизираните процеси.

Геоповерителност и защита на геопространствените данни

Геопространствените данни имат специфични характеристики, които ги отличават от много други видове цифрова информация. Те могат да описват не само местоположението на обекти, но и пространствени взаимоотношения, движения и промени във времето. При интегрирането на данни от GNSS, UAV, IoT сензори и други цифрови източници съществува възможност за формиране на подробни пространствени модели и профили на определени обекти или дейности.

В този контекст геоповерителността (geo-privacy) може да се разглежда като съвкупност от принципи и мерки за защита на чувствителна информация, свързана с местоположението и пространственото поведение. В контекста на настоящото изследване геоповерителността се разглежда в по-широк смисъл от защитата на лични данни, като включва и предотвратяване на неоторизираното разкриване или извеждане на чувствителна информация за местоположение на лица, обекти, инфраструктура или дейности. Значението ѝ нараства с увеличаването на обема, детайлността и честотата на събиране на геопространствени данни. Дори когато отделен набор от данни не позволява директно идентифициране на лице, комбинирането му с други пространствени или времеви данни може да позволи извеждането на допълнителна информация за неговото местоположение или пространствено поведение [1].

Особено внимание е необходимо при използването на UAV, GNSS и IoT технологии. Тези системи могат да генерират големи количества пространствено и времево маркирани данни, които се предават между различни устройства, комуникационни мрежи и информационни платформи [8]. Поради това защитата

на геопространствената информация следва да обхваща целия жизнен цикъл на данните – от тяхното събиране и предаване до обработката, анализа, споделянето и архивирането.

В отбранителния контекст значението на геоповерителността е допълнително повишено поради характера на обработваната пространствена информация. При проектирането на интелигентни геопространствени системи е необходимо принципите за минимизиране на данните, контрол на достъпа, проследимост на обработката и защита на чувствителната пространствена информация да бъдат разглеждани още на етапа на проектиране на системата.

По този начин геоповерителността се превръща не само в правен или етичен въпрос, а в съществен компонент на надеждността и сигурността на интелигентните геопространствени системи.

Киберсигурност на интелигентните геопространствени системи

Интелигентните геопространствени системи са изградени от множество компоненти, включващи измервателни сензори, GNSS приемници, UAV платформи, IoT устройства, комуникационни мрежи, сървъри и софтуерни приложения. Взаимодействието между тях осигурява непрекъснат обмен и обработка на пространствена информация, но увеличава броя на потенциалните точки, през които може да бъде нарушена сигурността на системата.

Киберсигурността в този контекст следва да обхваща не само защитата на информационните системи, но и целия процес на събиране, предаване, обработка и съхранение на геопространствени данни [3]. Особено значение имат тяхната поверителност, цялост и достъпност, тъй като промяната или загубата на пространствена информация може да повлияе върху резултатите от анализа и последващото вземане на решения.

При използването на GNSS, UAV и IoT технологии надеждността на системата зависи както от сигурността на отделните устройства, така и от инфраструктурата, която ги свързва. Поради това киберустойчивостта трябва да бъде разглеждана като системно свойство, а не като допълнителна защитна функция, включвана след изграждането на геопространствената система [5].

В приложенията за отбраната това изискване придобива особено значение. Интелигентната система трябва да може не само да обработва големи обеми пространствени данни, но и да запазва тяхната надеждност при грешки, прекъсвания или опити за нарушаване на информационната сигурност. Това предполага прилагане на механизми за контрол на достъпа, удостоверяване на участниците, проследимост на операциите и проверка на целостта на данните [3].

Следователно киберсигурността и геопространствената точност не трябва да се разглеждат като независими характеристики. Надеждността на крайния геопространствен резултат зависи както от качеството на измерванията и алгоритмите, така и от сигурността на цифровата среда, в която данните се събират, предават и обработват [9].

Отговорен AI и човешки контрол

Използването на изкуствен интелект в интелигентните геопространствени системи позволява автоматизирано разпознаване на обекти, анализ на пространствени зависимости, откриване на промени и подпомагане на вземането на решения. Прилагането на AI обаче поставя въпроси, свързани с надеждността на резултатите, прозрачността на алгоритмите и проследимостта на процеса, чрез който е получено дадено решение.

Особено значение има проблемът с „черната кутия" при някои AI модели, когато връзката между входните данни, алгоритмичната обработка и крайния резултат трудно може да бъде обяснена [2], [4]. В геопространствените приложения това е съществено, тъй като решенията се основават на данни от различни сензори и измервателни технологии, които могат да съдържат неопределености и грешки.

Поради това отговорното използване на AI предполага не само висока изчислителна ефективност, но и прозрачност, проследимост на обработката на данните и възможност за човешка оценка на резултатите [10]. При приложения, при които автоматизираните решения могат да имат значими последици, AI следва да се използва като инструмент за подпомагане на експертната преценка при ясно дефинирани роли и човешки контрол.

В геопространствения контекст това означава автоматизираните резултати да бъдат свързани с информация за използваните данни, методите на обработка и степента на неопределеност. Така се създават условия за по-добра проверимост и отговорност при използването на интелигентни технологии в отбранителни приложения.

Основните направления на защита и отговорност, разгледани в настоящото изследване, са обобщени в табл. 1.

Таблица 1. Основни направления, рискове и механизми за отговорност

Направление	**Основен риск**	**Механизъм за защита и отговорност**	**Очакван ефект**
Геопространствени данни	Разкриване на чувствителна информация за местоположение	Геоповерителност и контрол на достъпа	Защита на чувствителната пространствена информация
Цифрова инфраструктура	Нарушаване на поверителността, целостта и наличността	Киберсигурност и киберустойчивост	Устойчивост и надеждност на системата
AI обработка	Непрозрачност, грешки и алгоритмична неопределеност	Прозрачност, проследимост и обяснимост	Проверимост и по-добра интерпретируемост на AI резултатите
Вземане на решения	Неконтролирана автоматизация	Човешки контрол и експертна оценка	Контролируемост и отговорност при вземането на решения

Представеното обобщение показва необходимостта от интегриран подход, съчетаващ защита на геопространствените данни, киберсигурност, отговорно използване на AI и човешки контрол. Тези взаимосвързани компоненти са обединени в предложената концептуална рамка.

Концептуална рамка за отговорни интелигентни геопространствени системи

На основата на разгледаните технологични, защитни и етични аспекти се предлага концептуална рамка за отговорни интелигентни геопространствени системи. Тя обединява четири взаимосвързани функционални нива, които водят до краен резултат – надеждно геопространствено подпомагане на решенията. Научният принос на изследването се състои в разработването на концептуална многослойна рамка, която свързва четири взаимозависими аспекта – геопространствена информация, интелигентна обработка, сигурност и човешки контрол в контекста на отбранителни приложения.



Фиг. 1. Концептуална рамка за отговорни интелигентни геопространствени системи.

Както е показано на фиг. 1, първото ниво включва основните източници на геопространствена информация – GNSS, UAV, IoT сензори, дистанционни изследвания и GIS. Второто ниво обхваща автоматизираната обработка и анализа на данните чрез AI, машинно обучение и други интелигентни алгоритми.

Третото ниво интегрира изискванията за геоповерителност, киберсигурност, защита на данните, прозрачност и проследимост на обработката. Последното ниво

осигурява човешки контрол и експертна оценка на получените резултати. Обратната връзка от експертната оценка към интелигентната обработка позволява резултатите от автоматизираните процеси да бъдат проверявани и при необходимост коригирани.

Обсъждане на предложената рамка

Разработеният подход обединява технологичните възможности на интелигентните геопространствени системи с изискванията за сигурност и отговорност. Основно предимство на подхода е разглеждането на геопространствените данни, интелигентната обработка, защитата и човешкия контрол като взаимосвързани елементи, а не като отделни етапи.

Практическата стойност на рамката се състои във възможността рисковете, свързани с геопространствените данни и AI, да бъдат идентифицирани още при проектирането на системата. По този начин геоповерителността, киберсигурността и изискванията за прозрачност се разглеждат едновременно с технологичните възможности, а не като последващи мерки за защита.

Важен елемент на рамката е обратната връзка между човешкия контрол и интелигентната обработка. Тя позволява резултатите от автоматизираните алгоритми да бъдат оценявани от експерт и при необходимост да бъдат коригирани или допълнително проверени. Така се запазва ролята на човешката експертиза при използването на AI за подпомагане на решенията.

Настоящото изследване има концептуален характер и не включва експериментална валидация или количествено измерване на предложената рамка. Тя не определя конкретни алгоритми или прагове за надеждност, а задава принципна структура, която може да бъде конкретизирана според предназначението на системата. Следващ етап на изследването може да бъде разработването на измерими показатели и сценарии за оценка на надеждността, киберустойчивостта, геоповерителността, обяснимостта на AI и необходимостта от човешка намеса.

Рамката може да бъде адаптирана към различни приложения в областта на отбраната, без да се ограничава до конкретна технологична платформа. Това позволява включването на различни източници на пространствени данни и различни алгоритми за интелигентна обработка в зависимост от предназначението на системата.

Заключение

Интегрирането на AI, GNSS, UAV, IoT и GIS създава значителни възможности за развитие на интелигентни геопространствени системи за приложения в областта на отбраната. Наред с технологичните предимства обаче възникват предизвикателства, свързани с геоповерителността, киберсигурността, защитата на данните и отговорното използване на AI.

В настоящата статия е предложена концептуална рамка, която обединява тези аспекти и включва човешки контрол и експертна оценка като съществен компонент

на процеса. Подходът интегрира изискванията за сигурност и отговорност в цялостната архитектура на интелигентната геопространствена система.

Предложената рамка създава основа за по-нататъшно разработване на методи и практически модели за оценка на надеждността, сигурността и отговорността при използването на интелигентни геопространствени технологии в отбранителни приложения.

Литература

1. Georgiadou, Y., de By, R. A., & Kounadi, O. (2019). Location Privacy in the Wake of the GDPR. ISPRS International Journal of Geo-Information, 8(3), 157. https://doi.org/10.3390/ijgi8030157
2. Gevaert, C. M. (2022). Explainable AI for earth observation: A review including societal and regulatory perspectives. International Journal of Applied Earth Observation and Geoinformation, 112, 102869. https://doi.org/10.1016/j.jag.2022.102869
3. Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper NIST CSWP 29. National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.CSWP.29
4. Roussel, C., & Böhm, K. (2023). Geospatial XAI: A Review. ISPRS International Journal of Geo-Information, 12(9), 355. https://doi.org/10.3390/ijgi12090355
5. Stefanova, A. (2026). Cyber resilience of geodetic systems as an element of digital infrastructure. Security and Defense, 5(1), 93–101. https://doi.org/10.70265/JZPI2152
6. Stefanova, A. (2026). Geodesy 4.0: Scientific and Methodological Foundations and Applications of Intelligent Technologies in Geodesy. Sofia: Ani Adriyanova Stefanova. ISBN 978-619-93968-1-0.
7. Stefanova, A. A. (2025). Responsible geodesy: Ethical and sustainable models for the digital transformation of geodesy. Annals of Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, XV E, 399–410. https://doi.org/10.46687/YT25AAS
8. Denev, D. R., & Tsankov, Ts. S. (2018). Use in Internet of Protocols Transport Layer Security and its now-deprecated predecessor Secure Sockets Layer. Annual of Konstantin Preslavski University of Shumen, VIII E, 94–101. ISSN 1311-834X.
9. Hristova, E., Denev, D., & Tsankov, Ts. (2024). A survey of data quality in industrial networks and enhancing their reliability complex indicator for the needs of the industry. Environment. Technology. Resources, II, 120–126.
10. Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.AI.100-1

ETHICAL CHALLENGES IN IMPLEMENTING AUTOMATION AND AI

Ekaterina M. Hristova[1], Aleks Ya. Danev[2]

Faculty of Technical Sciences, Department of Communication and Computer Engineering and Security Technologies, Konstantin Preslavsky University of Shumen, Shumen, Bulgaria,
[1]ekaterinamkonstantinova@gmail.com, [2]aleksdanev@gmail.com

***Abstract**: The development of automation and artificial intelligence (AI) is fundamentally changing the way modern societies and economies function. Along with the many benefits, these technologies raise a number of ethical questions related to transparency, accountability, employment and data protection. This report examines the main ethical challenges in the implementation of AI and automation, as well as possible guidelines for their management.*

***Keywords**: Artificial intelligence, Automation, Ethical challenges, Algorithmic transparency, Personal data protection*

ЕТИЧНИ ПРЕДИЗВИКАТЕЛСТВА ПРИ ВНЕДРЯВАНЕТО НА АВТОМАТИЗАЦИЯ И AI

Екатерина М. Христова[1], Алекс Я. Данев[2]

Факултет по технически науки, катедра „Комуникационна и компютърна техника и технологии за сигурност“, Шуменски университет „Епископ Константин Преславски“, гр. Шумен, България, [1]ekaterinamkonstantinova@gmail.com, [2]aleksdanev@gmail.com

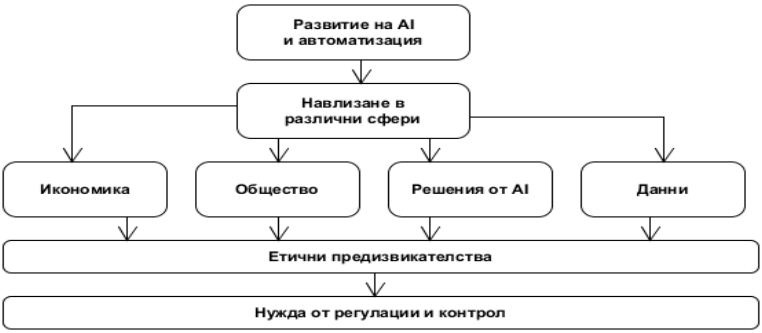
***Резюме**: Развитието на автоматизацията и изкуствения интелект (AI) променя съществено начина, по който функционират съвременните общества и икономики. Наред с множеството ползи, тези технологии пораждат редица етични въпроси, свързани с прозрачност, отговорност, заетост и защита на личните данни. Настоящият доклад разглежда основните етични предизвикателства при внедряването на AI и автоматизация, както и възможни насоки за тяхното управление.*

***Ключови думи**: Изкуствен интелект, Автоматизация, Етични предизвикателства, Алгоритмична прозрачност, Защита на личните данни*

Въведение

През последните десетилетия технологичният напредък доведе до бързо навлизане на автоматизирани системи и интелигентни алгоритми в различни сфери – от индустрията до здравеопазването и образованието [12]. Изкуственият интелект вече взема решения, които преди са били изцяло в ръцете на човека. Това поражда необходимост от внимателен анализ на моралните и социалните последици от тези промени. Етичните въпроси, свързани с AI, не са само технически, а засягат основни човешки ценности като справедливост, равенство и автономия. Липсата на ясни регулации и стандарти допълнително усложнява ситуацията и изисква интердисциплинарен подход. Развитието на изкуствения интелект е тясно свързано

с глобализацията и дигитализацията на обществото. Все по-голям обем от човешките дейности се прехвърля в цифрова среда, където алгоритмите играят ключова роля при вземането на решения. Това поставя въпроса доколко тези решения отразяват човешките ценности и дали могат да бъдат контролирани ефективно. Съществен аспект на проблема е скоростта, с която се внедряват новите технологии. Често иновациите изпреварват създаването на етични и правни рамки, което води до ситуации, в които обществото реагира постфактум. Това увеличава риска от негативни последици и подчертава необходимостта от проактивен подход. Освен това, внедряването на AI не е равномерно в различните региони и индустрии. Някои държави и организации имат значително предимство, което създава нови форми на неравенство. Това прави етичните въпроси не само локални, но и глобални по своя характер. Важно е също да се отбележи, че общественото възприятие за AI често се влияе от медии и популярна култура. Това може да доведе до както неоправдани страхове, така и до прекомерни очаквания. Затова е необходимо балансирано и информирано разбиране на възможностите и ограниченията на технологията. На фиг. 1 е показана схема на влиянието на изкуствения интелект върху обществото. [1], [3]

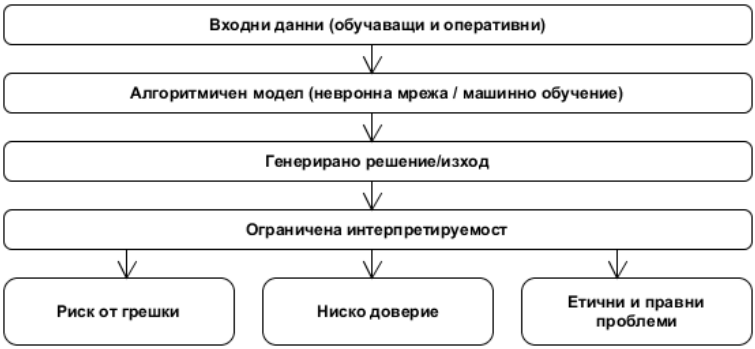


Фиг. 1. Влияние на изкуствения интелект върху обществото

Прозрачност и обяснимост на алгоритмите

Едно от основните предизвикателства е така наречения ефект на „черната кутия" при AI системите. Много алгоритми, особено тези базирани на машинно обучение, са трудни за разбиране дори от специалистите, които ги създават. Това създава проблеми при проследяването на решенията и оценката на тяхната справедливост. Липсата на прозрачност може да доведе до недоверие от страна на обществото [13]. Ако хората не разбират как се вземат решения, които ги засягат (например при кредити или медицински диагнози), те могат да отхвърлят тези технологии. Необходима е разработка на обясними AI системи, които позволяват проследяване и интерпретация на резултатите, без да се компрометира тяхната

ефективност. Допълнително усложнение възниква при използването на дълбоки невронни мрежи, които работят с огромни обеми от данни и сложни вътрешни структури. Тези модели често дават изключително точни резултати, но тяхната вътрешна логика остава неразбираема за човека. Това създава парадокс – колкото по-ефективна е системата, толкова по-трудно е да бъде обяснена. В контекста на чувствителни области като медицина или правосъдие това може да доведе до сериозни етични дилеми. Освен това липсата на обяснимост ограничава възможността за откриване на грешки и злоупотреби. Ако даден алгоритъм взема систематично неправилни решения, но причината не може да бъде проследена, рискът от дългосрочни негативни последици се увеличава значително. Това налага разработването на инструменти за одит и мониторинг на AI системи. В дългосрочен план прозрачността трябва да се разглежда не само като техническо изискване, а като социална отговорност. Организациите, които разработват и внедряват AI, трябва да комуникират ясно как функционират техните системи и какви са ограниченията им. Това е ключово за изграждане на доверие и устойчиво развитие на технологиите . Фиг. 2 е показан модел на непрозрачност при алгоритмите за изкуствен интелект. [5]



Фиг. 2. Модел на непрозрачност при алгоритми за изкуствен интелект

Пристрастия и дискриминация

AI системите често наследяват пристрастия от данните, върху които са обучени. Това може да доведе до дискриминация по признак пол, раса или социален статус. Например, алгоритми за подбор на персонал могат неволно да фаворизират определени групи. Проблемът се задълбочава, когато тези системи се използват в мащаб. Малки грешки или пристрастия могат да доведат до значителни социални неравенства. За да се намали този риск, е необходимо внимателно подбиране и анализ на данните, както и внедряване на механизми за откриване и коригиране на пристрастия. Пристрастията в AI често са отражение на

съществуващи социални неравенства. Данните, използвани за обучение, могат да съдържат исторически предразсъдъци, които алгоритмите възпроизвеждат и дори усилват. Това означава, че технологиите не са неутрални, а могат да задълбочат съществуващи проблеми, ако не бъдат внимателно контролирани. Особено тревожен е фактът, че дискриминацията, причинена от AI, често е трудно забележима. Тя може да се проявява под формата на малки отклонения в решенията, които на пръв поглед изглеждат незначителни, но в дългосрочен план водят до сериозни неравенства. Това прави необходим систематичен анализ и оценка на алгоритмите. За да се справим с този проблем, е необходимо участие на различни специалисти – не само инженери, но и социолози, етици и юристи. Таблица 1 показва влиянието на пристрастяването към AI системи. [7]

Таблица 1. Влиянието на пристрастяването към AI системите

Категория	Процент засегнати случаи (%)	Основен риск	Ниво на въздействие (1–5)
Подбор на персонал	35%	Дискриминация по пол/етнос	4
Кредитиране	28%	Неравен достъп до финанси	5
Правосъдие	22%	Несправедливи присъди	5
Здравеопазване	15%	Неправилни диагнози	4

Влияние върху заетостта

Автоматизацията води до заместване на човешкия труд в редица отрасли. Това поражда опасения за масова безработица и социална нестабилност. Особено уязвими са нискоквалифицираните работници. От друга страна, AI създава нови професии и възможности, но те често изискват различни умения. Това води до необходимост от преквалификация и адаптация на работната сила. Етичният въпрос тук е как обществото да осигури справедлив преход, като подкрепи засегнатите групи чрез образование и социални политики. Автоматизацията не само премахва работни места, но и променя естеството на труда. Много професии се трансформират, като изискват нови умения, свързани с работа с технологии и анализ на данни. Това поставя предизвикателства пред образователните системи, които трябва да се адаптират към новите реалности. Социалното неравенство може да се увеличи, ако достъпът до образование и преквалификация не е равномерно разпределен. Хората с по-ниски доходи често имат по-малко възможности да се адаптират към промените, което ги поставя в по-неблагоприятна позиция. Това превръща проблема не само в икономически, но и в морален въпрос. От друга страна, автоматизацията може да освободи хората от рутинни и тежки задачи, позволявайки им да се фокусират върху по-креативни и смислени дейности. В този контекст е важно да се намери баланс между ефективност и човешко благополучие, като се гарантира, че технологичният напредък носи ползи за всички. Таблица 2,

таблица 3 и таблица 4 показват различни аспекти на влиянието върху заетостта [2], [4].

Таблица 2. Автоматизация по сектори

Сектор	Ниво на автоматизация (%)	Риск за работни места (%)	Нови възможности (%)
Производство	70%	50%	30%
Транспорт	65%	45%	35%
Администрация	60%	40%	30%
IT сектор	40%	20%	60%

Таблица 3. Влияние върху квалификацията

Ниво на квалификация	Засегнати работни места (%)	Нужда от преквалификация (%)
Ниска	60%	70%
Средна	30%	50%
Висока	10%	20%

Таблица 4. Положителни и отрицателни ефекти

Тип ефект	Процент (%)	Описание
Загуба на работни места	40%	Автоматизация на рутинни задачи
Създаване на нови роли	35%	AI, анализ на данни
Повишена ефективност	25%	Оптимизация на процеси

Защита на личните данни

AI системите често разчитат на огромни обеми от лични данни. Това поражда сериозни рискове за поверителността и сигурността на информацията. Неправомерното използване на данни може да доведе до злоупотреби и нарушаване на права. Съществува и риск от масово наблюдение, особено при използване на технологии като лицево разпознаване. Това поставя под въпрос баланса между сигурност и свобода. Необходима е строга регулация и прозрачност при събирането и използването на данни, както и информирано съгласие от страна на потребителите [11]. С нарастването на обема от събирани данни се увеличава и рискът от злоупотреби. Компаниите често събират информация за потребителите без пълна прозрачност, което поставя под въпрос тяхното право на личен живот. Това създава необходимост от по-строги регулации и механизми за контрол. Друг важен аспект е сигурността на данните. Кибератаките и изтичането на информация

могат да имат сериозни последици както за отделните лица, така и за цели организации. Това изисква инвестиции в сигурност и разработване на надеждни системи за защита. Етичният подход към данните включва не само тяхната защита, но и отговорното им използване. Организациите трябва да гарантират, че данните се използват по начин, който е в интерес на обществото и не нарушава правата на индивидите. [6]

КАЗУС: В голяма онлайн платформа за електронна търговия се внедрява система за изкуствен интелект, която анализира поведението на потребителите с цел персонализиране на реклами и препоръки. Системата събира данни като история на покупки, време на престой в сайта, търсения и дори местоположение. В началото това води до повишаване на продажбите и по-добро потребителско изживяване. С течение на времето обаче се установява, че част от събраните данни се използват без изричното съгласие на потребителите. Освен това възниква пробив в сигурността, при който лична информация на хиляди потребители изтича в интернет пространството. Това води до загуба на доверие, правни последствия и финансови санкции за компанията. Проблемът се задълбочава от факта, че системата е сложна и липсва прозрачност относно начина, по който се обработват данните. Потребителите не са достатъчно информирани каква информация се събира и с каква цел се използва, което представлява сериозно нарушение на етичните принципи и регулации като GDPR. В таблица 5 са представени данните от казуса, а на фиг. 3 – техният анализ.

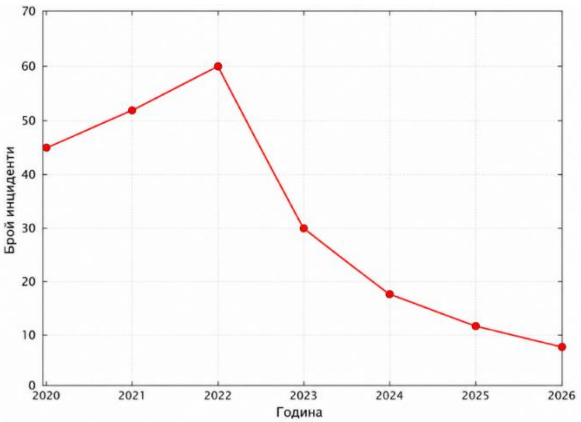
Таблица 5. Брой инциденти с лични данни (преди и след мерки)

Година	Инциденти (бр.)
2020	45
2021	52
2022	60
2023	30
2024	18
2025	12
2026	8

За да се преодолеят възникналите проблеми, организацията предприема редица мерки, насочени към повишаване на сигурността и прозрачността. На първо място се въвежда политика за минимизиране на данните, при която се събира само необходимата информация. Освен това се внедряват механизми за криптиране и защита на данните. Паралелно с това се разработва система за информирано съгласие, чрез която потребителите ясно разбират какви данни се събират и могат да контролират тяхното използване. Въвеждат се и инструменти за анонимизация, които намаляват риска от идентифициране на отделни лица. В резултат на тези мерки се наблюдава постепенно възстановяване на доверието, намаляване на инцидентите със сигурността и по-добро съответствие с регулаторните изисквания.

Това показва, че етичният подход към данните не само защитава потребителите, но и носи дългосрочни ползи за организациите.

Данните показват увеличение на инцидентите, свързани с нарушения на личните данни, през периода 2020–2022 г., като през 2022 г. е достигнат най-високият регистриран брой от 60 случая. След внедряването на допълнителни мерки за сигурност, включително криптиране на данните, многофакторна автентикация и по-строг контрол върху достъпа до информация, се наблюдава значително намаляване на инцидентите. През периода 2023–2026 г. броят на нарушенията намалява постепенно от 30 до 8 случая годишно. Тази тенденция показва ефективността на приложените мерки за защита и повишената осведоменост относно сигурността на личните данни. Намалението с над 85% спрямо пиковата стойност през 2022 г. демонстрира значението на етичния подход при обработката и съхранението на потребителска информация. [8], [9]



Фиг. 3. Резултати от казус

Отговорност и контрол

Когато AI система вземе грешно решение, възниква въпросът кой носи отговорност – разработчикът, компанията или самата система. Липсата на ясна отговорност затруднява правното регулиране. Освен това, автономните системи могат да действат по начини, които не са напълно предвидими. Това създава риск от неконтролируеми последици. Важно е да се разработят ясни рамки за отговорност и механизми за човешки контрол, които да гарантират безопасното използване на AI. Въпросът за отговорността става още по-сложен с развитието на автономни системи като самоуправляващи се автомобили. В случаи на инциденти е трудно да се определи кой носи вина – производителят, разработчикът или потребителят. Това създава правна несигурност и изисква нови регулаторни рамки. Освен юридическата отговорност, съществува и морална такава. Компаниите

трябва да поемат ангажимент за етично поведение и да гарантират, че техните технологии не причиняват вреда. Това включва провеждане на тестове, оценка на риска и прозрачност в процеса на разработка. Накрая, човешкият контрол остава ключов елемент. Въпреки напредъка на AI, е важно да има възможност за човешка намеса при критични ситуации. Това гарантира, че решенията остават в рамките на човешките ценности и етични норми. [10]

Заключение

Етичните предизвикателства при внедряването на автоматизация и изкуствен интелект са сложни и многопластови. Те изискват сътрудничество между учени, политици, бизнес и общество. Само чрез балансиран подход може да се гарантира, че технологичният напредък служи на човека, без да нарушава основни ценности. В бъдеще ще бъде от съществено значение да се разработят глобални стандарти и регулации, които да насърчават етичното използване на AI. Образованието и обществената осведоменост също играят ключова роля в този процес. В крайна сметка, успехът на AI няма да се измерва само с технологични постижения, а с неговото въздействие върху човечеството и способността ни да го управляваме отговорно. В контекста на бързо развиващите се технологии, необходимостта от етично управление на AI става все по-належаща. Това включва не само създаване на регулации, но и изграждане на култура на отговорност сред разработчиците и организациите. Етиката трябва да бъде интегрирана още в процеса на създаване на технологиите, а не да се разглежда като допълнение. Също така е важно да се насърчава активното участие на обществото в тези процеси. Гражданите трябва да бъдат информирани и да имат възможност да изразяват мнение относно начина, по който се използват технологиите. Това ще допринесе за по-голяма прозрачност и доверие. Образованието играе ключова роля за подготовката на бъдещите поколения да се справят с предизвикателствата на AI. Необходимо е развитие на критично мислене, дигитална грамотност и етично съзнание, които да позволят на хората да използват технологиите отговорно. В заключение, бъдещето на автоматизацията и изкуствения интелект зависи не само от технологичния напредък, но и от способността на обществото да поставя ясни морални граници. Само чрез съзнателно и отговорно управление може да се гарантира, че тези технологии ще служат в полза на човечеството.

Литература

1. Denev, D., & Tsankov, Ts. (2022). Communication-based dynamic packet optimization for visual PLC monitoring. Proceedings of the Annual University Scientific Conference of Vasil Levski National Military University, 1259–1266.
2. Denev, D., & Tsankov, Ts. (2022). Design and implementation of a field level of an industrial communication network for the needs of the industry. Proceedings of the 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST 2022), 1–4.

3. Denev, D., & Tsankov, Ts. (2022). A survey of data quality and processing of information in innovative smart devices. Proceedings of the International Conference Automatics and Informatics (ICAI 2022), 1–4.
4. Denev, D., & Tsankov, Ts. (2022). A survey of data quality in digital processing of acoustic signals. Proceedings of the International Conference on Communications, Information, Electronic and Energy Systems (CIEES), 1–4.
5. Denev, D., & Tsankov, Ts. (2021). Temperature measurement with microcontroller PIC18F452. SocioBrains, 83, 99–103.
6. Dimitrova, E., & Denev, D. (2024). The development of artificial intelligence and its applications in the modern world. Proceedings of the International Scientific Conference MATTECH 2024, 2: Communication and Computer Technologies, 153–160.
7. Denev, D., & Sotirov, P. (2026). Virtual and augmented reality for training in automation and network technologies. Annual of Konstantin Preslavsky University of Shumen, XV E, 97–108.
8. Hatib, I., & Denev, D. (2025). Integrating artificial intelligence for autonomous traffic management in industrial networks and automation systems. Proceedings of the International Scientific Conference Defense Technology Forum, 813–820.
9. Denev, D., & Nikolova, S. (2025). A novel algorithm for industrial network reliability estimation and AI-based system optimization. Proceedings of the XXXIII National Conference with International Participation TELECOM. https://doi.org/10.1109/TELECOM66943.2025.11304081
10. Nedkova, B., & Denev, D. (2026). An algorithmic model for adaptive gamification in cybersecurity training. Proceedings of the Scientific and Technical Conference "Black Sea Experts", 104–107.
11. Simeonova, I. (2025). How GDPR treats automated decision-making. Journal Scientific and Applied Research, 28(1), 164–175. Shumen: Konstantin Preslavsky University Press. ISSN 1314-6289.
12. Stefanova, A. A. (2025). Responsible geodesy: Ethical and sustainable models for the digital transformation of geodesy. Annual of Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, XV E, 399–410.
13. Stefanova, A. (2026). Geodesy 4.0: Scientific and Methodological Foundations and Applications of Intelligent Technologies in Geodesy. Sofia: Ani Adriyanova Stefanova. ISBN 978-619-93968-1-0.

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**, Faculty of Artillery, Air Defense and Communication and Information Systems

CYBERSECURITY IN AUTOMATED INDUSTRIAL SYSTEMS

Petar G. Sotirov[1], Ilker A. Hatib[2]

Faculty of Technical Sciences, Department of Communication and Computer Engineering and Security Technologies, Konstantin Preslavsky University of Shumen, Shumen, Bulgaria, [1]2470020006@shu.bg, [2]i.hatib@shu.bg

***Abstract**: With the development of industrial automation and the introduction of the "Industry 4.0" concept, automated industrial systems are becoming increasingly connected and dependent on information technology. This connectivity provides significant opportunities for optimization of production processes, but at the same time increases the risk of cyberattacks. Cybersecurity in industrial systems aims to protect critical infrastructure, production processes and sensitive information from unauthorized access, sabotage and malicious actions. This report examines the main aspects of cybersecurity in automated industrial systems, threats, protection methods and future challenges in this area.*

***Keywords**: Cybersecurity, Automated industrial systems, Industrial networks, Cyber threats, Critical infrastructure*

КИБЕРСИГУРНОСТ В АВТОМАТИЗИРАНИТЕ ИНДУСТРИАЛНИ СИСТЕМИ

Петър Г. Сотиров[1], Илкер А. Хатиб[2]

Факултет по технически науки, катедра „Комуникационна и компютърна техника и технологии за сигурност", Шуменски университет „Епископ Константин Преславски", гр. Шумен, България, [1]2470020006@shu.bg, [2]i.hatib@shu.bg

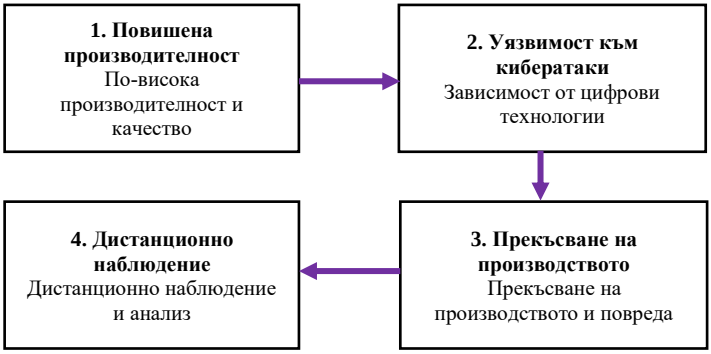
***Резюме**: С развитието на индустриалната автоматизация и навлизането на концепцията „Индустрия 4.0" автоматизираните индустриални системи стават все по-свързани и зависими от информационните технологии. Тази свързаност предоставя значителни възможности за оптимизация на производствените процеси, но същевременно увеличава риска от кибератаки. Киберсигурността в индустриалните системи има за цел да защити критичната инфраструктура, производствените процеси и чувствителната информация от неоторизиран достъп, саботаж и злонамерени действия. В настоящия доклад са разгледани основните аспекти на киберсигурността в автоматизираните индустриални системи, заплахите, методите за защита и бъдещите предизвикателства в тази област.*

***Ключови думи**: Киберсигурност, Автоматизирани индустриални системи, Индустриални мрежи, Киберзаплахи, Критична инфраструктура*

Въведение

Автоматизираните индустриални системи представляват съвкупност от хардуерни и софтуерни компоненти, които управляват и контролират

производствени процеси с минимална човешка намеса. Те включват програмируеми логически контролери (PLC), системи за надзор и управление на процеси (SCADA), индустриални мрежи и различни сензори и изпълнителни механизми. През последните години индустриалните предприятия все по-често свързват своите производствени системи към корпоративни мрежи и интернет. Това позволява дистанционно наблюдение, анализ на данни в реално време и подобряване на ефективността. Въпреки тези предимства, свързаността увеличава повърхността за атака и създава нови рискове за сигурността [12]. Затова киберсигурността се превръща в ключов фактор за надеждната работа на индустриалните системи и за защитата на критичната инфраструктура от потенциални заплахи. Автоматизацията на индустриалните процеси допринася за повишаване на производителността, намаляване на разходите и подобряване на качеството на продукцията. Благодарение на внедряването на интелигентни системи предприятията могат да събират и анализират големи количества данни, което позволява по-добро планиране и вземане на решения в реално време. В същото време зависимостта от цифровите технологии прави индустриалните среди по-уязвими към киберинциденти. Дори една успешна атака може да доведе до прекъсване на производството, повреда на оборудването и сериозни икономически последици. Поради тази причина киберсигурността е сред основните приоритети на съвременните индустриални организации. На фиг. 1 е показана общата представа за автоматизирани индустриални системи. [1]



Фиг. 1: Обща представа за автоматизирани индустриални системи

Характеристика на автоматизираните индустриални системи

Автоматизираните индустриални системи се използват в производството, енергетиката, транспорта, водоснабдяването и много други отрасли. Тяхната основна функция е да осигуряват автоматично управление и контрол върху технологичните процеси. Тези системи се отличават с висока степен на надеждност и непрекъснат режим на работа. За разлика от традиционните информационни

системи, при тях дори краткотрайно прекъсване може да доведе до сериозни финансови загуби, производствени аварии или риск за човешкия живот. Съвременните индустриални системи все по-често използват интернет базирани технологии и облачни услуги, което повишава ефективността, но също така изисква по-високо ниво на защита срещу киберзаплахи. Индустриалните контролни системи са проектирани да функционират в специфични условия, като високи температури, влажност, вибрации и други фактори на околната среда. Това ги отличава от стандартните компютърни системи и налага използването на специализирано оборудване и комуникационни протоколи. Друг важен аспект е необходимостта от работа в реално време. Много производствени процеси изискват незабавна реакция на системата при промяна на параметрите, което прави надеждността и сигурността на комуникациите особено важни за нормалното функциониране на производството. Таблица 1 представя характеристиките на автоматизираните индустриални системи. Данните показват високата степен на автоматизация, надеждност и свързаност на съвременните производствени среди. [2]

Таблица 1: Показатели на автоматизираните индустриални системи

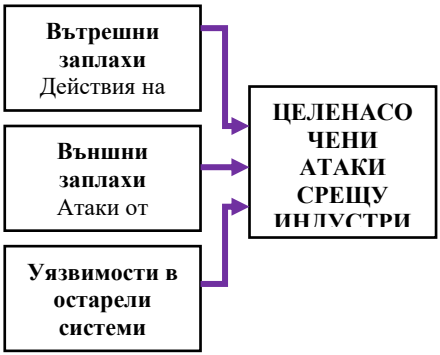
Показател	Стойност	Значение
Ниво на автоматизация	85%	Висока степен на автоматизирани процеси
Време за реакция на системата	50 ms	Бърза обработка на данни в реално време
Наличност на системата	99,8%	Минимални прекъсвания в работата
Брой свързани устройства	250	Широка мрежа от сензори и контролери
Среден обем обработени данни на ден	500 GB	Интензивен обмен на информация

Основни киберзаплахи за индустриалните системи

Сред най-разпространените заплахи са злонамереният софтуер, рансъмуер атаките, неоторизираният достъп и вътрешните заплахи, произтичащи от действия на служители или подизпълнители [11]. Подобни атаки могат да нарушат производствения процес и да причинят значителни щети. Особено опасни са целенасочените атаки срещу индустриални контролни системи. Нападателите могат да манипулират работата на оборудването, да променят производствени параметри или да прекъснат функционирането на цели производствени линии. Допълнителен риск представляват остарелите устройства и софтуер, които често не получават актуализации за сигурност. Това създава уязвимости, които могат да бъдат използвани от киберпрестъпници за проникване в системата. С развитието на киберпрестъпността се увеличава и сложността на атаките срещу индустриалните среди. Нападателите използват различни техники като социално инженерство, експлоатиране на софтуерни уязвимости и компрометиране на потребителски акаунти с цел получаване на достъп до критични системи. Заплаха представляват и

атаките срещу веригата за доставки, при които злонамерен код може да бъде внедрен още на етап разработка или доставка на софтуер и оборудване. Подобни атаки са трудни за откриване и могат да засегнат голям брой организации едновременно.

На фиг. 2 са показани многостранни киберзаплахи за индустриалните системи. [3], [4]



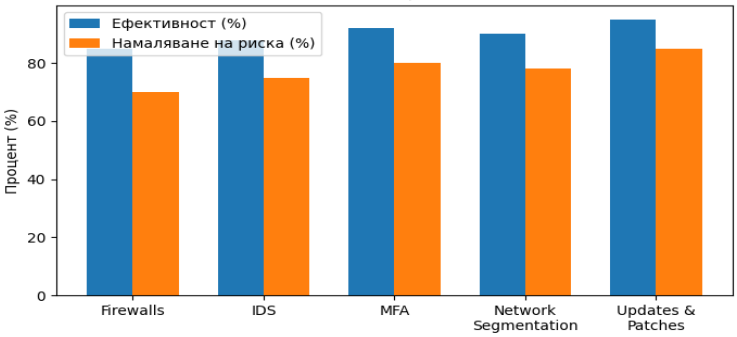
Фиг. 2: Многостранни киберзаплахи за индустриалните системи

Методи за защита на индустриалните мрежи

Една от основните мерки за защита е сегментирането на мрежите. Чрез разделяне на индустриалната и корпоративната мрежа се намалява рискът от разпространение на атаки между различните системи. Използването на защитни стени, системи за откриване на проникванията и криптирани комуникации допринася за по-висока степен на сигурност. Тези технологии позволяват контрол върху мрежовия трафик и откриване на подозрителни действия. Редовното актуализиране на софтуера и фърмуера също е важна част от защитата. Актуализациите отстраняват известни уязвимости и намаляват вероятността от успешна атака. Прилагането на многостепенен модел на защита значително повишава устойчивостта на индустриалните системи. Този подход включва използването на различни средства за сигурност на ниво устройство, мрежа и приложение, така че евентуален пробив в един слой да не компрометира цялата система. Съществена роля играят и резервните копия на данните и плановете за възстановяване след инцидент. Те позволяват бързо възстановяване на работата при възникване на кибератака или техническа повреда и минимизират негативните последствия за производството. Таблица 2 представя стойности за ефективността на основните методи за защита на индустриалните мрежи. Данните показват, че комбинираното прилагане на различни защитни механизми значително намалява риска от успешни кибератаки. [5], [6]

Таблица 2: Основни методи за защита на индустриалните мрежи

Метод за защита	Ниво на ефективност (%)	Намаляване на риска (%)
Защитни стени (Firewalls)	85	70
Системи за откриване на проникванията (IDS)	88	75
Многофакторна автентикация	92	80
Сегментиране на мрежата	90	78
Редовни актуализации и пачове	95	85



Фиг. 3: Сравнение на ефективността на методите за защита на индустриалните мрежи

Ролята на човешкия фактор в киберсигурността

Въпреки развитието на технологиите, човешкият фактор остава една от най-честите причини за инциденти, свързани с киберсигурността. Недостатъчната осведоменост или неправилните действия на служителите могат да доведат до компрометиране на системите. Обучението на персонала е ключов елемент от всяка стратегия за сигурност. Служителите трябва да разпознават фишинг атаки, да използват сигурни пароли и да спазват установените политики за информационна сигурност. Освен техническите специалисти, всички работещи в организацията трябва да бъдат ангажирани с процесите по защита на информацията. Създаването на култура на сигурност значително намалява риска от инциденти. Много от успешните кибератаки започват с човешка грешка, като отваряне на подозрителен имейл или използване на слаба парола. Поради това организациите трябва редовно да провеждат обучения и практически упражнения за повишаване на информираността относно актуалните заплахи. Ръководството на предприятието

също има важна роля в изграждането на ефективна политика за сигурност. Осигуряването на необходимите ресурси, контролът върху спазването на процедурите и насърчаването на добри практики създават основа за по-високо ниво на защита. Таблица 3 представя разпределение на киберинцидентите, причинени от човешкия фактор. Данните показват, че най-честите причини са отварянето на фишинг съобщения и използването на слаби пароли. Това подчертава необходимостта от редовно обучение на персонала и прилагане на добри практики за информационна сигурност с цел намаляване на риска от компрометиране на индустриалните системи. [7], [9]

Таблица 3. Основни методи

Причина за инцидент	Дял от инцидентите (%)	Ниво на риск
Отваряне на фишинг имейли	35	Високо
Използване на слаби пароли	25	Високо
Неспазване на политики за сигурност	18	Средно
Неправилна конфигурация на системи	12	Средно
Злоумишлени действия на служители	10	Високо

Бъдещи тенденции и предизвикателства

Развитието на Интернет на нещата (IoT), изкуствения интелект и облачните технологии променя начина, по който функционират индустриалните системи. Тези технологии предоставят нови възможности за автоматизация и анализ на данни. Наред с предимствата обаче се появяват и нови предизвикателства пред киберсигурността. Увеличава се броят на свързаните устройства, което разширява потенциалните точки за атака и усложнява управлението на сигурността. Организациите трябва непрекъснато да адаптират своите защитни механизми към новите заплахи. Инвестициите в модерни технологии за сигурност и квалификация на персонала ще бъдат решаващи за бъдещата защита на индустриалните системи. Очаква се използването на изкуствен интелект в областта на киберсигурността да се разширява все повече. Интелигентните системи могат автоматично да анализират големи обеми от данни, да откриват аномалии и да реагират на потенциални заплахи значително по-бързо от традиционните методи. Въпреки това и киберпрестъпниците започват да използват изкуствен интелект за създаване на по-сложни и трудни за откриване атаки. Таблица 4 представя очакваното разпространение на ключови технологии в индустриалната среда до 2030 г. Данните показват, че Интернет на нещата и изкуственият интелект ще бъдат сред най-широко внедрените технологии, но същевременно ще доведат до повишаване на киберрисковете поради увеличения брой свързани устройства и сложността на инфраструктурата. Таблица 5 показва прогнозните предизвикателства пред индустриалната киберсигурност през следващите години. Най-сериозни рискове се очакват от компрометирани IoT устройства, използването на изкуствен интелект за

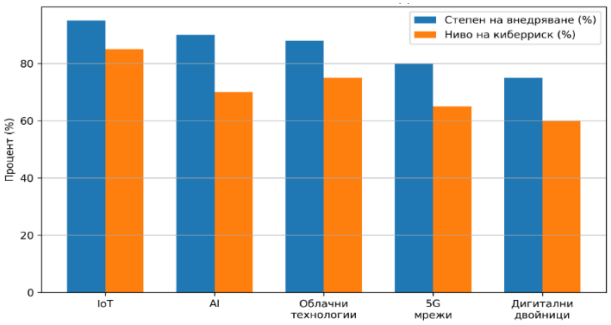
извършване на атаки и пробивите във веригата за доставки, които могат да засегнат едновременно множество организации. [10]

Таблица 4: Очаквано влияние на новите технологии върху киберсигурността в индустриалните системи

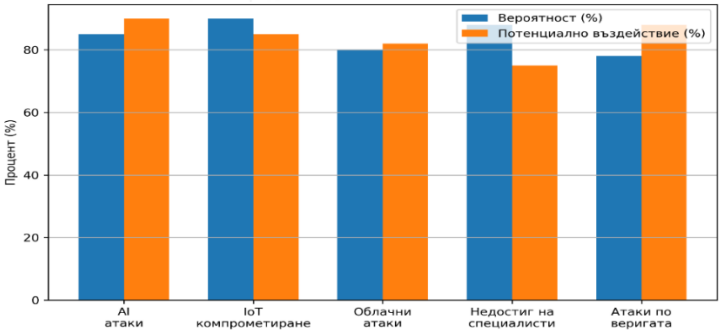
Технология	Степен на внедряване до 2030 г. (%)	Ниво на киберрисък (%)
Интернет на нещата (IoT)	95	85
Изкуствен интелект (AI)	90	70
Облачни технологии	88	75
5G индустриални мрежи	80	65
Дигитални двойници (Digital Twins)	75	60

Таблица 5: *Основни бъдещи предизвикателства пред киберсигурността в индустриалните системи*

Предизвикателство	Вероятност (%)	Потенциално въздействие (%)
Атаки чрез AI	85	90
Компрометиране на IoT устройства	90	85
Атаки срещу облачна инфраструктура	80	82
Недостиг на специалисти по киберсигурност	88	75
Атаки срещу веригата за доставки	78	88



Фиг. 4: Бъдещи технологии за киберсигурността



Фиг. 5: Бъдещи предизвикателства пред киберсигурността

Заключение

Киберсигурността е неразделна част от функционирането на съвременните автоматизирани индустриални системи. С нарастващата дигитализация и свързаност на производствените процеси необходимостта от надеждна защита става все по-голяма. Ефективната киберсигурност изисква съчетание от технически решения, организационни мерки и добре обучен персонал. Само чрез комплексен подход могат да бъдат намалени рисковете и да се гарантира непрекъснатата работа на критичните индустриални системи. В бъдеще значението на киберсигурността ще продължи да нараства, тъй като индустриалните технологии стават все по-интелигентни и взаимосвързани. Защитата на тези системи е от съществено значение за икономическата стабилност, безопасността и устойчивото развитие на обществото. Освен технологичен проблем, киберсигурността е и организационно предизвикателство, което изисква координирани усилия между ръководството, техническите специалисти и всички служители в предприятието. Само чрез активно сътрудничество могат да бъдат постигнати високи нива на защита и устойчивост. В условията на все по-динамична дигитална среда предприятията трябва да възприемат киберсигурността като непрекъснат процес, а не като еднократно действие. Постоянният мониторинг, актуализирането на защитните механизми и адаптирането към новите заплахи са ключови фактори за успешното функциониране на индустриалните системи. [8]

Литература

1. Denev, D., & Tsankov, Ts. (2020). Development of a virtual private network in computer networks and communication environments. SocioBrains, 71, 11–19.
2. Denev, D., & Tsankov, Ts. (2021). Analytical study of the delay introduced as a result of encryption/decryption of voice transmitted over VPN networks. Journal Scientific and Applied Research, 20, 73–77.
3. Denev, D., & Tsankov, Ts. (2022). Design and implementation of a field level of an industrial communication network for the needs of the industry.

Proceedings of the 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST 2022), 1–4.

4. Denev, D., & Tsankov, Ts. (2022). Communication-based dynamic packet optimization for visual PLC monitoring. Proceedings of the Annual University Scientific Conference of Vasil Levski National Military University, 1259–1266.
5. Denev, D. (2022). Modeled security in communication network coding. Annual of Konstantin Preslavsky University of Shumen, XII E, 153–161.
6. Denev, D. (2023). Surveillance with Wireshark and its use in communication networks. Annual of Konstantin Preslavsky University of Shumen, XIII E, 104–109.
7. Iliev, D., & Denev, D. (2024). Computer security and traffic management in communication networks. Proceedings of the International Scientific Conference MATTECH 2024, 2: Communication and Computer Technologies, 161–169.
8. Denev, D., & Dimitrova, E. (2024). Security and vulnerabilities in Zigbee technology. Annual of Konstantin Preslavsky University of Shumen, XIV E, 92–97.
9. Denev, D., & Petrov, I. (2026). Cybersecurity in multimedia networks of automated systems. Annual of Konstantin Preslavsky University of Shumen, XV E, 61–73.
10. Denev, D., & Danev, A. (2026). Building a multisegment IP network with traffic prioritization and network translation through QoS and NAT mechanisms in Cisco Packet Tracer. Annual of Konstantin Preslavsky University of Shumen, XV E, 47–60.
11. Тахиров, М., & Симеонова, И. (2025). Защита на административните процеси от външни и вътрешни заплахи. Национална научна конференция на Националния военен университет „Васил Левски“, Велико Търново, 12–14 ноември 2025 г.
12. Stefanova, A. (2026). Cyber resilience of geodetic systems as an element of digital infrastructure. Security and Defense, 5(1), 93–101.

HYBRID MODEL FOR RELIABILITY ASSESSMENT OF INTELLIGENT VIDEO SURVEILLANCE SYSTEMS USING FMEA AND MONTE CARLO SIMULATIONS

Silvia Hr. Nikolova

Faculty of Technical Sciences, Department of Communication and Computer Engineering and Security Technologies, Konstantin Preslavsky University of Shumen, Shumen, Bulgaria, silvia_nikolova73@abv.bg

***Abstract**: This paper proposes a normalized hybrid reliability model for AI-enabled video surveillance systems. The model integrates Failure Mode and Effects Analysis, component failure intensities, an AI uncertainty coefficient and Monte Carlo simulation. A six-subsystem case study with 10,000 iterations compares analytical, simulation and test-bench estimates. The communication network and AI analysis module are identified as dominant risk contributors. Monte Carlo reliability is 0.907, close to the test-bench estimate of 0.901, while the analytical model gives 0.921. The approach supports traceable prioritization of mitigation measures and quantifies uncertainty through 95% confidence intervals.*

***Keywords**: Artificial intelligence, Video surveillance, Reliability, FMEA, Monte Carlo simulation, Risk assessment*

ХИБРИДЕН МОДЕЛ ЗА ОЦЕНКА НА НАДЕЖДНОСТТА НА ИНТЕЛИГЕНТНИ СИСТЕМИ ЗА ВИДЕОНАБЛЮДЕНИЕ ЧРЕЗ FMEA И МОНТЕ КАРЛО СИМУЛАЦИИ

Силвия Хр. Николова

Факултет по технически науки, катедра „Комуникационна и компютърна техника и технологии за сигурност", Шуменски университет „Епископ Константин Преславски", гр. Шумен, България, silvia_nikolova73@abv.bg

***Резюме**: Предложен е нормализиран хибриден модел за надеждност на AI-базирани системи за видеонаблюдение, който интегрира FMEA, интензивности на отказите, коефициент за алгоритмична неопределеност и Монте Карло симулация. Казус с шест подсистеми и 10 000 итерации сравнява аналитична, симулационна и стендова оценка. Комуника-ционната мрежа и AI модулът са водещи рискови фактори. Получената симулацион-на надеждност 0,907 е близка до стендовата оценка 0,901, докато аналитичният модел дава 0,921. Методът осигурява проследимо приоритизиране на мерките и количест-вена оценка на неопределеността.*

***Ключови думи**: Изкуствен интелект, Видеонаблюдение, Надеждност, FMEA, Монте Карло, Оценка на риска*

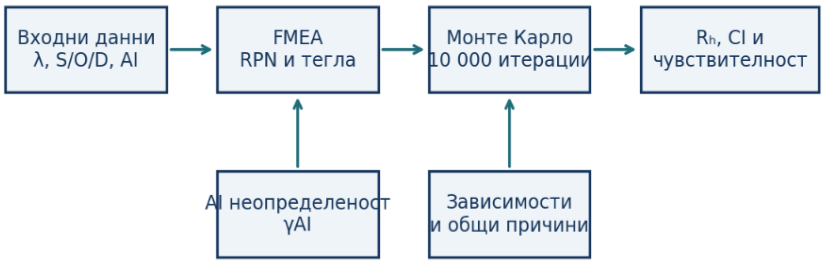
Въведение

Интелигентните системи за видеонаблюдение съчетават камери, IoDT сензори, комуникационна инфраструктура, периферни или облачни изчисления и модели за машинно обучение [6], [7], [8]. Поради това отказът вече не е само физическо прекъсване: пропуснат обект, неправилна класификация, дрейф на данните или прекомерна латентност също могат да доведат до неизпълнение на охранителната функция [8], [9]. Класическите последователни модели са прозрачни, но обичайно предполагат независими откази и постоянни интензивности [4], [5], [10]. FMEA приоритизира критичните режими, но RPN е относителна, ординална оценка [1], [11]. Монте Карло позволява въвеждане на неопределеност и зависимости, но изисква аргументирани входни параметри [3].

Целта е да се разработи възпроизводим хибриден модел, в който FMEA определя приоритетите и корекциите на вероятностите, а симулацията оценява системната надеждност и доверителния интервал [2]. Научният принос е: (1) нормализирана интеграция на RPN и AI неопределеност без риск от невалидни стойности; (2) сравнение на аналитична, симулационна и стендова оценка; (3) чувствителност на отказите на AI и комуникационната подсистема. Представените числени резултати са симулационен казус и демонстрационен стендов набор, а не статистика от сертификационно изпитване.

Архитектура и режими на отказ

Изследваната архитектура включва AI камери, комуникационна мрежа, IoDT сензори, модул за AI анализ, роботизирана въздушна платформа и център за управление. Успехът на мисията се дефинира като своевременно откриване, правилна интерпретация и доставяне на аларма до оператор. Критериите за отказ включват загуба на видео, прекъсване на канала, пропуснато събитие, фалшива аларма над допустимия праг, недостъпност на изчислителен ресурс и невъзможност за потвърждение от оператора.



Фиг. 1: Последователност на предложения хибриден алгоритъм

1. Математическо описание на хибридния модел

1.1 .Аналитична надеждност и FMEA

Нека системата съдържа компоненти $C=\{C_1,\ldots,C_n\}$. При експоненциален закон надеждността на компонент i за интервал t е $R_i(t)=\exp(-\lambda_i t)$. За последователна структура базовата аналитична оценка е:

$$R_a(t) = \prod_{i=1}^{n} exp(-\lambda_i t) \quad (1)$$

За всеки режим на отказ FMEA задава тежест S_i, честота O_i и откриваемост D_i по скала 1–10. Приоритетният номер и нормализираното рисково тегло са:

$$RPN_i = S_i O_i D_i, \quad \rho_i = RPN_i / \sum_j RPN_j \quad (2)$$

Така $\sum \rho_i=1$ и FMEA служи като разпределение на приоритета, а не като вероятност за отказ. Това избягва неправомерното директно изваждане на RPN от надеждност.

1.2. AI неопределеност и коригирани вероятности

Алгоритмичната неопределеност се оценява чрез четири валидирани показателя A (accuracy), P (precision), Re (recall) и F_1. За да се отчете по-високата цена на пропуска, recall получава двойно тегло:

$$\gamma AI = 1 - (A + P + 2Re + F_1)/5\,, \quad 0 \le \gamma AI \le 1 \quad (3)$$

Базовата вероятност $q_i=1-\exp(-\lambda_i t)$ се коригира с ограничена FMEA добавка и фактор на средата z_i:

$$q_i* = min\{1, q_i[1 + \alpha \rho_i + \beta z_i] + \mathbb{1}AI(i)\gamma AI\} \quad (4)$$

където α и β се калибрират чрез исторически или стендови данни, а 𝟙AI(i) е индикатор за AI модула. При липса на достатъчно данни се използват сценарийни диапазони и се докладва чувствителност.

1.3. Монте Карло оценка и доверителен интервал

В итерация k се генерира вектор на отказите $X^{(k)}$. Независимият случай използва $U_i \sim U(0,1)$ и $X_i=1$ при $U_i<q_i*$. Общопричинните откази се въвеждат чрез Bernoulli променлива за комуникационно-захранваща група; при задействане тя изменя едновременно съответните X_i. Функцията g(X) е 1, ако мисията е успешна, и 0 в противен случай. Тогава:

$$RMC = (1/N)\sum_{k=1}^{N} g(X^{(k)}),\ CI_{95} = RMC \pm 1{,}96\sqrt{[RMC(1-RMC)/N]} \quad (5)$$

Крайната хибридна оценка е R_h=RMC, защото FMEA и γAI вече са включени в q_i*. Отделно се докладват ρ_i и γAI, което запазва интерпретируемостта и предотвратява двойно отчитане на риска.

2. Алгоритъм и експериментална постановка

Алгоритъм 1. HybridReliabilityAssessment

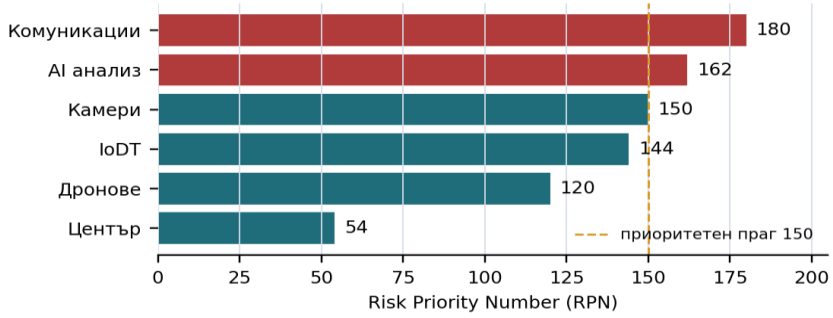
Вход: C, λ, S/O/D, AI метрики, сценарии z, N.
1: изчисли RPN_i и ρ_i; 2: изчисли γAI и q_i*;
3: за k=1…N генерирай общопричинни и компонентни откази;
4: оцени $g(X^{(k)})$ според логиката на мисията;
5: изчисли RMC, CI_{95} и приносите чрез one-at-a-time анализ;
Изход: R_h, CI_{95}, ранжирани рискове и препоръчани мерки.

Симулационният казус използва N=10 000, времеви хоризонт една мисия, независими компонентни откази плюс сценарий за обща комуникационна причина. Демонстрационната стендова оценка е формирана от повтаряеми изпитвания с инжектиране на загуба на пакет, закъснение, деградирала осветеност и пропуски на AI детектора. За AI модула са зададени A=0,936, P=0,924, Re=0,902 и F_1=0,913, откъдето γAI=0,069. Параметрите са предназначени за проверка на метода; при внедряване трябва да се заменят с наблюдавани данни.

3. Резултати

Таблица 1. FMEA приоритизация на подсистемите

Подсистема	S	O	D	RPN	Дял ρ
Комуникационна мрежа	9	5	4	180	22,2%
AI анализ	9	6	3	162	20,0%
Камери	6	5	5	150	18,5%
IoDT сензори	6	6	4	144	17,8%
Дронове	5	6	4	120	14,8%
Център за управление	6	3	3	54	6,7%

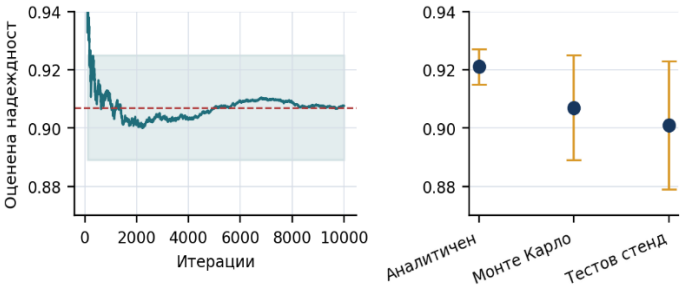


Фиг. 2: RPN профил и приоритетен праг

Комуникационната мрежа е с най-висок RPN=180, следвана от AI анализа (162). Двата компонента формират 42,2% от нормализирания FMEA приоритет. При праг RPN≥150 незабавни коригиращи действия се изискват още за камерите. Центърът за управление има по-нисък RPN поради резервираност и добра откриваемост, но остава критичен при общопричинен отказ.

Таблица 2. Сравнение на оценките за надеждност

Метод	R	Ст. откл.	95% интервал	Отклонение спрямо стенд
Аналитичен	0,921	0,003	0,915–0,927	+2,22%
Монте Карло	0,907	0,009	0,889–0,925	+0,67%
Демонстр. стенд	0,901	0,011	0,879–0,923	—



Фиг. 3: Сходимост на Монте Карло и 95% доверителни интервали

Монте Карло оценката се различава от стендовата с 0,006 абсолютни пункта (0,67% относително), докато аналитичният модел я надценява с 0,020 пункта (2,22%). При 10 000 итерации оценката се стабилизира около 0,907. Частичното припокриване на интервалите показва, че резултатът е съвместим със стендовия набор, но не доказва универсално превъзходство; необходимо е валидиране върху независими обекти.

4. Дискусия

Полученото разминаване е очаквано: аналитичният модел третира компонентите като независими и не включва алгоритмични грешки, докато хибридният модел отчита γAI, сценарийна деградация и общи причини. Чувствителността показва, че намаляване на комуникационната вероятност за отказ с 30% повишава R_h приблизително с 1,1 процентни пункта; подобряване на

recall от 0,902 на 0,940 намалява γAI и добавя около 0,6 пункта. Комбинираната мярка — резервиран комуникационен канал, наблюдение на дрейфа и периодично прекалибриране — има по-голям ефект от изолирана хардуерна подмяна [13], [14].

Практическите ограничения са три. Първо, S/O/D съдържат експертна субективност; препоръчва се Delphi оценяване и анализ на съгласието [12]. Второ, експоненциалният закон е опростяване при стареене и профилактика. Трето, демонстрационните данни не заменят полево изпитване. За сертификационна употреба входовете трябва да се проследят до журнали, тестови протоколи и версия на AI модела. Независимо от това методът е приложим за сравнение на архитектури и за планиране на мерки още на проектен етап.

Заключение

Разработен е хибриден модел, който свързва FMEA с вероятностна симулация, без да интерпретира RPN като директна вероятност. Нормализираните тегла ρ_i приоритизират режимите, γAI описва качеството на алгоритмичното решение, а Монте Карло включва сценарийна неопределеност и общопричинни откази. В разгледания казус R_h=0,907 е по-близо до демонстрационната стендова оценка 0,901 от аналитичната стойност 0,921. Комуникационната мрежа и AI модулът са водещите направления за подобрение. Бъдещата работа включва Bayesian актуализация на λ_i, моделиране на времезависим дрейф и валидиране в реални обекти за критична инфраструктура.

Литература

1. IEC. (2018). IEC 60812:2018—Failure modes and effects analysis (FMEA and FMECA). International Electrotechnical Commission.
2. ISO. (2018). ISO 31000:2018—Risk management—Guidelines. International Organization for Standardization.
3. Rubinstein, R. Y., & Kroese, D. P. (2017). Simulation and the Monte Carlo method (3rd ed.). Wiley.
4. Modarres, M., Kaminskiy, M., & Krivtsov, V. (2016). Reliability engineering and risk analysis (3rd ed.). CRC Press.
5. O'Connor, P. D. T., & Kleyner, A. (2012). Practical reliability engineering (5th ed.). Wiley.
6. Nikolova, S. (2024a). Design, development and research of process efficiency in a robotic intelligent security system "TEDI". KNOWLEDGE – International Journal, 63(3), 289–295.
7. Nikolova, S. (2024b). Exploring artificial intelligence machine learning in video surveillance. MATTEH 2024, 2, 17–22.
8. Nikolova, S. (2024c). Application of convolutional neural networks for object recognition in AI video cameras. MATTEH 2024, 2, 136–142.
9. NIST. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

10. Saleh, J. H., & Marais, K. (2006). Highlights from the early (and pre-) history of reliability engineering. Reliability Engineering & System Safety, 91(2), 249–256.
11. Arabadzhieva-Kalcheva, N., & Tsankov, Ts. (2022). Failure Modes and Effects Analysis – FMEA. Proceedings of the Scientific Conference with International Participation MATTEH 2022, 2, 58–62. ISSN 1314-3921.
12. Arabadzhieva-Kalcheva, N., Tsankov, Ts., Todorova, M., & Marinova, G. (2024). Application of Failure Mode and Effects Analysis for evaluating human reliability. Proceedings of the Scientific Conference with International Participation MATTEH 2024, 2, 147–152. https://doi.org/10.46687/BOIK9859
13. Hristova, E., Denev, D., & Tsankov, Ts. (2024). A survey of data quality in industrial networks and enhancing their reliability complex indicator for the needs of the industry. Environment. Technology. Resources, II, 120–126. https://doi.org/10.17770/etr2024vol2.8036
14. Denev, D., Hristova, E., & Tsankov, Ts. (2023). Improving network communication and enhancing the reliability of programmable devices in the industry. Annual of Konstantin Preslavsky University of Shumen, XIII E, 38–51. ISSN 1314-8818.

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**, Faculty of Artillery, Air Defense and Communication and Information Systems

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON SOCIAL WORK

Stefaniya M. Chervenkova[1], Daniel R. Denev[2]

Faculty of Technical Sciences, Department of Communication and Computer Engineering and Security Technologies, Konstantin Preslavsky University of Shumen, Shumen, Bulgaria, [1]2540090023@shu.bg, [2]d.denev@shu.bg

***Abstract**: Artificial intelligence is becoming one of the most significant technological innovations of the 21st century and is having an impact on various social spheres, including social work. Its application offers new opportunities for information analysis, improving administrative processes and increasing the quality of social services provided. At the same time, a number of ethical and professional challenges arise related to the protection of personal data, the fairness of algorithms and the role of the human factor. This report examines the main aspects of the impact of artificial intelligence on social work, analysing both the potential benefits and possible risks.*

***Keywords**: Artificial intelligence, Personal data, Information*

ВЛИЯНИЕТО НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ ВЪРХУ СОЦИАЛНАТА РАБОТА

Стефания М. Червенкова[1], Даниел Р. Денев[2]

Факултет по технически науки, катедра „Комуникационна и компютърна техника и технологии за сигурност", Шуменски университет „Епископ Константин Преславски", гр. Шумен, България, [1]2540090023@shu.bg, [2]d.denev@shu.bg

***Резюме**: Изкуственият интелект се превръща в една от най-значимите технологични иновации на XXI век и оказва влияние върху различни обществени сфери, включително социалната работа. Неговото приложение предлага нови възможности за анализ на информация, подобряване на административните процеси и повишаване качеството на предоставяните социални услуги. В същото време възникват редица етични и професионални предизвикателства, свързани със защитата на личните данни, справедливостта на алгоритмите и ролята на човешкия фактор. Настоящият доклад разглежда основните аспекти на влиянието на изкуствения интелект върху социалната работа, като анализира както потенциалните ползи, така и възможните рискове.*

***Ключови думи**: Изкуствен интелект, Лични данни, Информация*

Въведение

Развитието на цифровите технологии променя организацията и предоставянето на социални услуги. Изкуственият интелект осигурява инструменти за обработване на големи обеми данни, разпознаване на зависимости и подпомагане на решенията. В социалната работа тези възможности могат да подобрят оценката на потребностите, планирането на интервенции и разпределението на ограничените ресурси. Дигитализацията създава условия и за по-бързо обслужване и по-добра

подкрепа на уязвимите групи [11]. Прилагането на подобни технологии обаче засяга чувствителни лични данни и решения, свързани с човешкото благополучие, поради което изисква професионален контрол и спазване на етични принципи. Целта на доклада е да анализира основните възможности и ограничения на изкуствения интелект в социалната работа, като разгледа влиянието му върху административната ефективност, оценката на потребностите, достъпа до услуги и ролята на социалния работник. На фиг. 1 е представен концептуален модел на взаимодействието между изкуствения интелект и социалната работа [2].

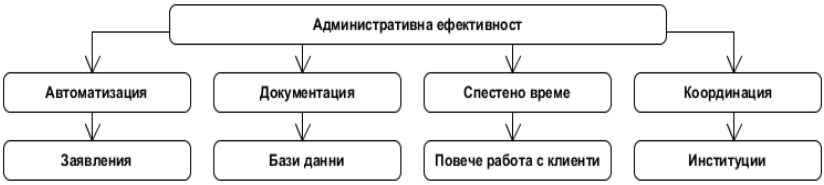


Фиг. 1: Концептуален модел на взаимодействието между ИИ и социалната работа

Подобряване на административната ефективност

Една от най-съществените ползи от използването на изкуствен интелект в социалната работа е намаляването на административната натовареност. Социалните работници често отделят значителна част от времето си за попълване на документи, обработка на заявления и изготвяне на отчети. Чрез автоматизиране на тези дейности ИИ може да съкрати времето за административна работа и да позволи на специалистите да се съсредоточат върху директната подкрепа на клиентите. Освен това интелигентните системи могат да организират и анализират информация от различни източници. Обработката и анализът на такава информация улесняват достъпа до необходимите данни и тяхното последващо използване [8]. Това води до по-бързо вземане на решения и по-ефективно управление на случаите, което повишава качеството на социалните услуги. Съвременните системи с изкуствен интелект могат да подпомагат обработката на голям брой документи за кратко време, като автоматично извличат важна информация и я подреждат в структуриран вид. Това намалява вероятността от допускане на технически грешки и улеснява проследяването на развитието на отделните случаи. По този начин организациите могат да поддържат по-добра отчетност и да реагират по-бързо при възникване на необходимост от намеса. Допълнително предимство е възможността за оптимизиране на вътрешната комуникация между различни институции и специалисти. Когато информацията се обработва и споделя чрез интелигентни системи, се съкращава времето за

координация и се подобрява сътрудничеството между социални служби, здравни заведения и образователни институции. Това създава предпоставки за по-цялостен подход към потребностите на клиентите. На фиг. 2 е показана схема на основните ползи от автоматизацията в социалната работа. [4]



Фиг. 2: Основни ползи от автоматизацията в социалната работа

Подпомагане на оценката и вземането на решения

Изкуственият интелект предоставя възможност за обработка на големи масиви от данни и откриване на закономерности, които биха могли да останат незабелязани от човека. В социалната работа това може да бъде използвано за идентифициране на рискови фактори, прогнозиране на нуждите на определени групи и оценка на вероятността от настъпване на социални проблеми. Чрез анализ на наличната информация специалистите могат да получат допълнителна подкрепа при планирането на интервенции и разпределението на ресурси. Важно е обаче решенията да не се основават единствено на алгоритмични оценки, а да се съчетават с професионалната преценка и опита на социалните работници. Чрез използване на предиктивни модели социалните институции могат да разпознават тенденции в развитието на определени социални проблеми. Например анализът на демографски и икономически показатели може да помогне за прогнозиране на повишен риск от социално изключване, бедност или безработица в дадени общности. Подобна информация позволява предприемането на превантивни мерки още преди проблемите да се задълбочат. Освен това интелигентните технологии могат да подпомогнат оценката на ефективността на различни социални програми. Чрез сравняване на резултати и анализ на събраните данни става възможно по-точното определяне на това кои интервенции дават най-добри резултати. В таблица 1 е показано влиянието на ИИ върху процеса на оценка и вземане на решения [1].

Данните показват, че използването на изкуствен интелект може да подпомогне социалните работници чрез по-бърз анализ на информацията и по-точно идентифициране на рисковите случаи. Намаляването на времето за оценка позволява по-бърза реакция при необходимост от социална интервенция, докато повишената точност допринася за по-ефективно насочване на потребителите към подходящи услуги.

Таблица 1: Влияние на ИИ върху процеса на оценка и вземане на решения

Показател	Без използване на ИИ	С използване на ИИ	Промяна
Средно време за анализ на случай (мин.)	120	75	-37,5%
Обработени случаи на месец	80	115	+43,8%
Точност при идентифициране на рискови случаи	78%	91%	+13%
Време за изготвяне на оценка (дни)	5	3	-40%
Успешно насочени случаи към подходяща услуга	72%	88%	+16%

Подобряване на достъпа до социални услуги

Използването на интелигентни дигитални инструменти създава възможности за по-лесен достъп до социални услуги. Чатботове, виртуални асистенти и онлайн платформи могат да предоставят информация и първоначални консултации по всяко време на денонощието. Това е особено полезно за хора, които живеят в отдалечени райони или изпитват затруднения при посещението на социални институции. Благодарение на тези технологии гражданите могат по-бързо да получават насоки относно своите права, възможностите за социално подпомагане и необходимите административни процедури [9]. По този начин се улеснява комуникацията между институциите и потребителите на социални услуги. Дигиталните платформи, базирани на изкуствен интелект, могат да предоставят персонализирана информация според конкретните нужди на потребителите. Вместо да търсят информация от множество източници, гражданите могат да получат насоки за подходящите услуги, програми и форми на подпомагане чрез една централизирана система. Това прави процеса по-достъпен и по-лесен за разбиране. Особено важно е значението на тези технологии за хора с увреждания или ограничени възможности за придвижване. Чрез гласови асистенти, автоматичен превод и адаптирани интерфейси се създават условия за по-голяма социална включеност. В таблица 2 е показано влиянието на ИИ върху достъпа до социални услуги [3].

Таблица 2: Влияние на ИИ върху достъпа до социални услуги

Показател	Преди внедряване на ИИ	След внедряване на ИИ	Промяна
Средно време за получаване на информация (мин.)	30	5	-83,3%
Брой обслужени потребители месечно	500	750	+50%
Достъп до услуги извън работно време	10%	85%	+75%
Онлайн подадени заявления	120	380	+216,7%
Удовлетвореност на потребителите	74%	89%	+15%

Представените данни показват, че използването на инструменти с изкуствен интелект може значително да подобри достъпа до социални услуги. Намаленото време за получаване на информация и увеличеният брой обслужени потребители свидетелстват за по-висока ефективност на обслужването. Освен това възможността за достъп до услуги извън стандартното работно време и увеличеният брой онлайн заявления улесняват гражданите и повишават тяхната удовлетвореност от предоставяната социална подкрепа. [6]

Етични предизвикателства и защита на личните данни

Наред с положителните страни на изкуствения интелект възникват и редица етични въпроси. Социалната работа борави с чувствителна информация, свързана със здравословно състояние, семейни отношения, финансово положение и други лични данни. Използването на интелигентни системи изисква високо ниво на защита на тази информация и гарантиране на поверителността. Допълнително предизвикателство представлява рискът от алгоритмична дискриминация. Ако данните, използвани за обучението на дадена система, съдържат съществуващи социални предразсъдъци, е възможно те да бъдат възпроизведени в процеса на вземане на решения. Поради тази причина е необходимо разработването на ясни етични стандарти и механизми за контрол [10], [13]. С нарастването на зависимостта от цифрови технологии се увеличава и необходимостта от прозрачност при тяхното използване. Потребителите трябва да бъдат информирани по какъв начин се събират, съхраняват и обработват техните данни [12]. Липсата на достатъчна прозрачност може да доведе до намаляване на доверието в социалните институции и до нежелание за използване на предоставяните услуги. Друг съществен аспект е въпросът за отговорността при вземане на решения. Когато дадена система предостави препоръка или оценка, е необходимо ясно да се определи кой носи отговорност за крайния резултат. Независимо от степента на автоматизация, професионалистите следва да запазят контрола върху процеса и да могат да аргументират своите решения пред клиентите и обществото. На фиг. 3 е показана схема на етичните предизвикателства и защита на личните данни. [7]



Фиг. 3: Етични предизвикателства и защита на личните данни

Ролята на човешкия фактор в социалната работа

Въпреки бързото развитие на технологиите изкуственият интелект не може напълно да замени социалния работник. Основата на социалната работа е изграждането на доверие, емпатия и подкрепящи взаимоотношения между специалиста и клиента. Тези качества са свързани с човешките емоции и социалната чувствителност, които трудно могат да бъдат възпроизведени от компютърни системи. Изкуственият интелект следва да се разглежда като инструмент, който подпомага професионалната дейност, а не като заместител на човешкото участие. Най-добри резултати могат да бъдат постигнати чрез комбиниране на технологичните възможности с професионалната компетентност и етичната отговорност на социалните работници. Социалната работа често включва взаимодействие с хора, които преживяват трудни житейски ситуации, емоционални кризи или социална изолация. В подобни случаи подкрепата не се изчерпва с предоставяне на информация или административна помощ. Необходима е способност за разбиране на индивидуалните преживявания и създаване на усещане за сигурност, което е характерно за човешкото общуване. Същевременно навлизането на изкуствения интелект изисква развитие на нови компетентности сред социалните работници. Те трябва да умеят да използват технологичните инструменти ефективно и критично да оценяват получените резултати. Това предполага непрекъснато обучение и адаптиране към променящата се професионална среда, в която технологиите и човешката експертиза работят съвместно за постигане на по-добри социални резултати. [5]

КАЗУС: Подкрепа на самотен възрастен човек

В социална служба постъпва сигнал за 78-годишен мъж, който живее сам и има затруднения при ежедневните дейности. Система с изкуствен интелект анализира наличните данни и препоръчва предоставяне на помощ за доставка на храна и лекарства, тъй като това е най-често използваната услуга при сходни случаи. При посещение на социален работник обаче се установява, че основният проблем не е липсата на материална подкрепа, а социалната изолация и влошеното психическо състояние на лицето след загубата на съпругата му. След разговор и оценка на ситуацията специалистът организира включване в дневен център за възрастни хора и регулярни социални контакти.

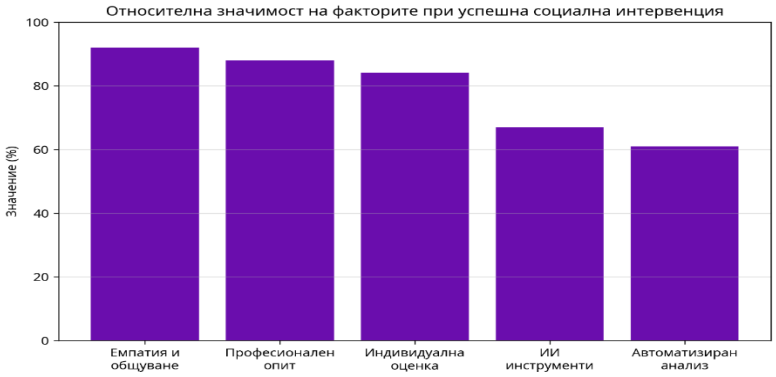
РЕШЕНИЕ

Казусът показва, че изкуственият интелект може успешно да подпомага процеса на анализ и да предлага възможни решения, но не може напълно да оцени емоционалните и психологическите аспекти на човешките проблеми. Професионалната преценка, емпатията и личният контакт остават ключови елементи в социалната работа. Най-ефективният подход е съчетаването на технологичните възможности с експертната намеса на социалния работник. Таблица 3 и Фигура 4 представят значимостта на основните фактори при социалната работа и показват, че въпреки ползите от изкуствения интелект,

човешкият фактор остава определящ за успешната социална интервенция.

Таблица 3: Значение на различни фактори при социалната работа (%)

Фактор	Значение (%)
Емпатия и общуване	92
Професионален опит	88
Индивидуална оценка	84
Използване на ИИ инструменти	67
Автоматизиран анализ на данни	61



Фиг. 4: Относителна значимост на факторите при успешна социална интервенция

Заключение

Изкуственият интелект създава възможности за автоматизиране на административни процеси, анализ на данни и подобряване на достъпа до социални услуги. Той може да подпомага специалистите при оценяване на потребностите и разпределяне на ресурсите, но не може да замени професионалната преценка, емпатията и личния контакт. Прилагането му поставя въпроси, свързани със защитата на личните данни, справедливостта, прозрачността и отговорността за взетите решения. Поради това интелигентните системи трябва да се използват като помощен инструмент под човешки контрол. Съчетаването на технологичните възможности с професионалните и етичните принципи е основно условие за устойчиво развитие на социалните услуги и защита на хората, които се нуждаят от подкрепа.

Литература

1. O'Leary, P., & Tsui, M. (2023). AI and social work. International Social Work, 66(5), 1353–1354.
2. Duran, R. (2026). Social workers' concerns about artificial intelligence: The mediating role of ethics and innovation. Journal of Social Work. Advance online publication.
3. Lehtiniemi, T. (2024). Contextual social valences for artificial intelligence: Anticipation that matters in social work. Information, Communication & Society, 27(6), 1110–1125.
4. Reamer, F. G. (2023). Artificial intelligence in social work: Emerging ethical issues. International Journal of Social Work Values and Ethics, 20(2), 52–71.
5. Meilvang, M. L. (2023). Working the boundaries of social work: Artificial intelligence and the profession of social work. Professions and Professionalism, 13(1).
6. Fernando, N., & Ranasinghe, P. (2023). Integration of artificial intelligence in social work: Opportunities, challenges, and considerations. Journal of Computational Social Dynamics, 8(9), 13–24.
7. Hagerty, A., & Rubinov, I. (2019). Global AI ethics: A review of the social impacts and ethical implications of artificial intelligence.
8. Тодорова-Лазарова, В. П. (2025). Dynamic arrays in MS Excel for data processing and analysis in information systems. Proceedings of the International Scientific Conference UNITECH 2025, 1–6.
9. Konstantinova, E., & Tsankov, Ts. (2020). Social assistance with the help of operational programs from the European Union. International Scientific Refereed Online Journal with Impact Factor SocioBrains, 75, 62–68. Sofia: Smart Ideas – Wise Decisions Ltd. ISSN 2367-5721.
10. Nikolova, S., & Tsankov, Ts. (2025). Cognitive and ethical failures in AI-based scientific reviewing. Journal Scientific and Applied Research, 28, 207–215. ISSN 1314-6289.
11. Konstantinova, E., & Tsankov, Ts. (2021). An overview of sustainable urbanism with the help of artificial intelligence. Proceedings of the Ninth Student Scientific Conference "Ecology and Environment", 109–121. ISSN 2367-5209.
12. Simeonova, I. (2025). How GDPR treats automated decision-making. Journal Scientific and Applied Research, 28(1). Shumen: Konstantin Preslavsky University Press. ISSN 1314-6289.
13. Stefanova, A. A. (2025). Responsible geodesy: Ethical and sustainable models for the digital transformation of geodesy. Annual of Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, XV E, 399–410.

EXPLAINABLE ARTIFICIAL INTELLIGENCE IN MANUFACTURING SYSTEMS

Yuray Yu. Mehmedov[1], Ivaylo I. Petrov[2]

Faculty of Technical Sciences, Department of Communication and Computer Engineering and Security Technologies, Konstantin Preslavsky University of Shumen, Shumen, Bulgaria, [1]2470080006@shu.bg, [2]2470020007@shu.bg

***Abstract**: Explainable Artificial Intelligence is an approach to developing intelligent systems in which algorithmic decisions can be understood and interpreted by humans. This is especially important in manufacturing systems, where automation and optimization play a key role. As the use of artificial intelligence in industry increases, the need for transparency in decision-making arises. Manufacturing processes often involve complex dependencies and critical operations, making understanding algorithms a must. Explainable Artificial Intelligence helps engineers and operators analyse, validate, and improve systems. This leads to higher confidence in automated decisions and reduced risk of errors.*

***Keywords**: Artificial intelligence, Manufacturing systems, Industry*

ОБЯСНИМ ИЗКУСТВЕН ИНТЕЛЕКТ В ПРОИЗВОДСТВЕНИТЕ СИСТЕМИ

Юрай Ю. Мехмедов[1], Ивайло И. Петров[2]

Факултет по технически науки, катедра „Комуникационна и компютърна техника и технологии за сигурност", Шуменски университет „Епископ Константин Преславски", гр. Шумен, България, [1]2470080006@shu.bg, [2]2470020007@shu.bg

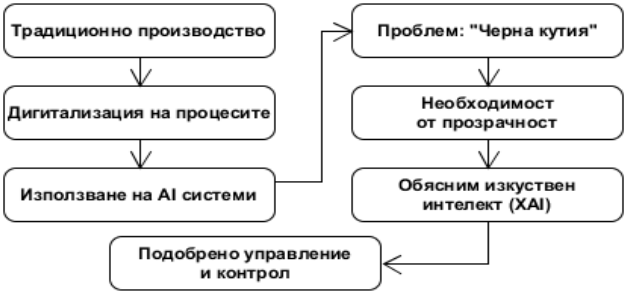
***Резюме**: Обяснимият изкуствен интелект представлява подход в развитието на интелигентни системи, при който решенията на алгоритмите могат да бъдат разбрани и интерпретирани от хората. Това е особено важно в производствените системи, където автоматизацията и оптимизацията играят ключова роля. С нарастването на използването на изкуствен интелект в индустрията, възниква необходимостта от прозрачност при вземането на решения. Производствените процеси често включват сложни зависимости и критични операции, което прави разбирането на алгоритмите задължително. Обяснимият изкуствен интелект подпомага инженерите и операторите да анализират, валидират и подобряват системите. Това води до по-високо доверие в автоматизираните решения и намаляване на риска от грешки.*

***Ключови думи**: Изкуствен интелект, Производствени системи, Индустрия*

Въведение

Съвременните производствени системи се развиват бързо благодарение на интеграцията на изкуствен интелект и машинно обучение. Те позволяват автоматизация на процеси, прогнозиране на дефекти и оптимизация на ресурси. Въпреки тези предимства, много от използваните модели функционират като

„черни кутии", при които е трудно да се разбере как се достига до дадено решение. Това създава проблеми при диагностика и контрол. Обяснимият изкуствен интелект цели да преодолее този недостатък, като предоставя методи за интерпретация на моделите. Той дава възможност за проследяване на логиката зад решенията и подобрява управляемостта на системите. В контекста на индустриалното производство, XAI се превръща в ключов инструмент за повишаване на ефективността, сигурността и надеждността на процесите. В допълнение към вече разгледаните аспекти, е важно да се отбележи, че внедряването на обясним изкуствен интелект в производствените системи е пряко свързано с дигиталната трансформация на индустрията. Съвременните предприятия се стремят към т.нар. „умни фабрики", в които всички процеси са взаимосвързани чрез информационни системи. В този контекст XAI не е просто допълнение, а необходим компонент, който гарантира, че автоматизираните решения могат да бъдат наблюдавани, анализирани и при необходимост коригирани от човешки специалисти. Това е особено важно при сложни производствени линии, където една малка грешка може да доведе до значителни загуби. Освен това, ролята на обяснимия AI става все по-значима при интеграцията на различни технологични платформи. Производствените системи често комбинират софтуерни решения, роботизирани механизми и аналитични инструменти, които работят съвместно. Без ясно разбиране на начина, по който тези компоненти взаимодействат, управлението на системата би било затруднено. Именно тук XAI предоставя необходимата прозрачност, като позволява да се проследят причинно-следствените връзки между отделните процеси и резултатите от тяхното взаимодействие. На фиг. 1 е показана схема на еволюцията към обясним AI в производството. [2], [3]

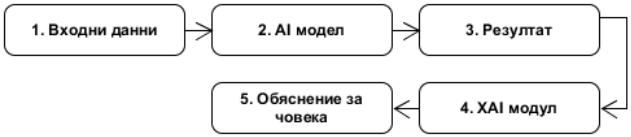


Фиг. 1: *Еволюция към обясним AI в производството*

Същност на обяснимия изкуствен интелект

Обяснимият изкуствен интелект представлява набор от техники, които правят работата на AI моделите разбираема за хората. Това включва визуализации, правила и анализ на факторите, влияещи върху решенията. Основната цел е да се

осигури прозрачност, така че потребителите да могат да разберат защо даден модел взема конкретно решение. Това е особено важно в критични индустриални приложения. Съществуват различни подходи към XAI – като модели с вградена интерпретируемост и външни методи за обяснение. Всеки от тях има своите предимства и ограничения. В производствените системи XAI позволява по-добро разбиране на поведението на алгоритмите и подпомага вземането на информирани решения. Към основните характеристики на обяснимия изкуствен интелект може да се добави и способността му да подпомага анализа на сложни зависимости между данните. В производствените системи често се работи с множество променливи, които влияят върху крайния резултат – температура, налягане, скорост на машините и други. XAI позволява да се идентифицира кои от тези фактори имат най-съществено значение и как те взаимодействат помежду си. Това не само улеснява анализа, но и подпомага вземането на по-информирани управленски решения. Допълнително, обяснимият AI играе важна роля при валидирането на моделите. В традиционните „черни кутии“ е трудно да се определи дали даден модел работи правилно или просто съвпада с данните. Чрез XAI специалистите могат да проверят логиката зад решенията и да установят дали тя е съобразена с реалните производствени процеси. Това намалява риска от грешки и повишава надеждността на системите. На фиг. 2 е показан принципа на работа. [1]



Фиг. 2: Принцип на работа

Приложения в производствените системи

Обяснимият AI намира широко приложение в автоматизацията на производството. Той се използва за контрол на качеството, прогнозиране на дефекти и оптимизация на процесите. Чрез XAI инженерите могат да разберат кои фактори влияят върху качеството на продукцията. Това позволява по-бързо откриване и отстраняване на проблеми. В системите за предиктивна поддръжка XAI помага да се идентифицират причините за повреди в машините. Това намалява престоя и увеличава ефективността. Освен това, XAI подпомага управлението на сложни производствени линии, като осигурява прозрачност и контрол върху автоматизираните решения. Разширявайки приложенията на XAI, може да се отбележи неговата роля в управлението на веригите за доставки. В съвременните производствени предприятия логистиката е тясно свързана с производствения процес, а всяко забавяне може да доведе до сериозни последствия. Чрез обясними модели могат да се анализират причините за закъснения и да се оптимизират

маршрутите и графиците. Това води до по-добра координация между отделните звена на производството. Също така, XAI се използва при персонализацията на производството, където продуктите се адаптират към специфичните изисквания на клиентите. В такива случаи е важно да се разбере как системата взема решения относно конфигурацията на продукта. На фиг. 3 са показани приложенията на обяснимия AI в производството. [5]



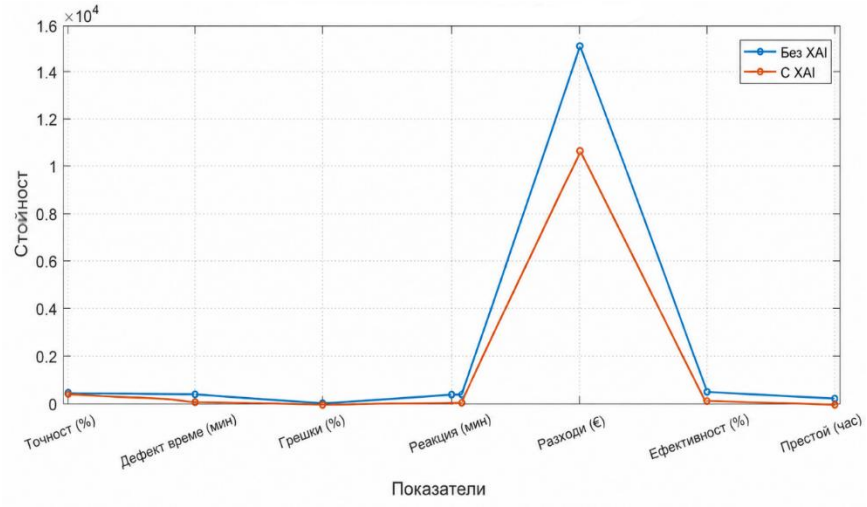
Фиг. 3: Приложения на обяснимия AI в производството

Предимства на обяснимия AI

Едно от основните предимства на XAI е повишеното доверие в системите. Когато решенията са разбираеми, потребителите са по-склонни да ги приемат. Друг важен аспект е подобрената диагностика на грешки. Обяснимостта позволява по-лесно откриване на проблеми в алгоритмите и данните. XAI също така подпомага съответствието със стандарти и регулации, които изискват прозрачност при автоматизирани решения [11]. В допълнение, той улеснява обучението и развитието на персонала, като предоставя по-добро разбиране на технологиите. Освен вече изброените предимства, XAI допринася и за по-добра комуникация между различните отдели в предприятието. Когато решенията на системите са ясно обяснени, те могат да бъдат по-лесно споделени и обсъдени между инженери, мениджъри и оператори. Това създава по-добра координация и води до по-ефективно управление на процесите. Друг важен аспект е възможността за непрекъснато подобрение. Чрез анализ на обясненията, предоставени от XAI, предприятията могат да идентифицират слабости в своите процеси и да предприемат мерки за тяхното отстраняване. Това превръща обяснимия AI в инструмент не само за анализ, но и за стратегическо развитие. Таблица 1 показва предимствата на обяснимия изкуствен интелект в производството, а фиг. 4 сравнителен анализ. [3], [4]

Таблица 1: Предимства на обяснимия изкуствен интелект в производството

№	Показател	Без XAI	С XAI	Подобрение (%)
1	Точност на прогнозиране (%)	78	89	+14%
2	Време за откриване на дефект (мин)	45	20	-55%
3	Производствени грешки (%)	12	5	-58%
4	Време за реакция (мин)	30	12	-60%
5	Разходи за поддръжка (€ / месец)	15 000	10 500	-30%
6	Ефективност на процеса (%)	65	82	+26%
7	Престой на машини (час/месец)	40	18	-55%



Фиг. 4: Сравнителен анализ на ефективността при внедряване на обясним AI

Предизвикателства при внедряване

Въпреки предимствата си, XAI среща редица предизвикателства. Един от тях е балансът между точност и обяснимост. По-сложните модели често са по-точни, но по-трудни за обяснение. Това изисква компромис при избора на подход. Друг проблем е необходимостта от допълнителни ресурси за разработка и внедряване на XAI решения. Това може да увеличи разходите. Освен това, липсата на стандартизирани методи за обяснение затруднява широкото прилагане на XAI в индустрията. Допълнително предизвикателство при внедряването на XAI е

свързано с необходимостта от обучение на персонала. За да могат специалистите да използват ефективно обяснимите модели, те трябва да разполагат с определени знания и умения. Това изисква инвестиции в обучение и развитие, които не всички предприятия са готови да направят. Също така, интеграцията на XAI в съществуващи системи може да бъде сложен процес. Много предприятия разполагат със стари технологии, които не са проектирани с мисъл за обяснимост. Адаптирането им към новите изисквания може да бъде технически предизвикателно и да изисква значителни ресурси. [6]

КАЗУС: Производствено предприятие внедрява система за изкуствен интелект с цел прогнозиране на дефекти в продукцията. Моделът използва голямо количество данни от сензори и показва висока точност (над 90%). Въпреки това, инженерите не могат да разберат как точно се вземат решенията, тъй като моделът функционира като „черна кутия". С течение на времето се появяват проблеми – системата започва да дава некоректни прогнози в определени ситуации, но причината не може да бъде установена. Това води до загуби и намалено доверие в технологията. Допълнително, ръководството изисква обяснение за решенията на системата с цел одит и съответствие със стандарти. Липсата на прозрачност се превръща в сериозно предизвикателство. В резултат на това внедряването на AI системата е поставено под въпрос, въпреки първоначалните добри резултати. Идентифицирани са проблеми:

- Липса на обяснимост на решенията
- Трудност при диагностика на грешки
- Недоверие от страна на персонала
- Невъзможност за одит и контрол

Фиг. 5 показва модела за решение на казуса, а таблица 2 резултатите от внедряване на XAI в производствена система.



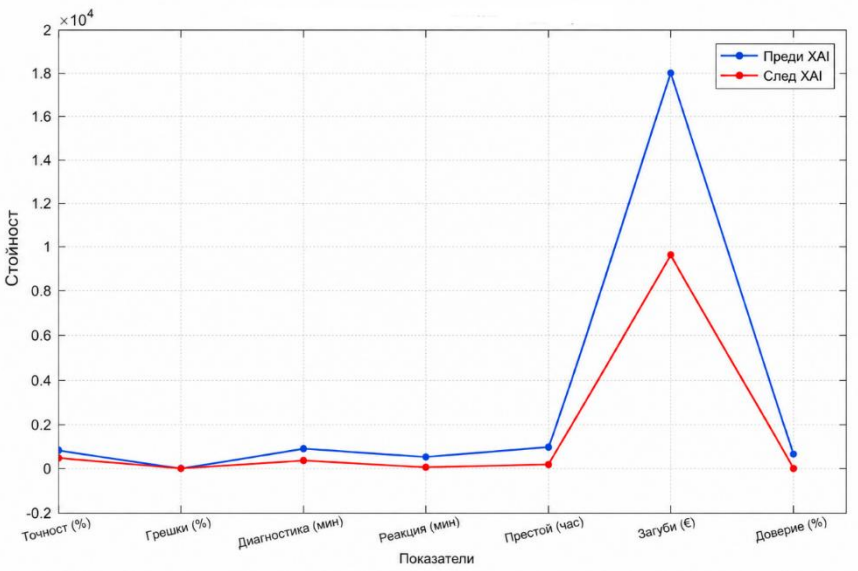
Фиг. 5: Модел за решение

Решение: Предприятието решава да внедри подходи за обясним изкуствен интелект (XAI). Първата стъпка е интеграция на методи за интерпретация на модела, които показват кои фактори влияят най-силно върху прогнозите. След това се внедряват визуализационни инструменти, които позволяват на инженерите да проследяват процеса на вземане на решения. Това улеснява анализа и откриването

на проблеми в данните или модела. Организацията инвестира и в обучение на персонала, за да може той ефективно да използва новите инструменти. Това подобрява взаимодействието между хората и системата. В допълнение, се създават стандартизирани процедури за проверка и валидиране на резултатите, което гарантира по-висока надеждност. Фиг. 6 показва резултатите от решения казус. [7], [9]

Таблица 2: Резултати от внедряване на XAI в производствена система

№	Показател	Преди XAI	След XAI	Промяна (%)
1	Точност на прогнозиране (%)	91	93	+2%
2	Грешни прогнози (%)	14	7	-50%
3	Време за диагностика (мин)	60	25	-58%
4	Време за реакция (мин)	35	15	-57%
5	Престой на машини (час/месец)	48	22	-54%
6	Загуби от дефекти (€ / месец)	18 000	9 500	-47%
7	Ниво на доверие (%)	40	78	+95%



Фиг. 6: Влияние на XAI върху производствени показатели

Бъдеще на обяснимия AI в индустрията

Очаква се XAI да играе все по-важна роля в развитието на интелигентните производствени системи. Технологиите ще стават по-достъпни и ефективни.

Развитието на нови методи ще позволи по-добра интерпретация на сложни модели. Това ще подобри тяхната приложимост в индустрията. Интеграцията на XAI с други технологии като Интернет на нещата (IoT) ще доведе до по-интелигентни и адаптивни системи. В бъдеще обяснимостта ще бъде стандарт, а не допълнение към AI системите. В бъдеще се очаква развитието на XAI да бъде тясно свързано с развитието на автономните производствени системи. Тези системи ще могат самостоятелно да вземат решения и да се адаптират към променящите се условия, но за да бъдат надеждни, те трябва да бъдат и обясними. Това ще изисква разработването на нови методи и технологии, които да комбинират висока ефективност с прозрачност. Освен това, нарастващото значение на етичните аспекти на изкуствения интелект ще постави допълнителни изисквания към обяснимостта. Предприятията ще трябва да гарантират, че техните системи не само работят ефективно, но и вземат решения по справедлив и прозрачен начин. Таблица 3 показва бъдещето на XAI в производството. [8], [10]

Таблица 3: Бъдеще на XAI в производството

№	Показател	2025	2030 (прогноза)	Ръст (%)
1	Внедряване на XAI (%)	25	70	+180%
2	Автоматизирани процеси (%)	40	85	+112%
3	Намаление на грешки (%)	20	60	+200%
4	Ефективност на производството (%)	65	90	+38%
5	Инвестиции в AI (млрд. €)	50	140	+180%

Заключение

Обяснимият изкуствен интелект е ключов елемент в развитието на съвременните производствени системи. Той осигурява прозрачност и доверие в автоматизираните решения. Чрез XAI предприятията могат да подобрят ефективността, качеството и надеждността на своите процеси. Това го прави важен инструмент за индустрията. Въпреки съществуващите предизвикателства, развитието на XAI продължава с бързи темпове. Очаква се той да стане неразделна част от бъдещите технологии. В обобщение може да се каже, че обяснимият изкуствен интелект представлява ключов фактор за успешното внедряване на AI технологии в производствените системи. Той не само подобрява разбирането на процесите, но и създава условия за по-добро управление и контрол. С развитието на индустрията и увеличаването на сложността на системите, необходимостта от обяснимост ще става все по-голяма. Това ще доведе до по-широко разпространение на XAI и до неговото утвърждаване като стандарт в индустриалните приложения.

Литература

1. Denev, D., & Tsankov, Ts. (2022). Communication-based dynamic packet optimization for visual PLC monitoring. Proceedings of the Annual University Scientific Conference of Vasil Levski National Military University, 1259–1266.

2. Denev, D., & Tsankov, Ts. (2022). Design and implementation of a field level of an industrial communication network for the needs of the industry. Proceedings of the 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST 2022), 1–4.
3. Denev, D., & Tsankov, Ts. (2022). A survey of data quality and processing of information in innovative smart devices. Proceedings of the International Conference Automatics and Informatics (ICAI 2022), 1–4.
4. Denev, D., & Tsankov, Ts. (2022). A survey of data quality in digital processing of acoustic signals. Proceedings of the International Conference on Communications, Information, Electronic and Energy Systems (CIEES), 1–4.
5. Denev, D., Hristova, E., & Tsankov, Ts. (2023). Improving network communication and increasing the reliability of programmable devices in industry. Annual of Konstantin Preslavsky University of Shumen, XIII E, 39–52.
6. Denev, D., & Nikolova, S. (2025). A novel algorithm for industrial network reliability estimation and AI-based system optimization. Proceedings of the XXXIII National Conference with International Participation TELECOM, 1–4. https://doi.org/10.1109/TELECOM66943.2025.11304081
7. Dimitrova, E., & Denev, D. (2024). The development of artificial intelligence and its applications in the modern world. Proceedings of the International Scientific Conference MATTEH 2024, 2: Communication and Computer Technologies, 153–160.
8. Denev, D., Yankova-Yordanova, Y., & Konstantinova, E. (2020). Program for managing an automated conveyor for packaged food products and 3D simulation of its work. SocioBrains, 68, 1–7.
9. Danev, A., & Denev, D. (2025). Intelligent garage door control system via PLC with built-in safety sensors. Proceedings of the International Scientific Conference Defense Technology Forum, 648–655.
10. Denev, D., & Sotirov, P. (2026). Virtual and augmented reality for training in automation and network technologies. Annual of Konstantin Preslavsky University of Shumen, XV E, 97–108.
11. Simeonova, I. (2025). How GDPR treats automated decision-making. Journal Scientific and Applied Research, 28(1). Shumen: Konstantin Preslavsky University Press. ISSN 1314-6289.

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

QUANTITATIVE ASSESSMENT OF RADIO-FREQUENCY COUNTERMEASURES AGAINST CONSUMER UNMANNED AERIAL VEHICLES

Deyan N. Dimitrov, Nikola P. Petrov

Department of Air Defense, Artillery, Air Defense and CIS Faculty at the Vasil Levski National Military University, Shumen, Bulgaria,
deyandimitrov@aadcf.nvu.bg, nikola.petrov@aadcf.nvu.bg

Abstract: *This paper presents a corrected quantitative framework for comparing non-kinetic radio-frequency counter-UAS techniques at an analytical and source-verification level. The framework combines an interference-aware link model, receiver-input jammer-to-signal ratio, a probabilistic interference model, and a multi-criteria decision structure. The source draft was checked against the cited literature and authoritative public sources. Several numerical claims that could not be traced to the cited experiments—including fixed AHP weights, universal success probabilities, a specific spoofing lock probability, and an ANOVA procedure—are removed or reclassified as scenario assumptions. In contrast, the comparative ordinal scores reported by Rozenbeek (2020) are retained and visualized because they can be verified directly in the source thesis. The paper also corrects the use of SNR to SINR when interference is present and treats GNSS spoofing results as receiver- and scenario-dependent rather than universal performance values. The resulting model is intended for sensitivity analysis, controlled simulation, and lawful evaluation of counter-UAS concepts; it does not prescribe operational transmission parameters for intentional interference.*

Keywords: *counter-UAS, radio-frequency interference, jamming, GNSS spoofing, SINR, jammer-to-signal ratio, multi-criteria assessment, UAV*

Introduction

The widespread availability of small unmanned aircraft systems (UAS) has increased the need for reliable counter-UAS (C-UAS) architectures around critical infrastructure. The scale of civil use is substantial, but the source draft overstates the U.S. registration figure: the Federal Aviation Administration currently reports 837,513 registered drones, not more than 1.7 million registered drones [1]. C-UAS design is also broader than radio-frequency mitigation alone and typically combines detection, identification, tracking, decision support, and mitigation functions [3, 4].

Radio-frequency methods can disrupt command links or navigation services, but their effectiveness depends on protocol, receiver design, geometry, interference environment, autonomy logic, and the target aircraft fail-safe behavior. The literature therefore does not support a single universal success probability or a universally optimal jamming method [2, 4–8]. This paper revises the source draft by separating source-supported evidence from analytical assumptions and by retaining only numerical comparisons that can be traced to the cited literature.

The emergence of new types of aerial threats, characterized by different flight speeds and altitudes, low radar cross sections (RCS), and diverse combat employment tactics,

has created the need for the development of surface-to-air missile systems (SAM systems) with short reaction times. Such systems must be capable of engaging and destroying aerial targets across a wide range of speeds and altitudes, under conditions of high raid density and electronic warfare countermeasures [5].

The analytical treatment is intentionally non-operational. It provides no transmitter power, tuning, waveform, or field-deployment recipe for intentional interference. Any experimental use of RF countermeasures must be conducted in an authorized, controlled, or shielded environment and in accordance with applicable spectrum and aviation law [4]. Phase-manipulated signals with impulse-like autocorrelation properties are important in radar, radio-navigation, and remote-control applications because of their high resolution. However, maintaining electromagnetic compatibility and reliable signal processing in a hostile radio-electronic environment requires effective suppression of autocorrelation sidelobes. Bedzhev and Dimitrov demonstrate that mismatched filtering can be used to reduce the sidelobes of three-valued autocorrelation functions, thereby improving the processing characteristics of such signals [12].

1 Verification of Source Claims and Scope

1.1 Source verification and corrections

The source draft combines established communication-theory relations with numerical values that are not consistently supported by the cited references. Table 1 records the principal corrections made during verification. Rozenbeek's work is a KTH master's thesis, not a doctoral dissertation, and it evaluates techniques with four ordinal criteria rather than with the AHP-derived weights and normalized effectiveness coefficients stated in the draft [2].

Table 1: Verification of major factual and numerical claims in the source draft.

Source-draft statement	Verification result	Treatment in revised paper
>1,7 million registered U.S. drones by 2023	FAA currently reports 837,513 total registered drones [1].	Corrected; current official count used.
AHP weights 0,45/0,25/0,15/0,15 were obtained experimentally	No pairwise-comparison matrix or consistency check is documented in the cited experimental thesis [2].	Numerical weights removed; AHP retained only as an optional method [10].
Fixed effectiveness values such as $\alpha \approx 0{,}82–0{,}86$ and $\beta \approx 0{,}95$	These values are not the source thesis scoring scheme; Rozenbeek reports ordinal criterion totals [2].	Replaced by source-verified ordinal scores.
GPS spoofing lock probability $p<0{,}05$ after authentic lock	The thesis reports failure to obtain outdoor position lock after prior authentic GNSS lock, not an estimated probability [2].	Probability claim removed; qualitative result retained.

Source-draft statement	Verification result	Treatment in revised paper
Five repetitions and one-way ANOVA	Not substantiated by the cited thesis as the basis for the reported comparison scores [2].	Removed; future work should specify replication and statistical tests explicitly.

1.2 Evidence hierarchy and interpretation

Three evidence classes are used throughout the revised analysis: established analytical relationships from communication theory [11, 12] source-reported experimental or ordinal observations [2, 5–9]; and scenario variables that must be calibrated for a particular authorized test environment. This distinction is necessary because results from a small set of consumer aircraft cannot be generalized to all modern UAS receivers, protocols, or autonomy stacks.

2 Interference-Aware Link Model

2.1 Signal-to-interference-plus-noise ratio

When an additional interfering signal is present, the appropriate physical-layer quantity is the signal-to-interference-plus-noise ratio (SINR), not SNR. A compact receiver-input model is given by Eq. (1). It is a generic analytical abstraction; all powers are receiver-input quantities and no operational transmitter settings are implied [11, 12].

$$\mathrm{SINR} = \frac{P_s}{N_0 \mathrm{B} + \eta P_j} \tag{1}$$

where:

SINR – signal-to-interference-plus-noise ratio at the receiver input, linear;
P_s – received desired-signal power, W;
N_0 – one-sided noise power spectral density, W/Hz;
B – receiver noise-equivalent bandwidth, Hz;
P_j – received interference power integrated over the relevant band, W;
η – spectral-overlap factor between the interference and the wanted signal, $0 \leq \eta \leq 1$.

The factor η makes the model suitable for sensitivity studies involving partial spectral overlap. It should be estimated from measured spectra or a validated waveform model rather than assigned a universal value.

2.2 Shannon-Hartley reference capacity

For an ideal additive-noise channel, the Shannon-Hartley expression can be used as a theoretical upper bound on the information rate associated with a given SINR [11]. It does not, by itself, predict when a particular proprietary UAV link will disconnect, because real receivers have modulation, coding, synchronization, and protocol-dependent thresholds.

$$\mathrm{C} = \mathrm{B}\, log_2(1 + \mathrm{SINR}) \tag{2}$$

where:

C – ideal channel capacity, bit/s;

B – channel bandwidth, Hz;
SINR – linear signal-to-interference-plus-noise ratio.

2.3 Jammer-to-signal ratio at the receiver

A receiver-input jammer-to-signal ratio (JSR) is useful for comparing measured or simulated interference conditions without embedding a deployment-specific path-loss or antenna geometry model. Equation (3) therefore uses only received powers. Any threshold for loss of service must be calibrated for the tested waveform and receiver [5, 12].

$$\mathrm{JSR} = \frac{P_{\mathrm{j,r}}}{P_{\mathrm{s,r}}} \tag{3}$$

where:
JSR – jammer-to-signal power ratio at the receiver input, linear;
$P_{j,r}$ – received interference power, W;
$P_{s,r}$ – received wanted-signal power, W.

2.4 Probabilistic variability

Shadowing, antenna orientation, mobility, and receiver implementation make JSR a random quantity in many realistic scenarios. If the JSR expressed in decibels is modeled as normally distributed with parameters obtained from authorized measurements, the probability of exceeding an analyst-defined threshold can be represented by Eq. (4). This is a statistical scenario model and is not an empirically established universal jamming-success law.

$$P_{\mathrm{int}} = 1 - \Phi_N\left(\frac{J_{\mathrm{th}} - \mu_J}{\sigma_J}\right) \tag{4}$$

where:
P_{int} – probability that the modeled JSR exceeds the selected scenario threshold;
Φ_N – cumulative distribution function of a standard normal variable;
J_{th} – scenario threshold in dB, requiring receiver-specific calibration;
μ_J – mean JSR in dB for the modeled environment;
σ_J – standard deviation of JSR in dB.

3 Multi-Criteria Assessment Framework

3.1 Criterion normalization

Rozenbeek evaluates techniques using four criteria: avoiding collateral damage, mitigating radio interference, identification requirement, and the ability to address multiple intruding drones [2]. For a new decision model, raw criterion values can first be mapped to a common dimensionless interval using Eq. (5). The direction of preference must be defined before normalization so that larger normalized values consistently indicate a more desirable outcome.

$$x_k = \frac{s_k - s_{\mathrm{k,min}}}{s_{\mathrm{k,max}} - s_{\mathrm{k,min}}} \tag{5}$$

where:

x_k – normalized value of criterion k, dimensionless;
s_k – raw score or measured value of criterion k;
$s_{k,min}$ – minimum reference value used for normalization;
$s_{k,max}$ – maximum reference value used for normalization;
k – criterion index.

3.2 Weighted composite score

A weighted composite indicator may then be formed with Eq. (6). The source draft states numerical weights as if they had been derived by the Analytic Hierarchy Process (AHP), but it does not provide the required pairwise-comparison matrix or a consistency assessment. The revised model therefore does not assign numerical AHP weights. If AHP is used in future work, the elicitation and consistency procedure should be documented explicitly [10].

$$\Phi = \sum_{k=1}^{m} w_k x_k \quad ; \quad \sum_{k=1}^{m} w_k = 1 \tag{6}$$

where:

Φ – weighted composite effectiveness indicator, dimensionless;
w_k – weight assigned to criterion k, with $w_k \geq 0$;
x_k – normalized criterion value;
m – number of criteria;
k – criterion index.

3.3 Proposed interference-burden coefficient

To represent collateral spectrum occupancy in a coarse sensitivity model, Eq. (7) defines a dimensionless interference-burden coefficient as the product of affected-bandwidth and time-occupancy fractions. Unlike the dimensionally ambiguous expression in the source draft, both factors are normalized. The coefficient is a proposed planning metric and must not be interpreted as a regulatory interference limit.

$$\beta = \frac{B_{int}}{B_{ref}} \frac{T_{int}}{T_{obs}} \tag{7}$$

where:

β – proposed dimensionless interference-burden coefficient;
B_{int} – bandwidth affected by the modeled interference, Hz;
B_{ref} – reference protected or monitored bandwidth, Hz;
T_{int} – time during which interference is present, s;
T_{obs} – total observation interval, s.

4 Source-Verified Comparative Results

4.1 Ordinal scores reported by Rozenbeek (2020)

The most defensible numerical comparison available in the source material is Rozenbeek's ordinal scoring table. These values are not success probabilities and should not be converted into percentages without an independently justified model. Table 2 reproduces representative totals that can be traced directly to the thesis [2].

Table 2: Representative total scores reported by Rozenbeek (2020) [2].

Neutralization method	Representative technique	Total score	Evidence note
Wi-Fi RC/video-link interference	Full-band barrage	11	Source-reported ordinal total
Wi-Fi RC/video-link interference	Single-channel barrage	10	Source-reported ordinal total
Wi-Fi RC/video-link interference	De-authentication	10	Source-reported ordinal total
FHSS RC-link interference	Full-band barrage	11 (8)	Parentheses: DIY-drone score
FHSS RC-link interference	Sweep	10 (7)	Parentheses: DIY-drone score
FHSS RC-link interference	Protocol-aware	9 (6)	Parentheses: DIY-drone score
GPS spoofing	Static / no-fly-zone concept	10	Source-reported ordinal total
GPS spoofing	Dynamic / hovering	8	Source-reported ordinal total
GPS spoofing	Dynamic / waypoint	8**	**Based on theoretical/related-work results in source
Combined GNSS + RC/video-link interference	Full-band barrage	10	Source-reported ordinal total
Combined GNSS + RC/video-link interference	Single-channel barrage	9	Source-reported ordinal total

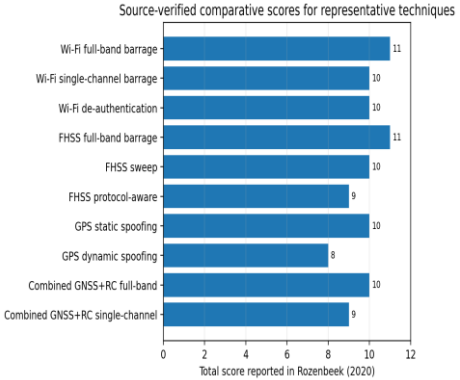


Figure 1: Source-verified comparative ordinal scores for representative techniques reported in Rozenbeek (2020) [2].

4.2 Criterion-level trade-offs for Wi-Fi RC/video-link techniques

The criterion-level values in Figure 2 show why a single total score must be interpreted carefully. In the source evaluation, full-band barrage scores well for broad applicability and limited identification requirements, but receives the lowest score for mitigating radio interference. De-authentication has the opposite spectrum-compatibility advantage but requires greater protocol identification [2, 9]. This is a trade-off, not evidence that either method is universally preferable.

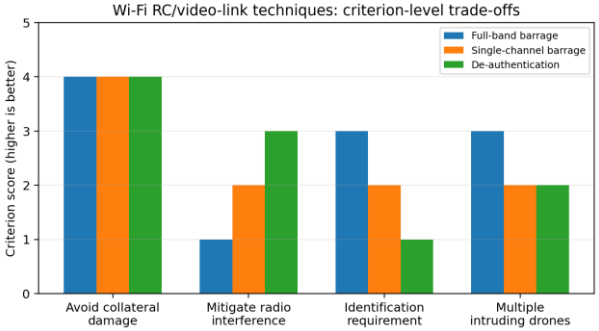


Figure 2: Criterion-level trade-offs for three Wi-Fi RC/video-link techniques; values reproduced from the source thesis [2].

4.3 GNSS spoofing results and limitations

The GPS-spoofing scores in Figure 3 are also ordinal. Rozenbeek's controlled indoor tests demonstrated susceptibility when authentic satellite reception was absent, whereas the outdoor trials performed after authentic GNSS lock did not obtain a spoofed position lock [2]. The thesis does not estimate this outcome as $p < 0,05$ and does not establish a universal anti-spoofing probability. Other research demonstrates that UAV capture by GPS spoofing is possible under specific receiver, state-estimation, and attack conditions [6–8], reinforcing that the result is architecture- and scenario-dependent.

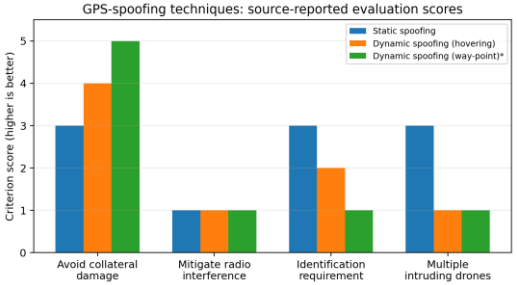


Figure 3: Source-reported GPS-spoofing criterion scores. The waypoint-mode score marked with an asterisk relies on theoretical/related-work evidence in the source [2].

5 Evaluation of Effectiveness and Limitations

The corrected analysis changes the interpretation of the original results in several important ways. First, full-band barrage interference has the highest or joint-highest ordinal total in several categories in Rozenbeek's evaluation, but the same source explicitly penalizes it for radio interference [2]. Therefore, the result cannot be restated as a universal effectiveness coefficient such as 0,82 or 0,86. Second, protocol-aware and de-authentication techniques can reduce unnecessary spectrum occupation, but their usefulness depends on successful identification and protocol compatibility [5, 9].

Third, GNSS-only disruption did not constitute a generally sufficient neutralization mechanism in the source evaluation when other control paths remained available. The combined treatment of navigation and command/video links received a higher source score for the considered scenarios [2]. This observation should be interpreted at architecture level only; it does not imply a universal method or a fixed probability of success.

Fourth, GPS spoofing should not be summarized by a single "lock probability." Kerns et al. demonstrate capture under specific experimental conditions, Noh et al. show adaptive approaches against selected consumer drones, and Gaspar et al. examine low-cost SDR-based GPS spoofing, while Rozenbeek reports difficulties after prior authentic satellite acquisition [2, 6–8]. Together these works support a scenario-dependent vulnerability model rather than a universal numerical success rate.

Finally, the original draft's statement that an AHP procedure produced the listed weights is not reproducible from the information provided. A defensible multi-criteria study should report the expert panel, pairwise-comparison matrix, consistency ratio, normalization direction, sensitivity of the ranking to the weights, and uncertainty of any measured inputs [10].

6 Recommended Validation Procedure

A future experimental campaign should be designed for reproducibility and safety rather than around fixed performance claims. At minimum, the study should pre-register the aircraft/receiver class, controlled test environment, response categories, number of independent repetitions, randomization policy, measurement uncertainty, and statistical method. Any interference or spoofing experiment should be conducted only under appropriate authorization or shielding. Results should be reported with confidence intervals and should distinguish loss of a communication link, loss of navigation, fail-safe activation, and safe neutralization as separate outcomes.

- Calibrate SINR/JSR and any threshold parameters from receiver-input measurements in an authorized test setup; do not transfer thresholds across unrelated receivers.
- Report criterion scores and physical measurements separately; do not convert ordinal scores into probabilities without a validated mapping.
- Use sensitivity analysis for decision weights and publish the AHP consistency ratio if AHP is used.
- Evaluate electromagnetic compatibility and collateral-service impact as explicit constraints rather than as a secondary qualitative note.

- Validate results across multiple UAS architectures and autonomy/fail-safe behaviors before making general claims [3, 4].

Conclusion

This paper revised the source draft into a traceable quantitative framework for assessing RF-based counter-UAS concepts. The main technical corrections are the use of SINR in the presence of interference, a receiver-input JSR definition, a calibrated probabilistic exceedance model, a dimensionally consistent interference-burden coefficient, and a multi-criteria model that does not claim unsupported AHP weights. Source verification also removes unsupported success probabilities, the unsubstantiated $p < 0,05$ GPS-spoofing claim, and the undocumented ANOVA statement. The comparative figures retain only source-verifiable ordinal values from Rozenbeek (2020). The resulting framework is suitable for sensitivity studies and controlled validation, while emphasizing that RF neutralization performance is receiver-, protocol-, environment-, and scenario-dependent and must be tested lawfully.

References

1. Federal Aviation Administration. (2026). FAA by the numbers. Retrieved August 31, 2026, from https://www.faa.gov/node/26;
2. Rozenbeek, D. J. (2020). Evaluation of drone neutralization methods using radio jamming and spoofing techniques (Master's thesis, KTH Royal Institute of Technology). TRITA-EECS-EX 2020:276;
3. Shi, X., Yang, C., Xie, W., Liang, C., Shi, Z., & Chen, J. (2018). Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges. IEEE Communications Magazine, 56(4), 68–74. https://doi.org/10.1109/MCOM.2018.1700430;
4. Lykou, G., Moustakas, D., & Gritzalis, D. (2020). Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies. Sensors, 20(12), 3537. https://doi.org/10.3390/s20123537;
5. Kirov, M., Algorithm For Servicing Requests From A Multisensor System, Proceedings of International Scientific Conference ―Defense Technologies‖ DefTec2025, Faculty of Artillery, Air Defense and Communication and Information Systems, 110 – 116, ISSN 2815-4282.
6. Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2014). Unmanned aircraft capture and control via GPS spoofing. Journal of Field Robotics, 31(4), 617–636. https://doi.org/10.1002/rob.21513;
7. Noh, J., Kwon, Y., Son, Y., Shin, H., Kim, D., Choi, J., & Kim, Y. (2019). Tractor Beam: Safe-hijacking of consumer drones with adaptive GPS spoofing. ACM Transactions on Privacy and Security, 22(2), Article 12. https://doi.org/10.1145/3309735;
8. Gaspar, J., Ferreira, R., Sebastião, P., & Souto, N. (2020). Capture of UAVs through GPS spoofing using low-cost SDR platforms. Wireless Personal Communications, 115(4), 2729–2754. https://doi.org/10.1007/s11277-020-07211-7;

9. Sun, A., Gong, W., Shea, R., Liu, J., Liu, X., & Wang, Q. (2017). Drone privacy shield: A WiFi based defense. In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 1–5. https://doi.org/10.1109/PIMRC.2017.8292780
10. Saaty, T. L. (1980). The analytic hierarchy process. McGraw-Hill;
11. Shannon, C. E. (1948). A mathematical theory of communication. Bell System Technical Journal, 27, 379–423, 623–656;
12. Bedzhev, B., & Dimitrov, D. (2024). Mismatched filters for processing of phase manipulated signals with three-valued autocorrelation. Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference, 3, 29–33. https://doi.org/10.17770/etr2024vol3.8111;
13. Rappaport, T. S. (2002). Wireless communications: Principles and practice (2nd ed.). Prentice Hall;

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

CYBERSECURITY ANALYSIS USING DEEP LEARNING NEURAL NETWORKS

Nikola R. Lazarov

Department "Computer Systems and Technologies", National Military University "Vasil Levski", Shumen, Bulgaria, lazarovn35@gmail.com

Abstract: *This paper investigates a deep learning approach for malware-family classification using a Convolutional Neural Network (CNN) applied to grayscale representations of malware embedded in PDF files. The experimental dataset is derived from the Microsoft BIG2015 dataset [1], where samples from each of the nine malware families are used to generate PDF-based specimens. Raw byte content is mapped to two-dimensional grayscale images and processed by a CNN that automatically extracts spatial and textural characteristics associated with malware families. The study evaluates whether these PDF-based visual representations preserve sufficient discriminative information for accurate malware-family classification without relying on manually engineered features.*

Keywords: *malware classification, PDF malware, deep learning, convolutional neural network, CNN, Microsoft BIG 2015.*

Introduction

The most common malware detection techniques are based on signatures, predefined rules, or manually selected characteristics. Although these methods remain useful for identifying known threats, the modification of the malicious code through like obfuscation, polymorphism, packing or other techniques intended to alter its observable representation, reduces their effectiveness. Static analysis provides an efficient mechanism for examining potentially malicious files, without executing them. But its effectiveness can be affected by transformations that conceal the underlying code. Because of these limitations, there is an increase of the interest in machine learning and deep learning methods capable of automatically extracting discriminative characteristics from large collections of malware samples.

The primary objective of this research is to determine whether spatial characteristics extracted from grayscale representations of PDF-embedded malware can provide an effective basis for malware-family classification. In particular, the study evaluates the ability of a convolutional neural network to learn discriminative visual patterns directly from the byte-level structure of the generated PDF samples.

The remainder of this paper is organized as follows. Section 1 reviews related work in deep learning-based malware detection and classification, with particular attention to image-based approaches. Section 2 describes the Microsoft BIG 2015 dataset, the procedure used to construct and preprocess the PDF-based experimental samples, and the CNN architecture. Section 3 presents the experimental setup, while Section 4 reports the CNN classification results. Finally, Section 5 discusses the observed performance, limitations, and directions for future research.

1. Related Work

1.1 Deep Learning for Malware Classification

The application of machine learning to malware detection has developed into an active research area, driven by the growing sophistication of cyber threats. Early approaches relied predominantly on manually engineered features – structural data, n-gram representations of opcode sequences, or behavioural indicators – which were subsequently fed into classical classifiers such as support vector machines (SVM) or random forests. These methods achieved satisfactory results under controlled conditions but proved vulnerable to obfuscation, packing, and polymorphism, since handcrafted features lose discriminative power when the underlying binary is structurally transformed [2].

1.2 CNN-Based Malware Classification

The visualization of malware binaries represents an early and influential contribution to this research direction. The approach introduced by Nataraj et al transforms the raw binary content of executable files into pixel matrices and analyses the resulting greyscale images using computer vision descriptors [3]. The central intuition is that files belonging to the same malware family share characteristic visual structures and textural patterns, whereas surface-level obfuscation operations affect symbolic names and addresses to a greater extent than the overall structural proportions of the binary. This partial robustness makes visual representation an attractive starting point for classification tasks [4] [5].

1.5 PDF Malware Detection

PDF documents have become a preferred vector for delivering malicious content owing to their structural characteristics: the format supports the embedding of JavaScript, compressed content streams, and references to remote resources, making it a convenient wrapper for concealing malicious code. Early machine learning approaches targeting PDF malware focused primarily on statically extracted structural features – object counts and types, the presence of specific keywords in stream headers, and the frequency of JavaScript usage. Saxe and Berlin demonstrate that a combination of metadata and structural features yields robust classification results even against adaptive adversaries seeking to evade detection [6].

1.6 Research Gap

Existing studies demonstrate the effectiveness of image-based representations for malware classification, particularly when raw binary content is transformed into grayscale images that preserve structural regularities. However, the use of CNN-based visual analysis on malware samples represented within PDF containers remains comparatively less explored. This study addresses that gap by evaluating a CNN classifier on PDF-based samples derived from the Microsoft BIG 2015 dataset.

2. Methodology

2.1 Dataset and Sample Preparation

Experimental data for this study were drawn from Microsoft BIG 2015, a publicly available benchmark released through a Kaggle malware classification competition. Comprising 10 868 binary executable files, the dataset spans nine distinct malware families: Ramnit, Lollipop, Kelihos_ver3, Vundo, Simda, Tracur, Kelihos_ver1,

Obfuscator_ACY, and Gatak. Class distribution is notably imbalanced – a characteristic explicitly accounted for during preprocessing. From each family, PDF-based specimens were generated by embedding raw binary content into a PDF document, preserving the underlying byte structure within a widely used container format. Each specimen was then converted into a grayscale image for CNN-based classification.

2.2 PDF-Based Malware Representation

PDF sample generation was designed to preserve the maximum volume of diagnostically relevant information from each original binary file. Raw bytes of the executable were embedded as inline content within the generated document, without applying compression or byte-level transformations that might obscure structurally significant dependencies. Consequently, each generated PDF inherits the byte-level organisation of its source file, including family-characteristic headers, recurring structural regions, and segment boundaries. Chosen for its ubiquity as a delivery mechanism and its capacity to encapsulate heterogeneous data, the PDF format provides a standardized container from which grayscale image representations can be derived for CNN analysis.

2.3 Data Preprocessing

Before specimens were passed to the CNN, a standardized preprocessing pipeline was applied. Data were partitioned into training, validation, and test subsets in an 80:10:10 ratio using a random permutation, with 80% of specimens allocated to training and the remaining 20% divided equally between validation and test. To address the inherent class imbalance of the Microsoft BIG 2015 dataset, a moderate oversampling procedure was applied to the training set. For each family, a target count was set to max (2 × median class size, 50), with the number of selected instances capped at three times the original family count to prevent excessive duplication. Image pixel values were normalized to [0, 1] by dividing by 255 inside the network's first functional layer.

2.4 Image Representation for the CNN

Each specimen fed into the CNN branch was converted into a two-dimensional grayscale image. Bytes were read sequentially and arranged into a rectangular matrix of predefined dimensions, with pixel values in the range 0÷255 normalized to [0.0, 1.0] via division by 255 inside the network's first functional layer. Resulting images were resized to 128×128 pixels to ensure a uniform input dimensionality across all files. Visual inspection of executables belonging to different families reveals characteristic structural patterns: recurring textural blocks, regions of elevated information density, and family-specific spatial configurations. Such observations suggest that the spatial organisation of an image encodes discriminative information regarding family membership, accessible to convolutional feature extractors without explicit feature engineering or file format parsing.

2.5 CNN Architecture

Four successive convolutional blocks form the spatial processing core of the CNN, each comprising a convolutional layer with 3×3 kernels, batch normalization, ReLU activation, and max-pooling with a 2×2 window. Filter counts increase progressively from 32 in the first block to 64, 128, and 256 in the subsequent three, enabling the extraction of increasingly abstract spatial features. After the final convolutional block,

global average pooling reduces each 256-channel feature map to a 256-dimensional vector. A dropout component with rate 0.3 follows before a fully connected output layer of nine neurons activated by Softmax, producing a probability distribution over the nine malware families (Figure 1).

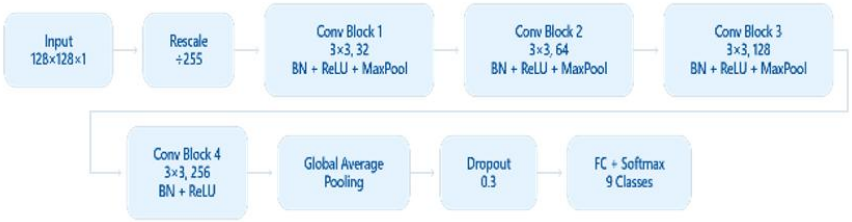


Figure 6: CNN layer architecture.

2.6 Training Strategy

The CNN was trained on the oversampled training subset using the Adam optimizer with a batch size of 64 and a maximum of 15 epochs. A piecewise learning rate schedule was used to support stable convergence, while gradient clipping and L2 regularization were applied to reduce instability and overfitting. Early stopping monitored validation performance and retained the best-performing checkpoint for final evaluation.

2.7 Evaluation Protocol

Performance was assessed using standard metrics for multi-class classification, with validation accuracy used as the primary reported measure. Training and validation curves were examined to assess convergence and potential overfitting. The evaluation focuses exclusively on the CNN classifier operating on grayscale PDF-based representations.

2.8 Implementation Environment

The CNN was implemented in MATLAB using the Deep Learning Toolbox. Core functions include trainNetwork, trainingOptions, imageDatastore, and augmentedImageDatastore. Training and evaluation ran on a system equipped with an NVIDIA GeForce RTX 3080 GPU, with the execution environment set to "auto" to enable GPU acceleration where available. Reproducibility was ensured by fixing the random seed to 42 at session start via rng(42) and by recording all hyperparameters as named configuration variables at the top of the script.

3. Experimental Setup

3.1 Experimental Objectives

The experiments described in this section assess the ability of a Convolutional Neural Network (CNN) to classify malware families from grayscale image representations derived from PDF-based samples. The evaluation is conducted on a dataset derived from the BIG2015 benchmark corpus transformed into a PDF-based intermediate representation. The objective is to determine whether spatial texture patterns and

structural regularities preserved in these representations provide sufficient discriminative information for accurate nine-class malware-family classification.

3.2 Dataset Configuration

The source data for the experiment is the Microsoft BIG2015 malware classification dataset, which encompasses binary executable samples distributed across nine distinct malware families: Ramnit, Lollipop, Kelihos_ver3, Vundo, Simda, Tracur, Kelihos_ver1, Obfuscator_ACY, and Gatak. Rather than processing these executables directly in their original form, each sample was converted into a PDF document that preserves the original byte-level content in a standardized portable format. Each resulting specimen was converted into a grayscale image for CNN processing. The dataset was partitioned into training, validation, and test subsets, with the training subset oversampled to reduce the effect of class imbalance.

3.3 CNN Model Configuration

The evaluated model is a CNN classifier trained on grayscale image representations obtained by mapping the byte values of each PDF sample to pixel intensities arranged in raster order. The network learns hierarchical spatial features directly from these images and maps the resulting representation to one of the nine malware-family classes.

3.4 CNN Training Configuration

The CNN branch operates on fixed-size grayscale images derived from the byte content of each PDF sample, with pixel intensity values normalized to the [0, 1] range prior to training. The network architecture follows a deep convolutional design with multiple feature extraction stages, each comprising convolutional, batch normalization, and pooling layers, followed by fully connected classification layers adapted to the nine-class output space. Training employed a batch-based gradient descent procedure with cross-entropy loss as the optimization objective. A piecewise learning rate schedule was applied to facilitate convergence: the initial learning rate was reduced at predefined epoch boundaries to allow the optimizer to settle into progressively finer parameter regions. Regularization was achieved through a combination of dropout in the fully connected layers and L2 weight decay applied globally. Early stopping based on validation accuracy was used to prevent overfitting and to identify the optimal parameter state for subsequent feature extraction and evaluation.

3.5 Evaluation Metrics

Classification performance is assessed primarily through validation accuracy, supported by inspection of the training and validation accuracy and loss curves. These measurements provide an indication of overall predictive performance, convergence behaviour, and whether substantial overfitting occurs during training.

3.6 Hardware and Software Environment

All training and evaluation experiments were conducted on a workstation equipped with a single GPU, as indicated by the hardware metadata logged during the training run. The CNN was implemented and trained using MATLAB with the Deep Learning Toolbox, which provided training progress monitoring, learning rate scheduling, and early stopping functionality. The GPU-accelerated training pipeline allowed the CNN to complete its training cycle in approximately six and a half minutes.

4. Results

4.1 Overall Classification Performance

The CNN-only model achieved a validation accuracy of 94.20% on the BIG2015 dataset processed through grayscale PDF-based representations. This result indicates that the visual representation retains strong family-discriminative information and provides an effective basis for convolutional classification.

Table 1. CNN classification performance.

Model	Validation Accuracy
CNN	94.20%

4.2 CNN Classification Results

The convolutional neural network was trained for 15 epochs using a piecewise learning rate schedule with an initial rate of 0.0001, completing 3,015 iterations in approximately six minutes and thirty seconds of wall-clock time. The training and validation accuracy curves exhibited consistent convergence without observable overfitting (Figure 2).

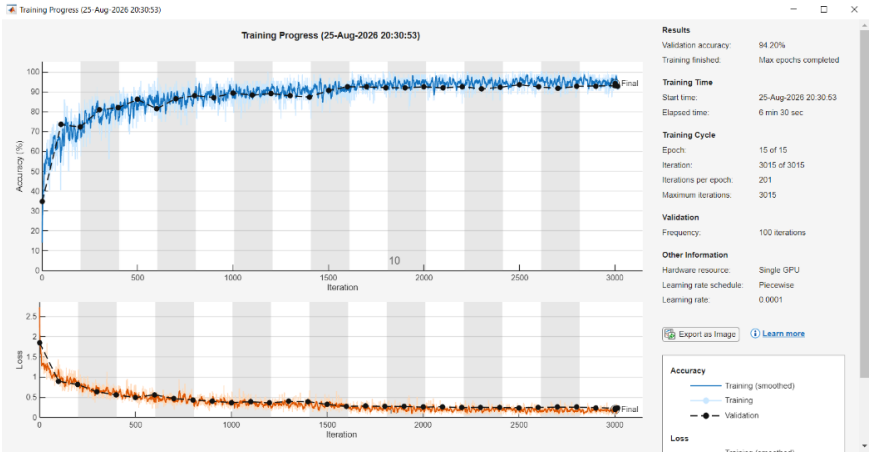


Figure 2: CNN classification results.

Both curves rise steadily through the first ten epochs before stabilizing, and the validation loss decreases monotonically throughout training. The model reached a final validation accuracy of 94.20%, demonstrating that the grayscale PDF-based representations retain discriminative spatial characteristics associated with the malware families present in the dataset. The relatively rapid convergence within fifteen epochs suggests that the visual texture and structural regularity of the grayscale representations

provide strong class-separating features that are accessible to convolutional operations, even without explicit feature engineering.

4.3 Summary of Experimental Findings

The experiment demonstrates that the CNN can effectively classify samples from the nine malware families represented in the PDF-based dataset. Leveraging grayscale visualizations of the raw binary content, the model achieved a validation accuracy of 94.20%, establishing that spatial representations derived directly from binary structure provide strong discriminative signals accessible to standard convolutional architectures.

5. Discussion and Conclusion

5.1 Interpretation of the Experimental Results

The convolutional neural network (CNN) operating on grayscale image representations achieved a validation accuracy of 94.20%. This result indicates that the spatial representation of PDF-transformed malware samples provides a strong basis for malware-family classification.

The CNN, trained over 15 epochs in approximately six and a half minutes, reached its final accuracy with stable convergence. The training and validation curves show that the model learned discriminative visual features efficiently without observable severe overfitting.

5.2 Contribution of the CNN

The CNN processes two-dimensional grayscale images derived from the PDF-based representation of the malware samples and learns spatial structures, local pattern distributions, and characteristic visual textures associated with each malware family. These spatial features are well-suited to the classification task, as evidenced by the 94.20% validation accuracy achieved without explicit feature engineering.

5.3 Classification Performance

The achieved validation accuracy demonstrates that grayscale representations of PDF-embedded malware preserve substantial family-specific structure. The result supports the use of convolutional feature extraction as a compact approach for learning discriminative patterns directly from the visualized byte content.

5.4 Classification Challenges

Although the overall validation accuracy is high, the aggregate result alone does not establish uniform performance across all nine malware families. The BIG2015 dataset is imbalanced, and smaller classes may be represented less reliably than larger families. Future evaluation should therefore include CNN-specific per-family precision, recall, F1-score, and confusion-matrix analysis to identify systematic class-level errors.

5.5 Implications of the PDF-Based Representation

The experimental results indicate that family-discriminative characteristics of the original malware samples remain sufficiently observable after their transformation into the PDF-based representation used in this study. The classification performance achieved across the majority of families suggests that the conversion process preserves structural and low-level byte patterns that are informative for distinguishing between malware families derived from the BIG 2015 corpus.

5.6 Limitations

Several limitations constrain the generalizability of the findings reported here. The dataset derives from Microsoft BIG 2015, which bounds the diversity of represented malware families and samples to those present in that corpus. Because the PDF files were generated experimentally rather than obtained from live malware campaigns, the experimental setting may not reproduce the characteristics of naturally occurring malicious documents. The experiment addresses malware-family classification rather than binary malware detection: all inputs are assumed to belong to one of nine known families, and the CNN is not evaluated on its ability to distinguish malicious from benign PDF documents, which represents a fundamentally different and operationally more relevant task.

5.7 Future Work

Several logical extensions of the present work suggest themselves. The most immediately relevant would be to introduce a benign PDF class and evaluate the CNN's capacity for malware-versus-benign discrimination, which is the more practically meaningful classification problem. Evaluation on naturally occurring malicious PDF datasets rather than programmatically generated samples would provide a more realistic assessment of the approach's generalizability. Further work could also investigate alternative CNN depths, input resolutions, regularization strategies, and transfer-learning architectures to determine whether classification performance can be improved while preserving computational efficiency.

Conclusion

This study investigated a CNN architecture for malware-family classification operating on PDF-based representations of samples derived from the Microsoft BIG 2015 dataset. The approach uses grayscale image representations of the PDF-embedded malware content and applies convolutional feature extraction to learn spatial and textural characteristics associated with the nine malware families.

The experimental results show that the CNN achieved a validation accuracy of 94.20%, demonstrating that the grayscale PDF-based representation preserves substantial discriminative information from the underlying malware samples. The findings support CNN-based visual analysis as an effective approach for malware-family classification in this experimental setting, while further evaluation on benign documents and naturally occurring malicious PDFs is required before conclusions can be extended to operational malware detection.

References

1. Ronen, R., Radu, M., Feuerstein, C., Yom-Tov, E., & Ahmadi, M. (2018). Microsoft Malware Classification Challenge. arXiv preprint arXiv:1802.10135.
2. Bensaoud, A., Kalita, J., & Bensaoud, (2024) M. A Survey of Malware Detection Using Deep Learning. Department of Computer Science, University of Colorado Colorado Springs.
3. Nataraj, L., Karthikeyan, S., Jacob, G., & Manjunath, B. S. (2011). Malware images: visualization and automatic classification. In Proceedings of the 8th

International Symposium on Visualization for Cyber Security (VizSec '11), pp. 1–7. ACM.

4. Simonyan, K., & Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556.
5. He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 770–778.
6. Saxe, J., & Berlin, K. (2015). Deep neural network based malware detection using two dimensional binary program visualization. In Proceedings of the 10th International Conference on Malicious and Unwanted Software (MALWARE 2015), pp. 63–69. IEEE.

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

MALICIOUS ACTIVITIES HUNTING IN NETWORK DEVICES

Linko G. Nikolov, Svetoslav Kirilov

"Cybersecurity and IT" Section, Scientific Research Instutite, National Military University,
linkonikolov@gmail.com ; kirilovsk5@gmail.com

***Abstract**: Network services support is one of the most significant batlefield IT operations in contemporary warfare. Ignoring the social engineering techniques, network devices and their operating systems are the plane whereas attacker will try to enter at first. In this research paper malicious activities into network devices is searched and checked in the means of MAC tables, ARP tables, IP and DHCP spoofing, as well as several other network security aspects. Specialized packet inspection software is used into a hardware environment as a controlled laboratory setup.*

***Keywords**: network device malware, network security, cybersecurity*

Introduction

Computer network operation support during military tactical operations comprises contemporary equipment, alongside with skilled personel. Network services and administration support includes network devices appropriate configuration and monitoring. Communication and information systems (CIS) support during military tactical operations relies on a combination of contemporary equipment and skilled personnel, working together to maintain seamless connectivity and ensure operational readiness. Effective network support involves the precise configuration of networks devices, ensuring that the infrastructure remains stable and capable of handling network traffic efficiently, while also preserving traffic data as a cybersecurity artifact [4] whenever possible. This is critical for maintaining situational awareness in dynamic environments and responding swiftly to potential cyber attacks.

Network analysis is a fundamental aspect of maintaining operational availability and performance, proving especially valuable during cyber incidents. It allows for the identification of unusual packet patterns, the evaluation of communication channel data rates, and the verification of protocol configurations. However, manual analysis is a time-consuming and resource-intensive process, requiring significant expertise and attention to detail. Although automation systems and artificial intelligence (AI) tools have been developed to assist in this area [3], [4], many still lack the fine precision and adaptability required for complex, real-time environments. As a result, specialized packet capture software is often utilized to gain a comprehensive understanding of network operations, providing detailed insights that are crucial for diagnosing issues, optimizing performance, and ensuring security. Threat hunting on the network is like trying to find a needle in the haystack when you don't even know for certain that a needle is there. Through packet analysis, incident responders have to discover threats themselves.

In this project, a complete network for an artillery division is to be established, providing a robust foundation for communication and coordination in a tactical setting. This project required the deployment of several essential network devices to ensure the network's reliability and functionality.

1. Building the network infrastructure.

The first step involved is the setting up of and IP address table, which is fundamental for managing and resolving network communication. IP configuration ensures that devices can communicate properly, enabling seamless access to network resources. Following the successful IP configuration, we proceeded to configure the Data-Link channel plane. This concludes into MAC address table check and VLAN configurations. To enhance network productivity, VoIP service may be configured. And having into account scalability, STP protocol can be used in proprietary technologies.

The final phase of this work focused on implementing monitoring and analysis. Yhe achieved results aimed at reconfiguring the network devices if required. We performed confugiretaions check on each network device, ensuring that the status lacks malicious activities. Several configurations were proposed to strengthen the security posture of the network and to provide valuable insights into the overall health and performance of the infrastructure.

This paper showcased the critical role of CIS in modern military operations, emphasizing the importance of cyberawareness and security planning, meticulous configuration, and continuous monitoring to maintain a resilient and secure network configuration.

An example of a computer network for artillery division is presented in fig. 1.

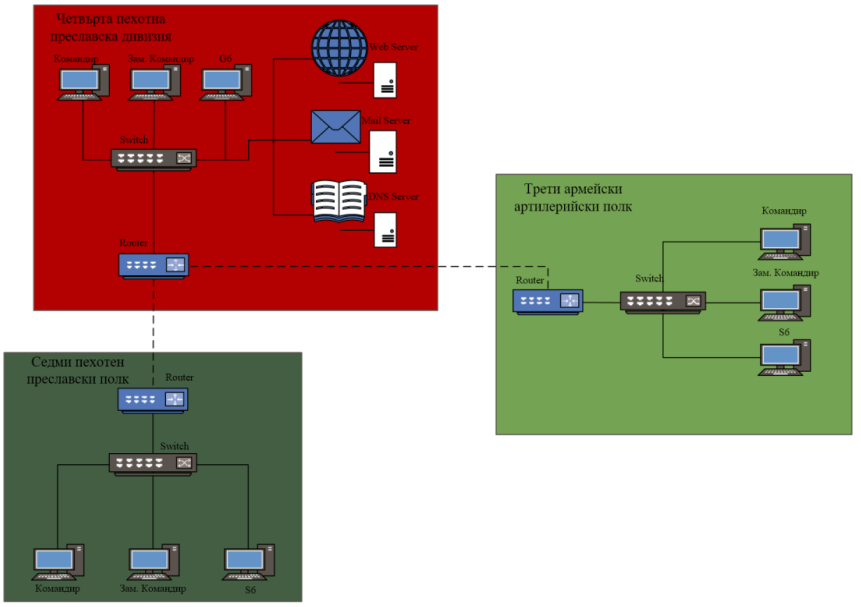


Figure 1: Example of Artillery division network topology

To ensure a more convenient and efficient-working network devices, a well-tuned IP adressation is implemented. IP routes and MAC-tables are critical to the functionality of the network, as they perform automatic communication outside users's visibility and interruption, allowing computers and servers to easily access switching and routing services without needing to remember complex numerical IP addresses.

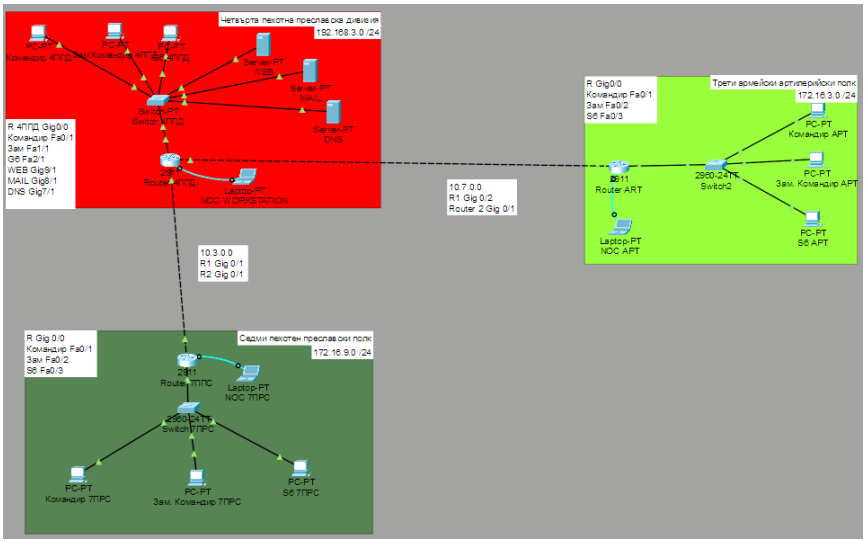


Fig. 2: IP address spaces

Important to the network administrator personnel is the Address Table document and interfaces allocation. On fig. 3 distribuiton over an excerpt LAN segment example is presented.

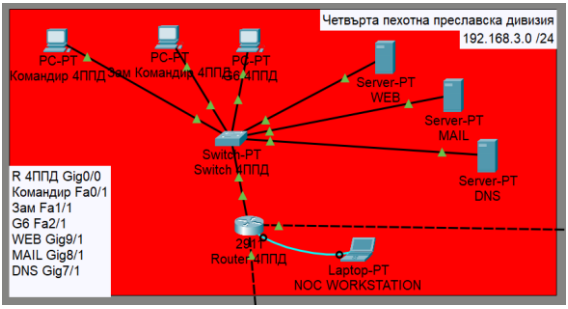


Fig. 3: IP interfaces allocation in a LAN segment

During education, a real-life training with hardware devices was proven as best practice. Hardware equipment was used for the purposes of this research paper (fig. 4). The ICMP protocol is used to check network connectivity.

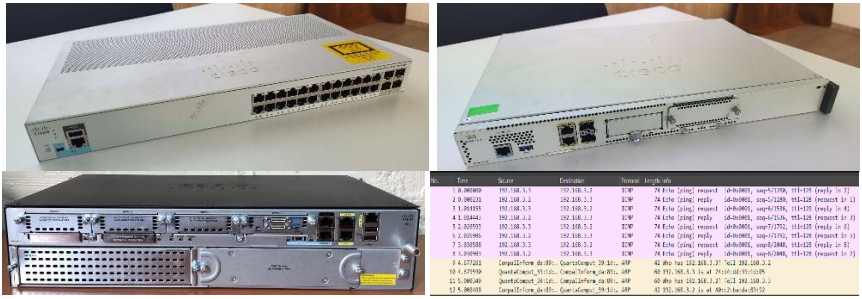


Fig. 4: Network devices in use

Malicious network activities may be present only if the network is gatewayed at Internet, or other external, out of control, networks.

2. Known Network- and Data-link layer attack threats.

It is important to pay attention to the threats that can arise at the individual communication layers. In the context of the task under consideration, attacks against the data link layer and the network layer are of the greatest importance. These layers perform addressing, forwarding, routing and management of the main network traffic.

2.1. Layer 3 threats.

Attacks targeting the network layer of the OSI model are particularly dangerous because they can be carried out remotely and often manage to disrupt normal communication between different devices on the network. These types of attacks are related to the IP protocol, interception and analysis of network packets, as well as Denial-of-Service (DoS) attacks. Examples of such attacks are ICMP attacks, as well as the so-called "Ping of Death", in which malformed or oversized packets are sent in order to overload or crash a system.

Most famous example of Network layer attacks is the IP address spoofing. It represents the forgery of the IP address of the packets, of the source. In this way, the attacker pretends to be another device on the network. This can be used to conceal the real source of the attack or to bypass the protection mechanisms.

Severe next example are the routing attacks - an issue frequently omitted by net admins. These are a type of attack where the attacker manipulates the routing process. As a result, traffic can be redirected, intercepted, or completely blocked.

Black Hole and Selective Forwarding attacks - in this type of attack, a malicious node pretends to be a normal participant in the network, but instead of forwarding packets, it discards them. Specifically, for "Selective Forwarding", only certain packets are blocked, which makes the attack more difficult to detect.

Many more examples can be found at [8].

2.2. Layer 2 threats.

Most threats on the second layer of the OSI model come from the internal part of the local network, but the attacker needs to have access to it. Attacks can lead to traffic interception, switch overload, data redirection, or denial of service.

ARP Spoofing - an attack in which an attacker sends fake ARP messages and associates his MAC address with the IP address of another device, such as a router or server. In this way, network traffic can be redirected through the attacker's device, allowing communication to be intercepted, blocked, or modified.

MAC Flooding - this involves the switch. Many frames with fake MAC addresses are sent to fill the MAC table. The switch can then start sending traffic to all ports, which could allow sensitive information to be intercepted.

Spanning Tree Attacks - attacks against the STP protocol, in which the attacker turns on an unauthorized switch and configures it with a lower root priority. In this way, it can become the root switch and control part of the network traffic.

The list of L3 and L2 vulnerabilities and threats is huge, but must be taken in mind when securing the network devices' operation plane.

3. Malicious activities hunting.

In the field of network security it seems difficult to find strict and concrete methodology for audits and checks. Anyway, one of the first things to do is check the current configuration. In Cisco IOS several commands are:

1) show version;
2) show startup-config;
3) show running-config;
4) show ip interface brief;
5) show ip route;
6) show mac-address-table;
7) show arp.

Important information that can be gathered is the version of the operating system and security certificates; version of used network and routing protocols and if authentication is avaliable; the size of the configuration files, respectively their hash values; interfaces IP address allocation; VLAN configuration.

Some results from issuing the mentioned commands are shown for routers in fig. 5 and for switches in fig. 6. Such information analysis can be made manually, but also can be automated with agentic AI algorithms and sensors. The actual analysis is still a responsibility to a security officer. In the analysis, information about activity from unknown IP and MAC-addresses, unknown TCP ports and services, in connection to malicious actors, is hunted. This is an enormous effort, that's why it should be performed carefully with good planning and coordination.

If there is a mismatch found, precautions must be performed immediately, like updating the versions to newest stable one, installing latest versions for network protocols, issuing commands for network security.

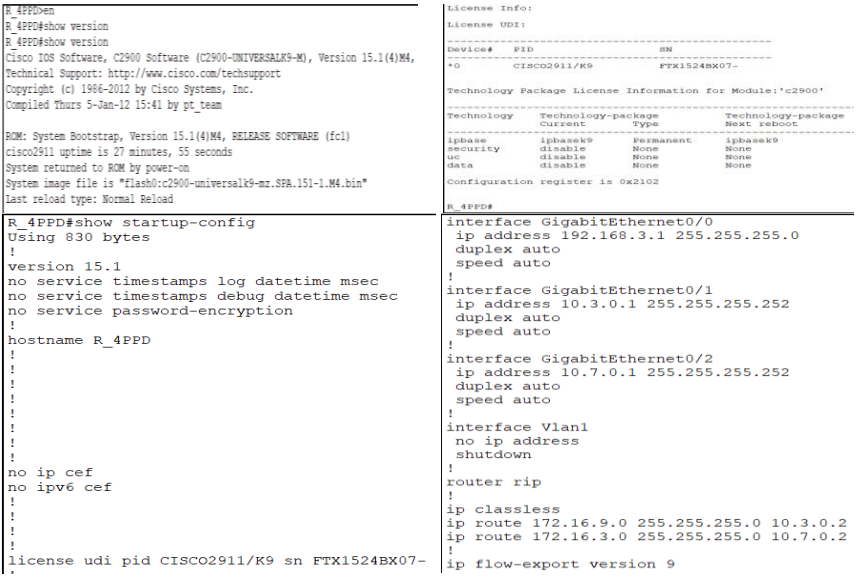


Fig. 5: Router configurations check

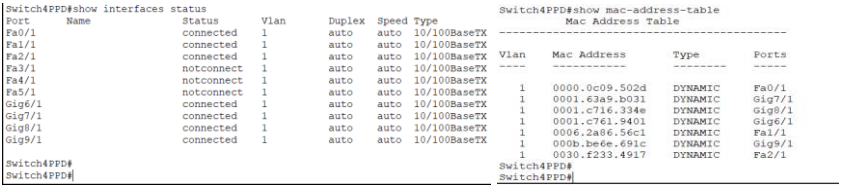


Fig. 6: Switch configurations check

Monitoring - in modern cybersecurity operations, the success of cyberdomain defence depends heavily on a robust software environment, encompassing a wide range of components such as network detecton and response (NDR), network access control (NAC), endpoint detection and response (EDR), extended detection and response (XDR), SIEM servers, and network devices that support both monitoring and proactive response. Such enhanced environment must be carefully configured and managed to ensure reliable and secure incident and event management, as well as efficient reposne (SOAR). The role of network security personnel in this context extends beyond basic monitoring: they must possess the practical skills required for precise security actions, ensuring that all systems and devices are properly set up to support security messages. These

configurations might include setting up secure protocols, managing IP address assignments, optimizing network paths, and implementing necessary security measures such as firewalls and encryption protocols. This hands-on expertise is vital to ensure the infrastructure is optimized for performance while minimizing vulnerabilities.

Control and evaluation - continuous control and evaluation of the network's operation are critical to maintaining availability and ensuring that packet traffic remains stable and secure. This involves not only monitoring the status of individual devices but also assessing the overall health of the network. Key metrics such as latency, packet loss, data throughput, and network jitter are monitored to detect potential bottlenecks or failures that could compromise combat mission success. Specialized software and dedicated hardware resources, such as Network Performance Monitors (NPM) and Security Information and Event Management (SIEM) tools, are employed to automate the monitoring process. These tools can visualize network traffic patterns, highlight anomalies, and provide real-time alerts, allowing IT personnel to quickly identify and address issues. Automated tools like these can also generate detailed reports that are valuable for both post-operation analysis and ongoing adjustments to improve network performance.

In summary, monitoring the digital environment of battlefield CIS is not merely about tracking performance—it is about creating a resilient and adaptive network infrastructure that can meet the dynamic needs of military operations, from supporting real-time decision-making to maintaining the security and integrity of critical data flows

4. Network defence.

To limit network layer threats, it is important to use mechanisms for controlling and filtering network traffic in real time. One of the most commonly used approaches is packet filtering, through which suspicious or incorrect packets can be detected and prevented from reaching the end devices. Furhter, is the contemporary solution of the so called "network behaviour" correlating between several network activity events. Such information is collected by sensors and revealed into machine learning algorithms in order to be classified and further processed. For routing attacks, preventive measures must be taken by implementing routing information authentication (OSPFv3), device monitoring, and detecting unusual network behavior (Next Generation Firewalls). For selective forwarding protection, node behavior monitoring, alternative routes and other tools must used.

To reduce the risk of Data-Link channel attacks, mechanisms that are responsible for port security, VLAN separation, ARP inspection, and proper STP configuration must be used, like Dynamic ARP Inspection, Private VLANs, or traffic filtering. Port security and authentication via an AAA server must be used for protection against MAC flooding. For protection agains STP attacks, proper configuration of the main switch, BPDU Guard, Root Guard and physical access restriction must be applied.

```
Switch4PPD#
Switch4PPD#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch4PPD(config)#interface fa0/1
Switch4PPD(config-if)#switchport mode access
Switch4PPD(config-if)#switchport port-security
Switch4PPD(config-if)#switchport port-security maximum 1
Switch4PPD(config-if)#switchport port-security mac-address sticky
Switch4PPD(config-if)#switchport port-security violation shutdown
Switch4PPD(config-if)#exit
Switch4PPD(config)#
```

Fig. 7: Port security configuration

```
R_4PPD#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R_4PPD(config)#ip access list extended SERVER-FILTER
                  ^
% Invalid input detected at '^' marker.

R_4PPD(config)#ip access-list extended SERVER-FILTER
R_4PPD(config-ext-nacl)#permit 192.168.10.0 0.0.0.255 host 192.168.20.252 eq 53
                        ^
% Invalid input detected at '^' marker.

R_4PPD(config-ext-nacl)#permit udp 192.168.10.0 0.0.0.255 host 192.168.20.252 eq 53
R_4PPD(config-ext-nacl)#permit udp 172.16.9.0 0.0.0.255 host 192.168.20.252 eq 53
R_4PPD(config-ext-nacl)#permit udp 172.16.3.0 0.0.0.255 host 192.168.20.252 eq 53
R_4PPD(config-ext-nacl)#
R_4PPD(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 host 192.168.20.250 eq 443
R_4PPD(config-ext-nacl)#permit tcp 172.16.9.0 0.0.0.255 host 192.168.20.250 eq 443
R_4PPD(config-ext-nacl)#permit tcp 172.16.3.0 0.0.0.255 host 192.168.20.250 eq 443
R_4PPD(config-ext-nacl)#
R_4PPD(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 host 192.168.20.251 eq 25
R_4PPD(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 host 192.168.20.251 eq 110
R_4PPD(config-ext-nacl)#permit tcp 172.16.9.0 0.0.0.255 host 192.168.20.251 eq 25
R_4PPD(config-ext-nacl)#permit tcp 172.16.9.0 0.0.0.255 host 192.168.20.251 eq 110
R_4PPD(config-ext-nacl)#permit tcp 172.16.3.0 0.0.0.255 host 192.168.20.251 eq 25
R_4PPD(config-ext-nacl)#permit tcp 172.16.3.0 0.0.0.255 host 192.168.20.251 eq 110
R_4PPD(config-ext-nacl)#
R_4PPD(config-ext-nacl)#deny any 192.168.20.0 0.0.0.255
                        ^
% Invalid input detected at '^' marker.

R_4PPD(config-ext-nacl)#deny ip any 192.168.20.0 0.0.0.255
R_4PPD(config-ext-nacl)#permit ip any any
R_4PPD(config-ext-nacl)#exit
R_4PPD(config)#
```

Fig. 8: Access control list configuration

With the proposed access control list (ACL), a certain, but not overall, layer of network security is applied, permitting only predefined LAN IP address spaces and known services.

```
R_4PPD#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R_4PPD(config)#interface giga
R_4PPD(config)#interface gigabitEthernet 0/0.20
R_4PPD(config-subif)#ip acc
R_4PPD(config-subif)#ip access-group SERVER-FILTER out
R_4PPD(config-subif)#end
R_4PPD#
%SYS-5-CONFIG_I: Configured from console by console

R_4PPD#write
Building configuration...
[OK]
R_4PPD#
```

Fig. 9: Server-filter application for a subinterface

The setting proposed on fig. 9 controls access to servers based on predefined rules. Only critically needed DNS, WEB and MAIL services are allowed, while the remaining traffic to the 192.168.20.0/24 network is blocked. This limits unnecessary communication to the segment and reduces the risk of unauthorized access.

Another adviced defensive actions are:

1. Stop the enabled protocols you are using from broadcasting information
2. Secure the protocols you are using
3. Evaluate what services you are using and disable unused services
4. Secure everything with access control lists
5. Keep your software/firmware/OS up to date

And also to be aware of what information the network device is sharing. [9]

Conclusion

Network device configuration must be precisely calculated, planned and implemented. After network operation start, devices functionality must be foreseen and monitored accordingly. Enhanced cyber attacks can be initiated at the OSI layer 3 and 2 level before further lateral movement. The presented small-scale research presented several steps and techniques, used for malicious activities checks inside the network devices such as routers and switches. Nevertheless, during routine cybersecurity operations, malicious hunting in network devices must not be rejected, but allegedly used and even improved over time in the means of personnel efforts, and equipment (hardware and software) evolution.

References

1. RFC documentations and blogs, Retrieved from https://www.ietf.org/rfc/rfc1035.txt
2. Николов, Л. Г., Киберсигурност на комуникационно-информационните системи, Монография, Шумен, 2021, ISBN 978-619-7531-22-0
3. Slavyanov, K., Dimov, R., Application of fuzzy logic in cybersecurity decision making and analysis after a cyber incident detection, ENVIRONMENT. TECHNOLOGIES. RESOURCES. Proceedings of the International Scientific

and Practical Conference, 2024, ISSN 1691-5402, DOI: https://doi.org/10.17770/etr2024vol2.8022.

4. Borisova, A. R., Network attack recognition using fuzzy logic, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 15th International Scientific and Practical Conference. Volume II, 55-60, 2024, ISSN 1691-5402, DOI: https://doi.org/10.17770/etr2024vol2.8054.
5. Joseph Migga Kizza, „Guide to Computer Network Security", Springer, 2009, ISSN 1617-7975.
6. Raphael Hertzog, „KALI LINUX Revealed", Offsec Press, www.offensive-security.com
7. Robert W. Beggs, „Mastering KALI LINUX for advanced penetration testing", PACKT Publishing, 2014, ISBN 978-1-78216-312-1
8. OSI Model layers attacks, Exabeam, URL: https://www.exabeam.com/explainers/osi-layers/osi-layer-attacks-38-network-attacks-by-layer-and-how-to-mitigate/
9. NetworkDefenceBlog, URL: https://www.networkdefenseblog.com/post/5-easy-router-attacks-and-protections

MALICIOUS ACTIVITIES HUNTING IN WINDOWS SERVER

Linko G. Nikolov, Evlogi Grigorov

"Cybersecurity and IT" Section, Scientific Research Instutite, National Military University,
linkonikolov@gmail.com; eevlogiev2003@gmail.com

***Abstract**: Windows services support is one of the most significant batlefield IT operations in contemporary warfare. Information services availability help comannder's decision making process faster and valuable. In this research paper Windows user operating system security is presented and analyzed in the means of malware presense, malicious traffic alerts and other cybersecurity aspects. Specialized system virtualization is used, as well as analyzing software as a laboratory setup.*

***Keywords**: Windows server, Windows configuration, Windows security, cybersecurity*

Introduction

Server operating systems, with their comprehensive computing capabilities, are increasingly entering the portfolio of business environments. However, many institutions are not aware of the threats to computer, network and information security when entering personal data and sensitive information into server services. Procedures for protecting computer systems, in turn, continue to be improved, as new techniques and tools are developed. Proper operation of the server determines computer security, while existing gaps in the program code of applications and services determine the level of security challenge. This is critical for maintaining situational awareness in dynamic environments and responding swiftly to potential threats.

Windows systems analysis is a fundamental aspect of maintaining endpoint availability and performance, proving especially valuable during cyber incidents. It allows for the identification of unusual patterns, the privilege escallation, and the verification of systems sprocessess. However, manual analysis is a time-consuming and resource-intensive process, requiring significant expertise and attention to detail. Although automation systems and artificial intelligence (AI) tools have been developed to assist in this area [2], [3], many still lack the precision and adaptability required for complex, real-time environments. As a result, specialized virtualization and analysis software is often utilized to gain a comprehensive understanding of Windows operations, providing detailed insights that are crucial for diagnosing issues, optimizing performance, and ensuring security.

In this project, a complete analysis of Windows Server machine is to be established, providing robust services for communication and coordination in a tactical setting. This project required the deployment of several essential services to ensure the system's reliability and functionality.

1. Specifics of Windows Server.

Windows Server provides flexibility in choosing where to deploy applications and data based on the business needs of the organization. Each deployment model offers

specific benefits that support growth and innovation. The system can be deployed in the cloud, in the data center, or as a hybrid solution at the edge in a variety of infrastructures.

Windows Server is available in different editions, designed for different scales and virtualization requirements, with the choice of a specific edition depending on the needs of the organization and the degree of virtualization of the infrastructure. The choice of approach for implementing Windows Server is determined by the current state of the infrastructure and organizational requirements. It is possible to install on new hardware, upgrade an existing system while preserving configurations and data, migrate roles and services to a new environment, or gradually update a clustered infrastructure.

When installing Windows Server, the choice of configuration depends on the way the server is managed and the required level of functionality. A minimal installation without a graphical interface or a full installation with a graphical environment and management tools can be used.

For the purposes of this study, a virtual environment was built to analyze the status, security, and integrity of a Windows server operating system. The use of a virtual environment allows for controlled experimentation, monitoring of system behavior, and safe execution of checks without risk to real production infrastructure. Oracle VM VirtualBox was used as a virtualization platform, which provides the ability to create and manage isolated virtual machines, configure hardware resources, and simulate a real server environment. For this experiment, virtual machines with the Windows Server 2022 Standart Evaluation (Desktop Experience) operating system and Kali GNU/Linux 2026.1 installed were created.

Table 1. Win Server virtual resources

OS	Windows Server 2022 Standard Evaluation
Processor	64-bit
Virtual RAM (RAM)	8 GB
cores	4
disk space	60 GB (Dynamic Allocation)
Boot	BIOS (EFI disabled)
Network adapter	Internal Network ("labnet")

In this lab environment, the virtual machines are in Internal Network mode named "labnet". This allows only virtual machines that are connected to the virtual network with the corresponding network name to communicate with each other. In the scenario presented, 2 machines are connected to the network "labnet" - Windows Server (target) and Kali (attacker). Wazuh server inspects the security behaviour.

2. Known vulnerabilities.

Major Recent Vulnerabilities in Windows Server are:

(CVE)CVE-2025-59287 (Critical – CVSS 9.8): Description: Remote Code Execution (RCE) vulnerability in the Windows Server Update Services (WSUS)

component.Affected: All supported versions of Windows Server (including Windows Server 2022).Risk: No privileges or user interaction required; full system compromise over the network.

CVE-2025-50171: Description: Critical Authorization Bypass vulnerability in the Remote Desktop Server (RDS) component.Risk: Allows spoofing attacks over the network, impersonation of legitimate users, and potential access to sensitive data.

CVE-2025-21326 (CVSS 7.8): Description: Type confusion vulnerability (CWE-843) for remote code execution in Internet Explorer components of Windows Server 2022 (23H2).Risk: Execution of arbitrary code when loading specially crafted content.

3. Malicious activities hunting.

Several instruments for traffic and process explorations are used and various results are presented.

PowerShell was used as the main tool for outputting system information and configuration management. It was used to execute commands for analyzing processes, network connections, and system parameters. The *ps* command shows the active processes in the system, as well as the resources used by them. In Fig. 1, which is shown after executing the command, the following data is visible:

- Handles – number of system objects used by the process
- NPM(K) – memory that always remains in RAM
- PM(K) – memory that can be moved to virtual memory
- WS(K) – real RAM memory used
- CPU(s) – accumulated processor time in seconds
- id – unique process identifier
- SI – session ID
- ProcessName

The first process that is started after the kernel loads is *Smss.exe* (session manager). Its main functions are: to create user sessions; to start csrss.exe; to start wininit.exe; to nitialize the system environment. If this process is missing, Windows cannot be started.

It is shown in fig. that there are dozens of *svchost.exe* processes and it is completely normal because this process is a container in which Windows services run. Such as:

- Windows Update
- DHCP Client
- DNS Client
- Event Log
- Time Service.

The functions of *MsMpEng.exe* process (Microsoft defender antivirus engine) are as follows malware scanning, file monitoring and real-time protection.

SecurityHealthService process monitors the status of: Defender; Firewall; Windows Security.

Process *spoolsv.exe* is responsible for managing printers and print queues.

Registry is responsible for accessing the Windows Registry.

dllhost is used to execute COM components outside the main process.

conhost.exe (console window host) ensures the operation of: CMD; PowerShell; Terminal windows.

WmiPrvSE.exe (Windows Management Instrumentation Provider Host) is extremely important for: monitoring; system diagnostics and PowerShell commands themselves.

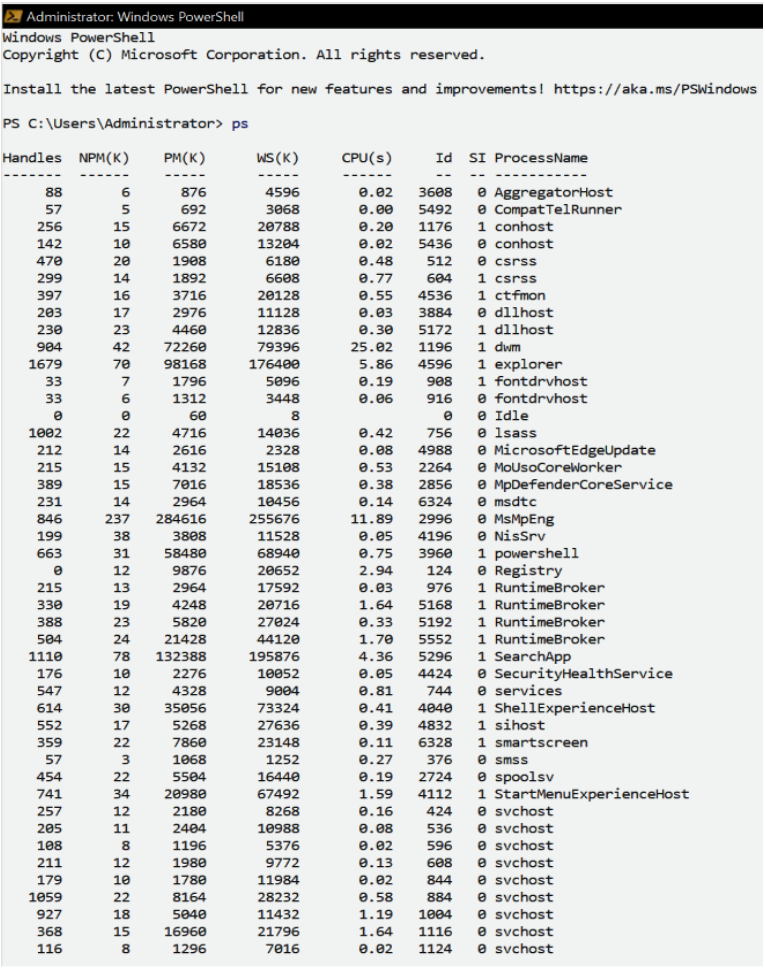


Fig. 1: - *ps* command output

Useful app is the Windows Event Viewer - it is a built-in tool in Windows Server that allows to analyze system logs. It allows you to view events related to security, system

errors, and user activity, which helps you detect anomalies and potential threats. The main categories of logs are:

- Application – contains events from installed software and applications
- Security – contains events related to security, such as successful and unsuccessful authentication attempts, changes in user rights, and other actions related to accessing the system
- System – contains events from the operating system, drivers, and system services
- Setup – contains information about installations, updates, and system changes.

The Windows Defender Firewall with Advanced Security tool was used to check the status of the operating system firewall. The tool itself offers the ability to manage incoming and outgoing network traffic, as well as create rules for accessing network resources. On Fig. 2 the three main Windows Firewall profiles are observed, namely: Domain Profile; Private Profile and Public Profile.

From the output, it can be seen the firewall for a domain environment is disabled. Domain profile is used when the computer is a member of an Active Directory domain and communicates with a domain controller. When Domain Firewall is disabled, there is a higher risk of unauthorized network connections in the domain infrastructure.

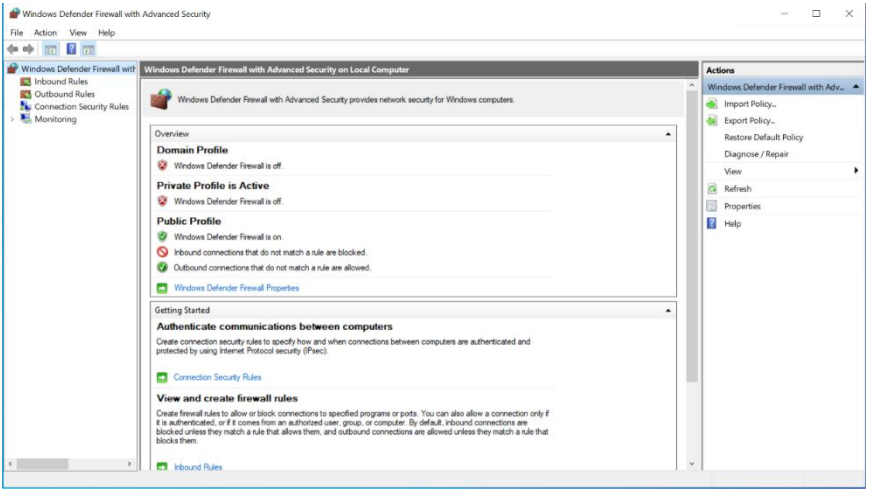


Fig. 2: - Windows Defender interface

For the essential hunting, A Wazuh environment was built, consisting of Wazuh Server and Wazuh Agent (Fig. 3 and Fig. 4). Wazuh Server was installed on the virtual machine with Kali GNU/Linux 2026.1, and Windows Server 2022 was monitored system by installing Wazuh Agent. Wazuh Dashboard is accessible via HTTPS on port 443, thus monitoring the status of the agent and the collected events was performed.

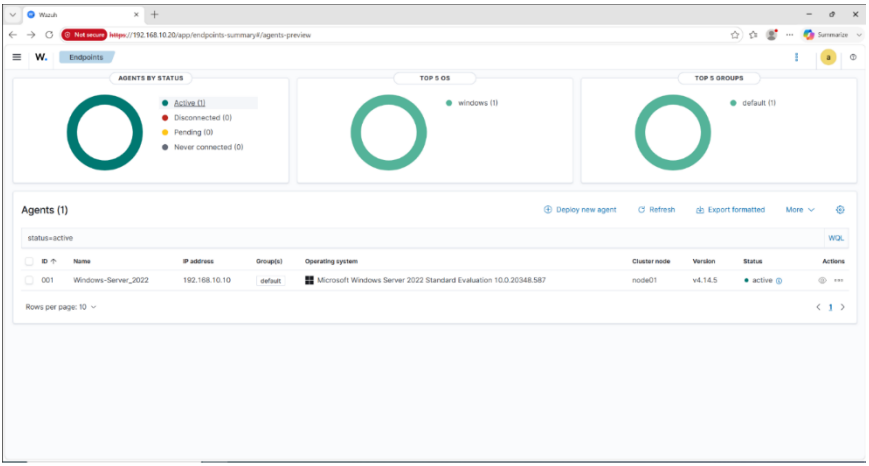


Fig. 3: - Wazuh agent installed to Wazuh manager

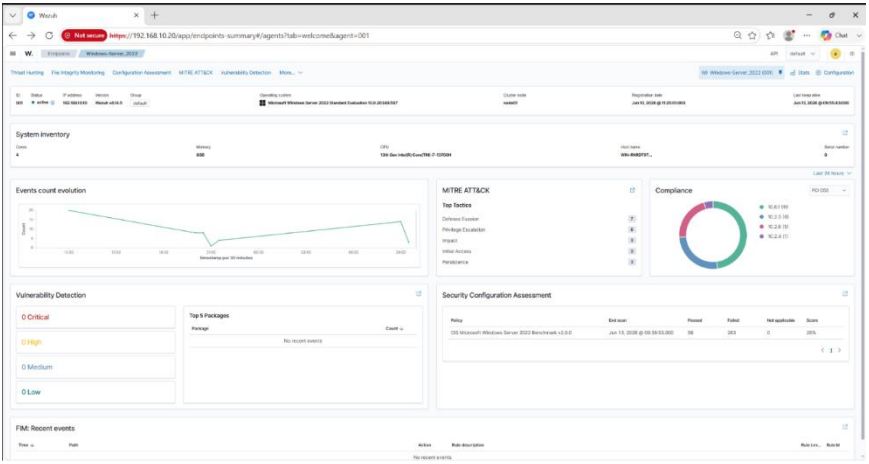


Fig. 4: - Wazuh information over Win Server 2022

The interface in Fig. 4 shows that Wazuh provides information about Windows Server 2022, including IP address, agent version, operating system and basic hardware characteristics. For successful communication between Windows Server and Wazuh

Manager, we are confirmed by the fact that the agent has an identifier of 001 and a status of Active. It is reported that 4 processor cores and 8 GB of RAM. It is shown that Wazuh classifies events by MITRE ATT&CK categories, such as Defense Evasion, Privilege Escalation, Initial Access and Persistence.

The observed in Fig. 5 is a summarized overview of the events, through the Threat Hunting module. For the corresponding period, a total of 58 events were reported, with none of them being of level 12 or higher. One unsuccessful attempt and three successful ones were registered for authentication. It is shown that there are periods with an increased number of events, which is normal when starting services, changing system configuration or performing administrative actions. Different groups are presented for the classification of the events, which are Windows, Windows Security and Windows Application.

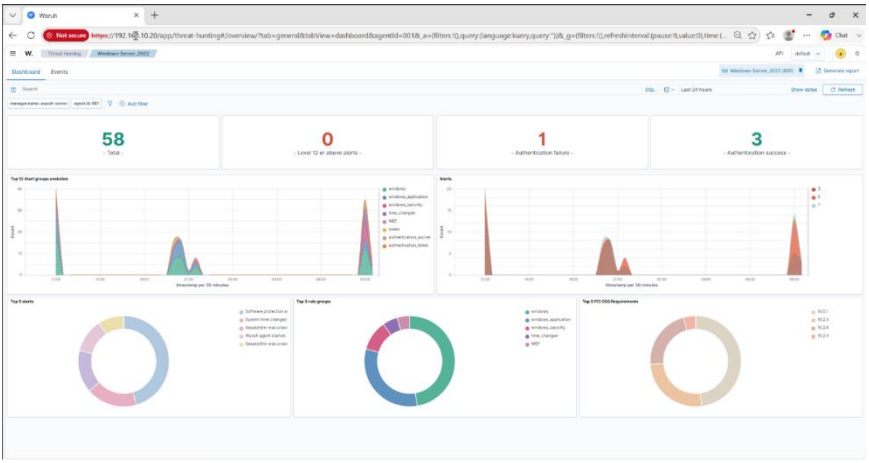


Fig. 5: - Threat Hunting module Event analysis

By correlating events and alarms, security workers may intercept malicious activities and hunt them from the initiation until end of attack vector. In any case, it is a bluky work in which automation is one kind of saving, yet insufficient.

Conclusion

The analysis examined the system configuration, active processes, services, network connections, and event logs. The correct operation of DNS and HTTPS communications is confirmed by the analysis of network traffic, and monitoring using Event Viewer and Wazuh allows tracking of events related to user authentication and the operation of system components.After it was found that the configuration of Windows Defender

Firewall was incorrect, as some of the security profiles were turned off. Then, by applying the necessary settings, the protection was improved and filtering of network traffic was achieved in all network profiles.With the use of modern analysis and monitoring tools, the results show that it allows for timely detection of potential vulnerabilities. The effectiveness of SIEM solutions in monitoring the health and protection of Windows Server 2022 is demonstrated by using Wazuh as a centralized platform for event collection and analysis.

It can be summarized that proper configuration, continuous monitoring and timely analysis of events are key to maintaining a high level of security and reliability in modern server environments.

References

1. Николов, Л. Г., Киберсигурност на комуникационно-информационните системи, Монография, 2021, ISBN 978-619-7531-22-0, стр. 46
2. Slavyanov, K., Dimov, R., Application of fuzzy logic in cybersecurity decision making and analysis after a cyber incident detection, ENVIRONMENT. TECHNOLOGIES. RESOURCES. Proceedings of the International Scientific and Practical Conference, 2024, ISSN 1691-5402, DOI: https://doi.org/10.17770/etr2024vol2.8022.
3. Borisova, A. R., Network attack recognition using fuzzy logic, Environment. Technology. Resources. Rezekne, LatviaProceedings of the 15th International Scientific and Practical Conference. Volume II, 55-60, 2024, ISSN 1691-5402, DOI: https://doi.org/10.17770/etr2024vol2.8054.
4. Beggs, R. W. (2014). Mastering Kali Linux for Advanced Penetration Testing. Birmingham: Packt Publishing.
5. Hertzog, R., & O'Gorman, J. (2017). Kali Linux Revealed: Mastering the Penetration Testing Distribution. OffSec Press.

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

MALICIOUS ACTIVITIES HUNTING IN LINUX DEVICES

Linko G. Nikolov, Akan Hilmi

"Cybersecurity and IT" Section, Scientific Research Instutite, National Military University,
linkonikolov@gmail.com ; akin.hilmi.4@gmail.com

***Abstract**: Linux end devices support is one of the most significant batlefield IT operations in contemporary warfare. Focusing on the social engineering techniques, Linux devices and their operating systems are the plane whereas attacker will try to enter if possible. In this research paper malicious activities into Linux devices is searched and checked in the means of processes, services, Sysmon and Logmon security aspects. Specialized inspection software is used into a virtuali machine environment as a controlled laboratory setup.*

***Keywords**: Linux malware, Linux security, cybersecurity*

Introduction

Linux terminals operation support during military tactical operations comprises contemporary equipment, alongside with enhanced sysadmin skills. Linux services and administration support includes appropriate configuration and further monitoring. Communication and information systems (CIS) support during military tactical operations relies on a combination of contemporary equipment and devoted personnel, working together to maintain seamless connectivity and ensure operational readiness. Effective Linux support involves the precise configuration of servers and terminals, ensuring that the infrastructure remains stable and capable of handling service traffic efficiently, while also preserving traffic data as a cybersecurity artifact [3] whenever possible. This is critical for maintaining situational awareness in dynamic environments and responding swiftly to potential cyber attacks.

Linux system analysis is a fundamental aspect of maintaining operational availability and performance, proving especially valuable during cyber incidents. It allows for the identification of unusual OS behaviour, the evaluation of RAM and process resources usage, and the verification of system configurations. However, manual analysis is a time-consuming and resource-intensive process, requiring significant expertise and attention to detail. Although automation systems and artificial intelligence (AI) tools have been developed to assist in this area [2], [3], many still lack the fine precision and adaptability required for complex, real-time environments. As a result, specialized application software is often utilized to gain a comprehensive understanding of system operations, providing detailed insights that are crucial for diagnosing issues, optimizing performance, and ensuring security.

In this project, a virtual Linux machine for an artillery division is to be utilized, providing a robust foundation for communication and coordination in a tactical setting. This project required the deployment of several network services to ensure the infrastructure's reliability and functionality.

1. Linux OS operation.

A process is the basic unit of execution in the Linux operating system. Each program, command, or system service that is started creates one or more processes, each of which is assigned a unique identifier by the kernel, the Process ID (PID). The processes are isolated from each other: each has its own virtual address space, file descriptors, and security attributes. This isolation is a fundamental mechanism for system stability and security.. When a command is run or an application is opened, the kernel allocates memory, initializes the process structure, assigns a PID, and adds it to the process table (/proc). The process inherits the environment of its parent—current directory, environment variables, open files. All processes in the system form a hierarchical tree with init/systemd as the root.

```
remnux@akin:~$ pstree | head -25
systemd-+-ModemManager---3*[{ModemManager}]
        |-NetworkManager---3*[{NetworkManager}]
        |-VBoxDRMClient---5*[{VBoxDRMClient}]
        |-VBoxService---8*[{VBoxService}]
        |-accounts-daemon---3*[{accounts-daemon}]
        |-colord---3*[{colord}]
        |-dbus-daemon
        |-gdm3-+-gdm-session-wor-+-gdm-wayland-ses-+-gnome-session-b---3*[{gnome-session-b}]
        |      |                 |                 `-3*[{gdm-wayland-ses}]
        |      |                 `-3*[{gdm-session-wor}]
        |      `-3*[{gdm3}]
        |-gnome-remote-de---3*[{gnome-remote-de}]
        |-multipathd---6*[{multipathd}]
        |-networkd-dispat
        |-polkitd---3*[{polkitd}]
        |-rtkit-daemon---2*[{rtkit-daemon}]
        |-systemd-+-(sd-pam)
        |         |-VBoxClient---VBoxClient---3*[{VBoxClient}]
        |         |-VBoxClient---VBoxClient---2*[{VBoxClient}]
        |         |-dbus-daemon
        |         |-dconf-service---3*[{dconf-service}]
        |         |-evolution-addre---6*[{evolution-addre}]
        |         |-evolution-calen---9*[{evolution-calen}]
        |         |-evolution-sourc---4*[{evolution-sourc}]
        |         |-gcr-ssh-agent---2*[{gcr-ssh-agent}]
remnux@akin:~$ S
```

Fig. 1: Linux process hierarchy (*systemd* - the "parent of parents")

When a Linux system boots, the kernel starts only two processes directly: **systemd** (PID 1) and **kthreadd** (PID2). *Systemd* is the first user process and the parent of all other user processes. It initializes the system, starts services, manages the mounting of file systems, and is responsible for proper shutdown. If the system is configured without *systemd* (e.g., with OpenRC or SysVinit), then PID 1 is the corresponding init process. *Systemd* is also the parent of all orphan processes — when a parent process dies, its children are automatically adopted by PID 1.

The kernel daemon *kthreadd* (PID 2) is the kernel thread daemon. It is the parent of all kernel threads in the system—the processes shown in [square brackets] when you run ps aux. When the kernel needs to create a new internal thread (such as kworker, watchdog, or migration), it queues a request and kthreadd processes it. Kthreadd sleeps waiting for requests and wakes up only when needed.

All kernel processes are shown on fig. 2.

```
remnux@akin:~$ ps aux | head -30
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.4  0.3  22436 13524 ?        Ss   08:04   0:03 /sbin/init
root           2  0.0  0.0      0     0 ?        S    08:04   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    08:04   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   08:04   0:00 [kworker/R-rcu_g]
root           5  0.0  0.0      0     0 ?        I<   08:04   0:00 [kworker/R-rcu_p]
root           6  0.0  0.0      0     0 ?        I<   08:04   0:00 [kworker/R-slub_]
root           7  0.0  0.0      0     0 ?        I<   08:04   0:00 [kworker/R-netns]
root          10  0.0  0.0      0     0 ?        I<   08:04   0:00 [kworker/0:0H-events_highpri]
root          12  0.0  0.0      0     0 ?        I<   08:04   0:00 [kworker/R-mm_pe]
root          13  0.0  0.0      0     0 ?        I    08:04   0:00 [rcu_tasks_kthread]
root          14  0.0  0.0      0     0 ?        I    08:04   0:00 [rcu_tasks_rude_kthread]
root          15  0.0  0.0      0     0 ?        I    08:04   0:00 [rcu_tasks_trace_kthread]
root          16  0.0  0.0      0     0 ?        S    08:04   0:00 [ksoftirqd/0]
root          17  0.0  0.0      0     0 ?        I    08:04   0:00 [rcu_preempt]
root          18  0.0  0.0      0     0 ?        S    08:04   0:00 [migration/0]
root          19  0.0  0.0      0     0 ?        S    08:04   0:00 [idle_inject/0]
root          20  0.0  0.0      0     0 ?        S    08:04   0:00 [cpuhp/0]
root          21  0.0  0.0      0     0 ?        S    08:04   0:00 [cpuhp/1]
root          22  0.0  0.0      0     0 ?        S    08:04   0:00 [idle_inject/1]
root          23  0.0  0.0      0     0 ?        S    08:04   0:00 [migration/1]
root          24  0.0  0.0      0     0 ?        S    08:04   0:00 [ksoftirqd/1]
root          25  0.0  0.0      0     0 ?        I    08:04   0:00 [kworker/1:0-cgroup_destroy]
root          27  0.0  0.0      0     0 ?        S    08:04   0:00 [kdevtmpfs]
root          28  0.0  0.0      0     0 ?        I<   08:04   0:00 [kworker/R-inet_]
root          29  0.0  0.0      0     0 ?        S    08:04   0:00 [kauditd]
root          30  0.0  0.0      0     0 ?        S    08:04   0:00 [khungtaskd]
root          32  0.0  0.0      0     0 ?        S    08:04   0:00 [oom_reaper]
root          33  0.0  0.0      0     0 ?        I    08:04   0:00 [kworker/u4:2-events_power_efficient]
root          34  0.0  0.0      0     0 ?        I<   08:04   0:00 [kworker/R-write]
remnux@akin:~$ S
```

Fig. 2 - The first 30 kernel processes

Knowledge of Linux OS operating system is the initial requirement when conducting cyber activities hunting. Anyway, the presented output on figures is attained manually, which is not the case when number of expected analyzed machines is lagre. Software automation shall be in favor.

2. Several known vulnerabilities.

Active Exploits as of September 2026 are reported by The Cybersecurity and Infrastructure Security Agency (CISA) [6]. It added three actively exploited kernel flaws to its Known Exploited Vulnerabilities catalog:

- CVE-2025-39682 (TLS Zero-Length Record): A flaw in the Transport Layer Security (TLS) receive path allows crafted zero-length records to cause memory disclosure or a denial of service;

- CVE-2026-53266 (Netfilter ebtables SNAT): An out-of-bounds write vulnerability in the network bridge code can corrupt memory, leading to a system crash or local privilege escalation;

- CVE-2025-39964 (AF_ALG Socket Race Condition): A race condition in socket handling can leave the system in an inconsistent state and cause unexpected crashes.Recent 2026 Privilege Escalation Flaws;

- CVE-2026-31431 ("Copy Fail"): A high-severity local privilege escalation flaw affecting mainstream Linux kernels built since 2017;

- CVE-2026-43284 & CVE-2026-43500 ("Dirty Frag"): Two local privilege escalation vulnerabilities found in network security modules like IPsec and AFS protocol support. Fixes via official channels such as Ubuntu Security Notices can be reviewed [5].

3. Malicious activities hunting.

The following methodology for hunting is proposed in Table 1.

Table 1. A systematic analysis of Linux OS

№	**main steps / `example syntax`**
1	Analysis of suspicious processes - malware (such as cryptominers and rootkits) often consumes significant resources or tries to hide itself [7]. Check for deleted executables that are still running (a common sign of malware)

	`top -b -n 1 | head -n 20`
	`ps aux --sort=-%cpu | head -n 10`
	`ls -al /proc/*/exe | grep "deleted"`

2	Network activity check - malware typically communicates with Command & Control (C2) servers or performs scanning. Look for unusual open ports: check processes that are listening (LISTEN) for incoming connections, especially from unexpected binaries.
	`ss -tupna` `lsof -i -P -n | grep ESTABLISHED`
3	Persistence mechanisms check - checking Systemd services: malicious unit files can launch reverse shells. Cron tasks check.
	`ls -la /etc/systemd/system/ systemctl list-unit-files --type=service` `ls -la /etc/cron* /var/spool/cron/crontabs/ cat /etc/crontab`
4	Audit user accounts and permissions - search for new or unexpected users: Check for accounts with UID 0 (root permissions) or no passwords. Checking sudoers configuration: make sure there are no unauthorized users with full privileges.
	`grep 'x:0:' /etc/passwd sudo awk -F: '($2=="") {print $1}' /etc/shadow` `cat /etc/sudoers ls -la /etc/sudoers.d/`
5	Analysis of system logs and history - search for errors and unauthorized access. View command history (shell history): attackers often use commands like `curl`, `wget`, and `sh` to execute directly in memory
	`sudo journalctl -p err -b sudo journalctl _SYSTEMD_UNIT=ssh.service | grep "Failed"` `cat ~/.bash_history | grep -E "curl|wget|chmod|ssh"`

When the necessary macnihes for analysis are low as a number, the first step in the process of hunting may be manual inspection (Fig. 3).

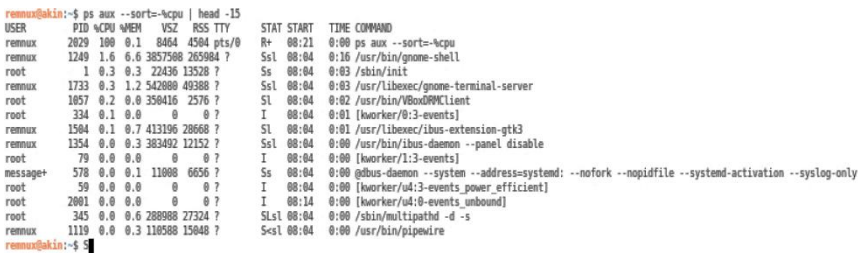
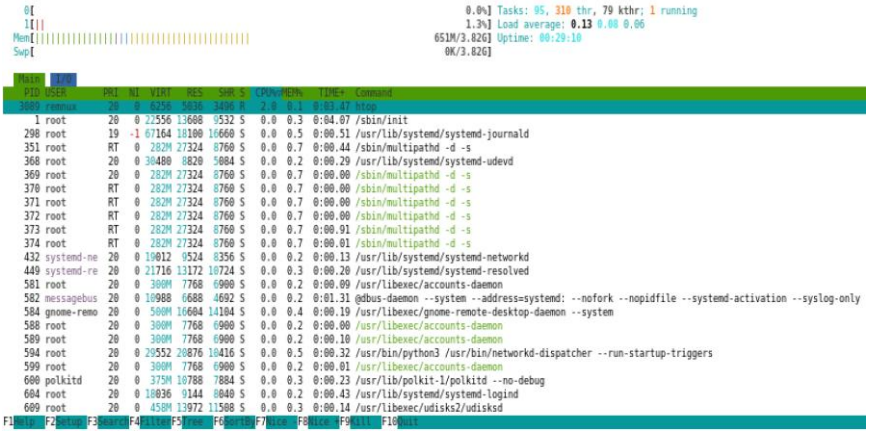


Fig. 3 - Output of command: *ps aux --sort=-%cpu | head -15* (high CPU utilization)

Watching processes manually is not the best practice, however it must be acquired as a skill. For automated hunting and enterprise-level protection, it is recommended to implement specialized tools such as ClamAV for scanning, Auditd for auditing system calls, or more complex EDR solutions such as Cortex XDR.

Another command for better human readable vision is the htop (Fig. 4).


0[0.0%] Tasks: 95, 310 thr, 79 kthr; 1 running
1[|| 1.3%] Load average: 0.13 0.08 0.06
Mem[|||||||

```
root@akin:/home/remnux# systemctl cat ssh
# /usr/lib/systemd/system/ssh.service
[Unit]
Description=OpenBSD Secure Shell server
Documentation=man:sshd(8) man:sshd_config(5)
After=network.target auditd.service
ConditionPathExists=!/etc/ssh/sshd_not_to_be_run

[Service]
EnvironmentFile=-/etc/default/ssh
ExecStartPre=/usr/sbin/sshd -t
ExecStart=/usr/sbin/sshd -D $SSHD_OPTS
ExecReload=/usr/sbin/sshd -t
ExecReload=/bin/kill -HUP $MAINPID
KillMode=process
Restart=on-failure
RestartPreventExitStatus=255
Type=notify
RuntimeDirectory=sshd
RuntimeDirectoryMode=0755

[Install]
WantedBy=multi-user.target
Alias=sshd.service
root@akin:/home/remnux# S
```

Fig. 5 - SSH service check

```
remnux@akin:~$ sudo bash
root@akin:/home/remnux# rkhunter --check --sk 2>/dev/null | tail -30 || echo
    Checking for other suspicious configuration settings      [ None found ]
    Checking for a running system logging daemon              [ Found ]
    Checking for a system logging configuration file          [ Found ]

  Performing filesystem checks
    Checking /dev for suspicious file types                   [ None found ]
    Checking for hidden files and directories                 [ Warning ]


System checks summary
=====================

File properties checks...
    Files checked: 139
    Suspect files: 3

Rootkit checks...
    Rootkits checked : 495
    Possible rootkits: 0

Applications checks...
    All checks skipped

The system checks took: 4 minutes and 45 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)

root@akin:/home/remnux#
```

Fig. 6 - Rootkit check by rkhunter package

```
remnux@akin:~$ clamscan -r --infected ~/diploma_lab/attack/
/home/remnux/diploma_lab/attack/eicar_test.txt: Eicar-Test-Signature FOUND

----------- SCAN SUMMARY -----------
Known viruses: 3627867
Engine version: 1.4.4
Scanned directories: 1
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 20.047 sec (0 m 20 s)
Start Date: 2026:06:10 07:29:13
End Date:   2026:06:10 07:29:34
remnux@akin:~$
```

Fig. 7 - EICAR file found

Monitoring - in modern cybersecurity operations, the success of cyberdomain defence depends on components such as network detecton and response (NDR), network access control (NAC), endpoint detection and response (EDR), extended detection and response (XDR), SIEM servers, and network devices that support both monitoring and proactive response. Such enhanced environment must be carefully configured and managed to ensure reliable and secure incident and event management, as well as efficient reposne (SOAR). The role of computer security personnel in this context extends beyond basic monitoring: they must possess the practical skills required for precise security actions, ensuring that all systems are properly set up to support security messages. These configurations might include setting up controls, secured protocols, optimizing OS processess, and implementing necessary security measures such as Next-generation firewalls and Behavioral Antivirus programs. This hands-on expertise is vital to ensure the end point is optimized for performance while minimizing vulnerabilities.

Specialized software and dedicated hardware resources, such as Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) tools, are employed to automate the monitoring process. These tools can visualize OS behaviour, highlight anomalies, and provide real-time alerts, allowing IT personnel to quickly identify and address issues. Automated tools like these can also generate detailed reports that are valuable for both post-operation analysis and ongoing adjustments to improve endpoint performance.

Linux defence - application of the latest kernel updates from the distribution vendor. Enable Firewalls: restrict unnecessary network exposure to lower the risk of remote attacks. Use Least Privilege: limit user permissions so attackers cannot easily gain root access. Monitor Logs: watch system logs regularly for strange activity or errors.

4. Conclusion

Network device configuration must be precisely calculated, planned and implemented. After network operation start, devices functionality must be foreseen and monitored accordingly. Enhanced cyber attacks can be initiated at the OSI layer 3 and 2 level before further lateral movement. The presented small-scale research presented several steps and techniques, used for malicious activities checks inside the network

devices such as routers and switches. Nevertheless, during routine cybersecurity operations, malicious hunting in network devices must not be rejected, but allegedly used and even improved over time in the means of personnel efforts, and equipment (hardware and software) evolution.

In summary, monitoring the digital environment of battlefield CIS is not merely about tracking performance — it is about creating a resilient and adaptive service infrastructure that can meet the dynamic needs of military operations, from supporting real-time decision-making to maintaining the security and integrity of critical data flows

References

1. Николов, Л. Г., Киберсигурност на комуникационно-информационните системи, Монография, Шумен, 2021, ISBN 978-619-7531-22-0
2. Slavyanov, K., Dimov, R., Application of fuzzy logic in cybersecurity decision making and analysis after a cyber incident detection, ENVIRONMENT. TECHNOLOGIES. RESOURCES. Proceedings of the International Scientific and Practical Conference, 2024, ISSN 1691-5402, DOI: https://doi.org/10.17770/etr2024vol2.8022.
3. Borisova, A. R., Network attack recognition using fuzzy logic, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 15th International Scientific and Practical Conference. Volume II, 55-60, 2024, ISSN 1691-5402, DOI: https://doi.org/10.17770/etr2024vol2.8054.
4. Joseph Migga Kizza, „Guide to Computer Network Security", Springer, 2009, ISSN 1617-7975.
5. Ubuntu, Linux kernel vulnerabilities, URL: https://ubuntu.com/security/notices/USN-8817-1
6. CISA - Linux kernel CVEs, URL: https://blog.qualys.com/product-tech/2026/09/23/cisa-bod-26-04-timelines-for-three-linux-kernel-cves
7. Tuxcare, 2026 Linux malware, URL: https://tuxcare.com/blog/linux-malware/

MODERN TECHNOLOGIES FOR SECURE STORAGE AND PROTECTION OF CRITICAL INFORMATION AGAINST CONTEMPORARY CYBER THREATS

Daniel Mitich, Elena Karadzhova, Nikoleta Pehlivanova

Vasil Levski National Military University, Faculty of Artillery, Air Defence and Communication and Information Systems, Shumen, Bulgaria, mitichinc@gmail.com

Abstract: *In the age of digital technology, proper management, recording, and protection of information is often neglected by average users, yet this exact aspect provides crucial opportunities and advantages for unauthorized individuals to access it. To effectively manage information risks, it is important to understand the differences between critical, personal, and other types of information, as well as the appropriate methods for their storage and protection.*

Keywords: *Critical Information, Personal Information, Cyber Attacks, Information Security*

МОДЕРНИ ТЕХНОЛОГИИ ЗА НАДЕЖДНО СЪХРАНЕНИЕ И ЗАЩИТА НА КРИТИЧНА ИНФОРМАЦИЯ В УСЛОВИЯТА НА СЪВРЕМЕННИТЕ КИБЕР ЗАПЛАХИ

Даниел Митич, Елена Караджова, Николета Пехливанова

НВУ „Васил Левски“, Факултет „Артилерия, ПВО и КИС“ гр. Шумен, mitichinc@gmail.com

Резюме: *В епохата на цифровите технологии правилното управление, записване и защита на информацията е често неглежирано от обикновенният им потребител, но точно този аспект е от съществено значение и преимущество за хората с неоторизиран достъп да се доберат до тях. За успешното справяне с информационните рискове е важно да разберем разликите между критичната, личната и другите видове информация, както и подходящите методи за нейното съхранение и защита.*

Ключови думи: *Критична информация, Лична информация, Кибер атаки, Информационна сигурност*

1. Видове информация и приоритетност на складиране

Правилното категоризиране на информацията е първата и най-съществена стъпка при осигуряването на нейната надеждна защита и подходящо съхранение. То позволява на потребителите и организациите да разпознават и прилагат различни нива на сигурност в зависимост от чувствителността и риска, който би възникнал при изтичане или компрометиране на съответните данни. Важно е да се различават, опазват и селектират, защото при изтичане на важна информация за дадена организация, освен съдебната отговорност която носи в повечето случаи, това изтичане може да навреди сериозно на хората в организацията и на самата организация.

В практиката се разграничават основно три категории информация, базирани на степента на важност и потенциалните последствия при неправомерен достъп или загуба:

-*Общодостъпна информация* Тази информация (например публични новини, рекламни материали, официални съобщения) не носи значителен риск при евентуалното ѝ изтичане. Съхранението ѝ не изисква високи нива на защита и не е приоритет от гледна точка на информационната сигурност. Общодостъпната информация има най-нисък приоритет и не изисква специални мерки за защита, което позволява спестяване на ресурси за подсигуряване на останалите категории информация.

-*Лична информация* Това са чувствителни данни, идентифициращи конкретни хора, като ЕГН, банкови сметки, домашен адрес, телефонни номера, медицински данни, семейни снимки и други лични материали. Тези данни задължително трябва да се съхраняват при високо ниво на сигурност, тъй като неправомерното им разпространение може да доведе до сериозни лични, финансови и правни последици за засегнатите лица. Личната информация има висок приоритет и трябва да бъде защитена чрез криптиране, ограничаване на достъпа, сигурно архивиране и подходящи политики.

-*Критична информация* Тази информация е ключова за дейността на организации и фирми. Включва финансови отчети, обороти, лични данни за служители, информация за налично имущество, търговски тайни, производствени процеси и други. Тя изисква най-високо ниво на защита, защото изтичането ѝ може да доведе до сериозни щети за организацията – както финансови и репутационни, така и до нарушения на законови изисквания. Критичната информация се складира с най-висок приоритет, като се използват криптиране, защитени мрежи, специализиран достъп и строг контрол.

2. Чести грешки и слабости

Сред слабостите в защитата на информацията по-рядко се среща, но все пак съществува проблемът с лошо изградена или неефективна софтуерна среда. Въпреки широкото разпространение на професионални решения за защита, понякога организации или потребители използват стари, неактуализирани или неправилно конфигурирани системи, които правят данните уязвими към кибер атаки и злонамерен достъп.

Средна по честота, но значима слабост, е неадекватно изградена физическа среда за съхранение на информацията. Често помещенията за съхранение на сървъри или носители с важни данни са недостатъчно обезопасени, с липсващ или слаб контрол на достъпа, както и недобре планирани варианти за резервно копиране и възстановяване при аварийни ситуации като неизправност или повреда на съхраняващите устройства. Това може да доведе до продължителна загуба на данни и сериозни оперативни проблеми.

Най-често срещаната слабост обаче остава човешкият фактор и недостатъчно обучените потребители. Голяма част от хората нямат ясна представа за потенциалните заплахи в дигиталната среда и са особено уязвими към социално-

инженерни техники като фишинг, манипулативни съобщения и злонамерени имейли, които целят измама или компрометиране на лични и критични данни. Потребителите нерядко използват слаби или повтарящи се пароли, не прилагат двуфакторна автентикация и съхраняват важна информация на необезопасени и незашифровани носители. Освен това, често те са склонни да използват публични и несигурни интернет мрежи за достъп до чувствителни данни, което повишава риска от тяхното неправомерно използване.

Ефективното преодоляване на тези слабости изисква цялостен подход, включващ постоянна актуализация на технологичните решения, внимателно планиране и контрол върху физическите системи за съхранение, както и системно обучение и информираност на потребителите за предотвратяване на грешките и рисковете в цифровата среда.

3. Актуални методи за защитено записване на информация

Сред съвременните подходи за защита на информацията от особено значение е използването на подходящите технологии и стратегии за съхранение и архивиране, съобразени с чувствителността и важността на данните. Като базово ниво на защита за информация, която не представлява висок риск при евентуално компрометиране (например публични материали или обща бизнес кореспонденция), е подходящо интелигентното и икономично използване на широко достъпните облачни (клауд) услуги като Google Drive, Microsoft OneDrive или Dropbox. Тези платформи са лесни за употреба, имат базова сигурност и са достатъчно ефективни при съхранение на данни с ниско до средно ниво на чувствителност, като могат да бъдат приложими и за съхранение на ограничено количество лична информация, стига тя да не съдържа най-чувствителните данни (например здравни записи или банкови детайли).

За информация, която не трябва да бъде достъпна от никой извън дадената организация не може да се разчита на външни корпоративни услуги, за това е нужно вътрешно издигане на инфра структура за тип данни, при които компрометирането би довело до сериозни последствия като бизнес отчети, финансова документация и по-чувствителни лични данни. Тогава е силно препоръчително да се прилагат системи за локално съхранение със средна до висока сигурност, включително RAID-системи. RAID-технологията осигурява надеждност и висока устойчивост срещу загуба на данни при хардуерна повреда, като информацията се разпределя между няколко диска и е възможно възстановяване дори при отказ на някое от записващите устройства. В допълнение, интегрирането на постоянен мониторинг (24/7) на трафика, състоянието и работоспособността на записващите устройства позволява бърза реакция при евентуални проблеми, както и превантивна диагностика, предотвратяваща загуба на данни.

Най-високото ниво на сигурност е необходимо при съхранението на критична информация, като строго секретни документи, налични боеприпаси, съдебни и/или административни архиви, чието изтичане или загуба може да застраши сериозно бизнеса, държавни институции и да има сериозни правни и финансови

последствия. За постигане на тази максимална защита се препоръчва подходът на използване на два физически сървъра, разположени на различни геотектонични плочи. Тази практика осигурява физическа устойчивост срещу сериозни природни бедствия като земетресения или наводнения. Освен това задължително е седмично записване на друго физическо устройство (backup) на критичните данни, което гарантира, че дори при загуба на информация на единия от сървърите, тя може да бъде бързо и ефективно възстановена от другия. Комбинацията от изброените методи и технологии позволява интелигентно и надеждно управление на информационната сигурност, при което нивото на защита е адаптирано спрямо реалния риск и чувствителност на конкретните данни. Така организациите и потребителите могат да използват ресурсите си оптимално и да осигурят ефективна защита на информацията във всяка ситуация.

4. Методи за висока сигурност в работна среда

Сигурността на информацията в работната среда изисква прилагане на комбиниран подход, включващ технически решения, строги организационни политики, адаптивност и проучване към нови заплахи и ефективна комуникация между служителите.

Високото ниво на защита започва още с физическата сигурност, като важен аспект е ограничаването на физическия достъп до чувствителни помещения и устройства. Такива помещения са например сървърните зали и архивите с документи, където достъпът трябва да бъде контролиран чрез използването на карти за идентификация(RFID технологията е за предпочитане), биометрични системи (пръстови отпечатъци, лицево разпознаване) и 24-часово видеонаблюдение с регистриране на всички посещения. Технически погледнато, от съществено значение е изграждането на защитени вътрешни мрежи, които задължително включват криптирана комуникация (VPN), стриктна автентикация на всички потребители и устройства в мрежата и внедряване на силни защитни стени (firewall). Системите за мониторинг на мрежовия трафик (IDS/IPS) позволяват бързо откриване на подозрителна активност или опити за пробиви и дават възможност за незабавна реакция при възникнали заплахи.

Особено важен аспект за висока сигурност е управлението на потребителски достъп. Защитената работна среда следва принципа на минимален необходим достъп, като служителите получават права само до онази информация и ресурси, които са им нужни за изпълнение на служебните задължения. Освен това задължително е прилагането на двуфакторна или многофакторна автентикация (2FA/MFA), което силно ограничава възможността за неоторизиран достъп при изтичане на пароли. Една от най-ефективните практики за висока сигурност е редовното обучение и информиране на служителите относно съвременните кибер рискове. Провеждането на периодични обучения и симулации на социално-инженерни атаки като фишинг и spear-phishing повишава общата киберхигиена и намалява риска служителите неволно да компрометират информационната сигурност. От гледна точка на технологиите за записване и архивиране, високата сигурност включва задължителното използване на криптиране на съхранената

информация, както и постоянни автоматични архиви на данни, пазени на различни локации и върху различни устройства, включително на физически отдалечени места, осигуряващи устойчивост при бедствия.

Не на последно място, строгите вътрешни политики за използване на служебни устройства и систематичният мониторинг на информационните системи гарантират бързото откриване и минимизиране на последствията при евентуални пробиви или инциденти. Изграждането на екипи за реакция при инциденти (Incident Response Teams) с предварително дефинирани роли и отговорности е добра педпоставка за бързото и ефективно овладяване на заплахите. Съчетанието на тези методи и подходи гарантира създаването и поддържането на среда с висока сигурност, способна да устои на съвременните заплахи в дигиталния свят.

Литература:

1. БДС ISO 7144:2011, Документация. Оформяне на дисертации и подобни документи.
2. Европейски правен преглед. София: Българска асоциация за европейско право, 2011. ISSN 1314-4847.
3. Australasian Journal of Educational Technology. Online. vol. 16 (Winter 2000), no. 2. Tugun, QLD: ASCILITE, 1985–. ISSN 1449-5554. Available from: https://ajet.org.au/index.php/AJET/issue/view/67. [viewed 2025-02-28].
4. STRINGER, John A., et al. Reduction of RF-induced sample heating with a scroll coil resonator structure for solid-state NMR probes. Online.

IMPACT OF HYPERPARAMETERS AND DATA SCALING METHODS ON THE PERFORMANCE OF DEEP NEURAL NETWORKS FOR NETWORK ATTACK DETECTION

Angela R. Borisova

Computer Systems and Technologies Department, Artillery, AAD and CIS Faculty, Vasil Levski National Military University, Shumen, Bulgaria, arborisova@nvu.bg

Abstract *The increasing volume of network traffic and its growing impact on both the Internet community and the performance and security of computer networks and related devices necessitates the use of deeply structured neural architectures. The effectiveness of deeply structured neural models for achieving cybersecurity depends on their overall pipeline, which includes selecting the correct architecture, tuning architectural and optimization hyperparameters, as well as preprocessing and scaling input parameters. In the proposed approach, two deeply structured neural networks are developed, trained, and tested – a One-Dimensional Convolutional Neural Network and a Bidirectional Long Sort-Term Memory. To accurately classify network data, the neural models extract specific features from the network traffic, group network packets into sequences of data of a certain length, determine a sliding window step, and normalize the data within a unified range.*

The conducted experiments demonstrate that the choice of appropriate parameters and proper data scaling is crucial in distinguishing the type of network traffic.

Keywords*: scaler, hyperparameters, network traffic, deep neural networks*

The rapid development of computer technologies is changing the way data is exchanged. The increasing integration of artificial intelligence, particularly deep structured learning, is a prerequisite for the growth in the number and power of computational resources. Almost without human intervention, neural networks operate independently thanks to a pre-built hierarchical representation of input features [3]. Deep learning models utilize semi-dynamic identification [3] of data from network traffic.Neural architectures such as 1D CNN and Bidirectional Long Short-Term Memory are used for analyzing and classifying network data. Convolutional layers extract local features, while the layers of the bidirectional LSTM model temporal dependencies in network data sequences. Reference [1] examines hybrid combinations, such as Attention-CNN-LSTM, aimed at reducing noise pollution. In [6], the authors in one study consider Software Defined Networking (SDN) an effective tool for detecting network intrusions, outlining key steps in developing traffic detection systems—from data preprocessing to hyperparameter tuning and creating a comprehensive model. In this regard, when scaling is not done correctly, the large numerical values of the input features have an asymmetrical impact on the learning process [6]. Data scaling transforms numerical input data into a specific range, most commonly 0 to 1 or -1 to 1. Well-known scaling algorithms provided by the scikit-learn library include: MinMaxScaler (which compresses the data such that the minimum value among the input features becomes 0 and the maximum value becomes 1), StandardScaler (centers data around 0—meaning

the mean becomes 0 and the variance or standard deviation becomes 1), RobustScaler (robust to extremely large values; uses the median and interquartile range (IQR) to scale input features), MaxAbsScaler (compresses data by dividing the numerical value of each input feature by the maximum absolute value in the corresponding column, resulting in a range of -1 to 1), Normalizer (scaling is performed for each input sample independently of the other samples) [7][8], and others. In [5], using deep learning technologies, the authors address issues like poor explainability, many false positive alarms, and low performance in real systems. To achieve good forecasting results, in addition to appropriate data scaling and the automatic adjustment of the model's internal parameters [4] (weights and biases), the neural network must also properly parameterize the input features. The selection and configuration of the so-called hyperparameters determine the success rate in distinguishing attacks from legitimate traffic [2]. Crucial hyperparameters include the number of neurons and hidden layers, activation functions, kernel size, the regularization coefficient (lambda), dropout, learning rate [2], window size, stride, dilation rate, attention heads, batch size, epochs, the patience parameter for early stopping, the factor and patience parameters for learning rate reduction, optimizer selection, loss functions, pooling and others. Reference [11] examines CNN and RNN (Recurrent Neural Network) models for feature extraction from network traffic and the approaches used for this purpose. Article [10] employs a CNN-LSTM architecture and performs automatic hyperparameter optimization using Particle Swarm Optimization (PSO). The authors address the issues of high-dimensional network data and the presence of large amounts of redundant and unnecessary network data.

The structure of the scientific report describes the sequential steps that were taken during the conducted research. CNN and LSTM models for deep learning, hyperparameters, and approaches for scaling input data have been examined. The methodology for processing, and normalizing network data is presented, input batch sequences have been generated, and the architectures of the developed 1D CNN and Bidirectional LSTM models are described. Experiments have been conducted to observe the influence of various hyperparameters and scaling methods on the performance of the models. The results obtained have been evaluated and analyzed using selected metrics – overall accuracy, weighted precision, weighted recall, weighted F1-score, as well as through a confusion matrix and ROC Curve. Finally, the main findings of the study have been summarized.

1. Metodology and methods

For the purposes of this research, two training scripts and two sniffer scripts have been developed, respectively for the One-dimensional Convolutional Neural architecture and for the Bidirectional Long Short-Term Memory. The software distributions used are: the development environment for scripts – Pycharm, the scripting language Python, the virtual environment for simulating attacks – Oracle VirtualBox, packet capturing software - The Wireshark Network Analyzer, the attacking machine - Kali Linux, and the victim machines of network attacks – Windows 11, Windows Server 2022, and Windows Server 2025.

In the Oracle VirtualBox virtual environment, 25,000 reverse shell type attacks and 25,000 legitimate packets (10,000 passively collected from real traffic and 15,000 from real production traffic) are simulated. These data are captured using The Wireshark Network Analyzer. The initially collected 50,000 packets are in raw form - .pcap format, then converted to a **csv** file, which is processed by removing unnecessary, non-informative columns (the No column, which reflects the sequence of the packet in the given Wireshark capture, is removed) and an additional column called Label is added, through which the data is labeled. Normal traffic is labeled as "BenignTraffic," while reverse shell type attacks are labeled as "RevShellAttack."

Training scripts are created using a unified pipeline. Their goal is to classify network data (specifically, to differentiate normal traffic from malicious traffic). The training is primarily conducted on two classes: "BenignTraffic" and "RevShellAttack". Initially, a uniform set of features, which are categorical in nature, is extracted from the network packets. In order to participate in the training, these features are transformed into numerical form using Ordinal Encoding, without employing a hierarchical sequence. The numerical values of the input features are scaled using RobustScaler (this applies to the first training out of a total of 5; for the remaining 4 trainings, the scaler is changed). The "RobustScaler" is chosen to limit the influence of extreme values and asymmetric distributions.

From a total of 50,000 packets (N = 50,000) located in 15 network streams, 24,993 sequences of network packets are generated. With a sequence length of 15 packets (L=15) and a sliding window shift step of 2 (S=2), the mathematical definition for generating the number of packet sequences (Nseq) is:

$$N_{seq} = \left[\frac{N-L}{s}\right] + 1 \quad [9], \tag{1}$$

With a total number of packets being 50,000, the number of formed sequences of packets will be:

$$N_{seq} = \left[\frac{50\,000-15}{2}\right] + 1, N_{seq} = 24\,993 \tag{2}$$

With a total number of packets being 50,000, the number of formed sequences of packets will be:The formation of sequences of packets takes place within a given network session (during the creation of the packet sequences, the mixing of data from different network flows is prevented), thereby providing the 1D CNN and BiLSTM inputs with a uniform conceptual structure.

Before the training process begins, certain hyperparameters of the neural networks are configured. They change their values over 5 consecutive trainings. However, after each training, one sniffer script is run for both deep neural networks, and the results of their performance are recorded. When the sniffers are running, attacks of the "revshell" type, DoS type attacks, and specifically TCP Syn flood, UDP flood, and DNS flood (which, if properly identified, are classified as Unknown), as well as legitimate real traffic, are simulated. During the first training, the hyperparameters are set as follows:

1. **batch size** = 128 - the model considers 128 sequences of packets in a specific training batch;

2. **epochs** – 120 - a maximum number of passes through all sequences of packets during training is chosen;
3. **learning rate (lr)** = 0.001 - the initial learning rate of the selected optimizer, automatically set by the keras library;
4. **L1 regularization (Lasso)** - with a set regularization coefficient of 10^{-5}, limiting the overfitting of the specific model;
5. **L2 regularization (Ridge)** - with a set regularization coefficient of 10^{-4}, again limiting overfitting or retraining of the 1D CNN and BiLSTM;
6. **early stopping patience coefficient** = 15 (es), training is stopped if there is no improvement in the neural network's metrics by the 15th epoch;
7. **Learning rate patience coefficient** = 7 and **learning rate factor coefficient** = 0.5 - the learning rate decreases by 50% if no improvement in the neural network's metrics occurs by the seventh epoch;регуляризация от тип "Dropout" – (0.2-0.3) и 0.1 за слой attention;
8. **dropout regularization** - (0.2-0.3) and 0.1 for the attention layer;
9. **AdaDelta optimizer** - the AdaDelta optimizer is chosen, coming from the keras library with an automatically set global parameter "initial learning rate" - 0.001;
10. **Categorical Cross-Entropy loss function** - measures the difference between the actual class distribution and the predicted results for class distribution. When a class is correctly classified with a high probability estimate for that, the loss function is low; when a class is misclassified with a high probability estimate for that, the loss function is again high.

In this experiment, in addition to identical hyperparameter and scaler settings, a similar architecture was constructed. The differences between the two architectures are as follows: the 1D CNN employs convolutional layers—featuring their characteristic dilation—and max-pooling layers, whereas the BiLSTM utilizes LSTM layers, which do not incorporate dilation or max-pooling layers.

The architecture of the one-dimensional convolutional neural network is as follows:

1. **Input layer** – the product of the number of packets in a given sequence - 15 packets and the number of features for each packet;
2. **First convolutional block** – consists of 5 layers – convolutional layer (with 64 filters, dilation 2, and L1, L2 regularizations), normalization layer (batch), activation layer (Mish), Max Pooling layer (with dimensions 2x2 pixels), and Drop-out layer (20% of the neurons are turned off during the current iteration);
3. **Second convolutional block** – again consists of 5 layers – convolutional layer (with 128 filters, dilation 3, and L1, L2 regularizations), normalization layer (batch), activation layer (Mish), Max Pooling layer (with dimensions 2x2 pixels), and Dropout layer (20% of the neurons are turned off during the current iteration);
4. **Third convolutional block** – again consists of 5 layers – convolutional layer (with 256 filters, dilation 4, and L1, L2 regularizations), normalization layer (batch), activation layer (Mish), Max Pooling layer (with dimensions 2x2 pixels), and Dropout layer (20% of the neurons are turned off during the current iteration);

5. **Multi Head Attention block** – consists of 4 layers – attention layer (a mechanism involving 4 parallel heads, each head works with a vector of size 64), output attention layer, normalization layer, and Global Average Pooling layer;
6. **Fully connected block** – consisting of 3 layers – fully connected layer (with 128 filters and applied L1 and L2 regularizations), activation layer (Mish), and Dropout layer (30%);
7. **Softmax output layer** – with two possible outputs: BenignTraffic or RevShellAttack.

Figure 1 presents a diagram of the architecture of the one-dimensional CNN.

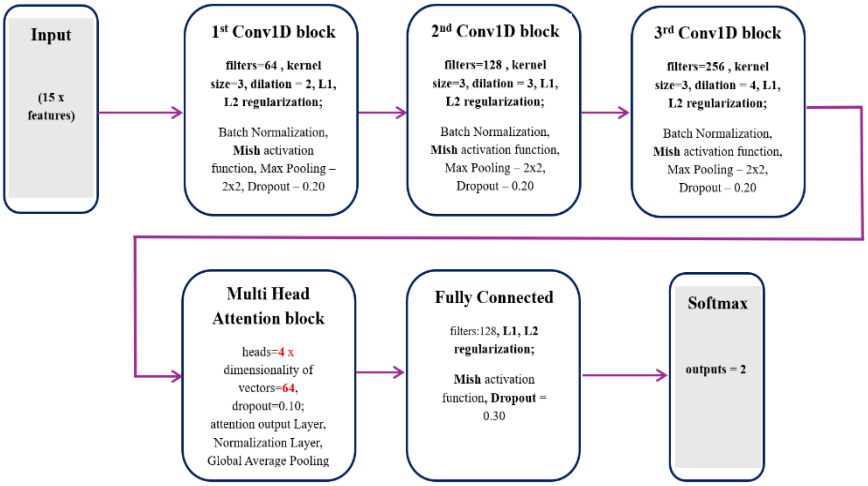


Figure 1: Architecture of 1D CNN with 24 layers.

The architecture of the bidirectional LSTM is similar to the architecture of the one-dimensional CNN (Figure 2).

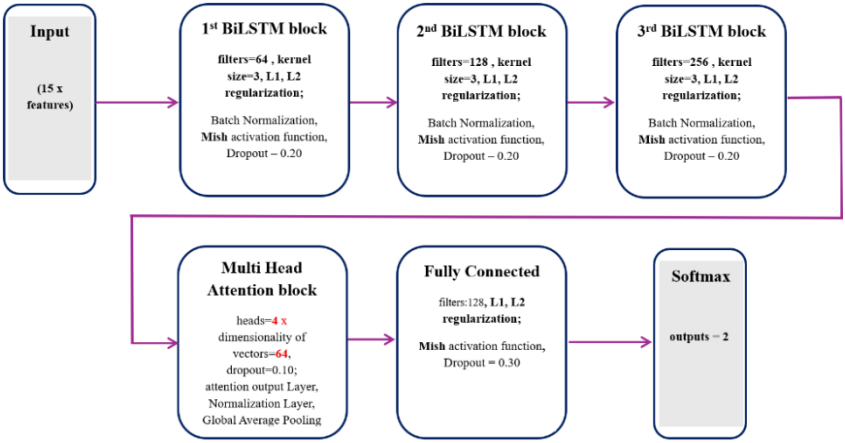


Figure 2: Architecture of Bidirectional LSTM with 21 layers.

Both architectures include a Multi-Head Self-Attention mechanism. Its purpose is to distinguish significant information from less significant information. With the help of the four heads, parallel learning of different dependencies in the batch sequences is carried out. After the training is completed, the models are evaluated using metrics: Overall Accuracy, Weighted Precision, Weighted Recall, Weighted F1-score, confusion matrix, and ROC/AUC analysis. This provides a common basis for comparative analysis of the effectiveness of the two architectures.

2. Results and discussion

To address the current issue, a total of 5 experiments are conducted. Within these 5 trials, some changes are made to the architectural hyperparameters of the One-dimensional Convolutional Neural Network and the architectural hyperparameters of the Bidirectional LSTM, as well as changes to the scaling tools and optimization hyperparameters. Table 1 describes the results of the experiments and the corresponding changes in configurations.

Experiment No. 1 reflects the state of the sniffer scripts of the two trained neural models, based on the initially described hyperparameter configurations and scalers in the text above and in Table 1. In the one-dimensional CNN, out of 1,347 packet sequences, 587 are legitimate packet sequences, with 555 (94.5%) recognized as such. Out of 498 packet sequences of the "RevShell" type, 482 (96.8%) are correctly identified, and 8 (1.6%) are misclassified into the other two classes. From 262 packet sequences of the "Unknown" class, 166 (63.4%) are correctly classified, 65 (24.8%) are incorrectly classified as "BenignTraffic", and 31 (11.8%) are misclassified as "RevShellAttack". In Experiment No. 1 of the two-dimensional LSTM, out of a total of 1,347 packet sequences, 587 are legitimate packet sequences, with 586 (99.8%) recognized as such, and only one packet sequence (0.2%) is incorrectly classified as "Unknown". Out of 498

packet sequences of the "RevShell" type, 492 (98.8%) are recognized as such, 5 (1.0%) are misclassified as "BenignTraffic", and one is misclassified as "Unknown". From 262 packet sequences of the "Unknown" class, 224 (85.5%) are correctly classified into this class, and 19 (7.3%) are misclassified into the other two classes.

For the needs of the second experiment, several changes are made to the parameters used and their values: batch size – 64; maximum number of epochs – 130; learning rate – 1e-4 ($1*10^{-4}$); patience for the learning rate is set to 8; factor coefficient for the learning rate again takes the value of 0.4; the patience coefficient for early stopping is changed to 12; L1 regularization coefficient – 10^{-6}; L2 regularization coefficient – 10^{-5}; dropout regularization in the main layers and before the output layer – (0.3-0.4), dropout regularization in the attention layer – 0.2; the pooling parameter is of size 3x3 (pool size = 3); the optimizer used is "Adam"; the loss function is changed to "Categorical Focal Cross-Entropy"; the scaler becomes "StandardScaler"; the dilation for the three convolutional layers takes values of 1, 2, and 3. For the one-dimensional CNN, it turns out that this is the best combination of selected parameters and settings made, as the sniffer script shows that out of 4050 captured network sequences of data, all are recognized correctly at 100% (figure 4 and figure 5). In the Bidirectional LSTM, based on the confusion matrix (figure 3), it is seen that the data collected with the sniffer totals 4084. The first row in the confusion matrix describes the legitimate network packet sequences, which are a total of 2000 and are recognized correctly at 100%. The second row contains the packet sequences of the "ReverseShell" type, which total 600, with 525 (87.5%) being correctly classified, while 75 are misclassified, of which 54 (9%) are incorrectly assigned to the legitimate class, and 21 (3.5%) are misclassified to the "Unknown" class. The third row describes the "Unknown" class with a total of 1484 packet sequences, with 1442 (97.2%) of them being correctly classified into the "Unknown" class and 42 (2.85%) being misclassified into the normal traffic class.

In the third experiment, the following configurations are made: batch size – 32; maximum number of epochs – 110; learning rate – 1e-5 ($1*10^{-5}$); patience for the learning rate is set to 9; factor coefficient for the learning rate again takes the value of 0.6; the patience coefficient for early stopping is changed to 10; L1 regularization coefficient – 10^{-7}; L2 regularization coefficient – 10^{-6}; dropout regularization in the main layers and before the output layer – (0.15-0.25), dropout regularization in the attention layer – 0.10; the pooling parameter is of size 2x2 (pool size = 2); the optimizer used is "Stochastic Gradient Descent" (SGD); the loss function is changed to "Root Mean Squared Error" (RMSE); the scaler becomes "MaxAbsScaler"; the dilation in the three convolutional layers retains values of 1, 2, and 3, respectively.

During the sniffing of the 1D CNN, 6795 packet sequences are captured, of which 1245 are legitimate, 2627 are reverse shell attacks, and 2923 are TCP Syn flood, UDP flood, and DNS flood. From the results matrix, it is established that 1245 packet sequences from legitimate packets are recognized correctly at 100%. Reverse shell attacks are recognized correctly at 96% or 2523 packet sequences, with 38 (1.4%) being incorrectly recognized as legitimate and 66 (2.5%) being misclassified to the "Unknown" class. The DoS attacks classified into the unknown class total 2866 (98%), with 15 (0.5%) packet sequences being misclassified into the "BenignTraffic" class and 42

(1.4%) being misclassified into the reverse shell attacks class. During the sniffing of the BiLSTM, 6836 packet sequences are intercepted, of which 1302 are data from normal traffic, 2641 are reverse shell attacks, and 2893 are DoS attacks (again TCP Syn flood, UDP flood, and DNS flood). Referring to the confusion matrix, it is seen that 1302 packet sequences from legitimate data are correctly recognized. Reverse shell attacks reach 2358 correctly recognized data or 89.3% accuracy of the results, with 35 (1.3%) packet sequences being misclassified into normal traffic and 248 (9.4%) being misclassified into the "Unknown" class. The distribution of DoS attacks by class is as follows: 2854 (98.7%) packet sequences correctly classified into the "Unknown" class, 18 (0.6%) packet sequences incorrectly classified into the legitimate data class, and 21 (0.7%) packet sequences misclassified into the reverse shell attacks class.

In the fourth experiment, the following settings are made: batch size – 16; maximum number of epochs – 140; learning rate – 1e-6 ($1*10^{-6}$); patience for learning rate is set to 10; factor coefficient for learning rate is again set to 0.7; patience coefficient for early stopping is changed to 20; L1 regularization coefficient – 10^{-4}; L2 regularization coefficient – 10^{-3}; dropout regularization in the main layers and before the output layer – (0.22-0.25), dropout regularization in the attention layer – 0.15; the pooling parameter is of size 2x2 (pool size = 2); the optimizer used is "Root Mean Squared Propagation" (RMSprop); the loss function is changed to "Log-Cosh Loss"; the scaler becomes "MinMaxScaler"; the dilation in the three convolutional layers is valued at 1, 2, and 2 respectively.

When sniffing with the 1D CNN, 8654 packet sequences were captured, of which 2024 are legitimate, 597 are "Reverse Shell" attacks, and 6033 are TCP Syn flood, UDP flood, and DNS flood. From the confusion matrix, it can be seen that 2024 packet sequences of legitimate data are correctly recognized. Of the 597 "Reverse Shell" attacks, 540 (90.5%) are correctly identified as such, and 57 (9.5%) are misclassified into the "Unknown" class. The distribution of DoS attacks by class is as follows: 5902 (97.8%) packet sequences correctly classified into the "Unknown" class, 115 (1.9%) packet sequences misclassified into the legitimate data class, and 16 (0.3%) packet sequences misclassified into the "Reverse Shell" attack class. When sniffing with BiLSTM, 8798 packet sequences were intercepted, of which 2427 are normal traffic data, 3281 are "Reverse Shell" attacks, and 3090 are DoS attacks. From the confusion matrix (Figure 6), it is established that all 100% of the 2427 packet sequences of legitimate data are correctly classified. The correctly recognized "Reverse Shell" attack sequences are 3150 (96%), while the misclassified ones are 131 packet sequences, with 61 (1.9%) being incorrectly classified into the "BenignTraffic" class and 70 (2.1%) being incorrectly classified into the "Unknown" class. The distribution of DoS attacks by class is as follows: 3012 (97.5%) packet sequences correctly classified into the "Unknown" class, 50 (1.6%) packet sequences misclassified into the legitimate data class, and 28 (0.9%) packet sequences misclassified into the "Reverse Shell" attack class.

In the fifth experiment, the following settings are made: batch size – 256; maximum number of epochs – 100; learning rate – 1e-7 ($1*10^{-7}$); patience for learning rate is set to 11; factor coefficient for learning rate is again set to 0.3; patience coefficient for early stopping is changed to 17; L1 regularization coefficient – 10^{-3}; L2 regularization

coefficient – 10^{-2}; dropout regularization in the main layers and before the output layer – (0.35-0.45), dropout regularization in the attention layer – 0.30; the pooling parameter is of size 3x3 (pool size = 3); the optimizer used is Adagrad; the loss function is changed to Kullback-Leibler Divergence; the scaler becomes Normalizer; the dilation in the three convolutional layers is valued at 2, 1, and 3 respectively.

When sniffing with the 1D CNN, 11278 packet sequences were captured, of which 3529 are legitimate, 4257 are "Reverse Shell" attacks, and 3492 are TCP Syn flood, UDP flood, and DNS flood. The result matrix shows that in the first row, recognizability is weak. The correctly recognized legitimate packet sequences are 131, or only 3.7%, while the authorized data misclassified into the "Reverse Shell" class are 2960 (83.9%), and the authorized data misclassified into the "Unknown" class are 438 (12.4%). In the second row, the recognized packet "Reverse Shell" sequences are 3644 (85.6%), and the misclassified into the other two classes are respectively: in the "Benign" class – 300 (7%), in the "Unknown" class – 313 (7.4%). In the third row of the matrix, the correctly classified DoS attacks are 452 (12.9%), while the misclassified ones are 3040, of which 640 (18.3%) incorrectly belong to the legitimate class and 2400 (68.7%) incorrectly belong to the "Reverse Shell" class. When sniffing with Bidirectional LSTM, 11410 packet sequences were intercepted, of which 3543 are legitimate, 4356 are "Reverse Shell" attacks, and 3511 are TCP Syn flood, UDP flood, and DNS flood. The confusion matrix shows that in the first row, the correctly recognized legitimate packet sequences are 656 (18.5%), and the misclassified ones are 2887, of which the misclassified into the "Reverse Shell" class are 2800 (79%), and the misclassified into the "Unknown" class are 87 (2.5%). In the second row of the confusion matrix, the recognized packet "Reverse Shell" sequences are 2623 (60.2%), and the misclassified into the other two classes are respectively 1733: in the "Benign" class – 991 (22.8%), in the "Unknown" class – 742 (17%). In the third row of the confusion matrix, the correctly classified DOS attacks are 666 (19%), while the incorrectly classified ones are 2845, of which 400 (11.4%) incorrectly belong to the legitimate class and 2445 (69.6%) incorrectly belong to the "Reverse Shell" class.

Graphs of the best results from the sniffers of 1D CNN and BiLSTM are presented in Figures 3-8.

Figure 3 shows an ideal result, represented by a confusion matrix, obtained during the sniffing of the one-dimensional CNN. Figure 4 demonstrates an ideal case in which all the metrics used have a value of 1. Figure 5 shows the area under the curve (AUC) of the 1D CNN for the three main classes, indicating that the sniffer distinguishes between them with 100% accuracy. Figure 6 presents the best result obtained from BiLSTM sniffing, shown via a confusion matrix. Figure 7 demonstrates good results for the overall accuracy of the BiLSTM sniffer - 0.9762, as well as the other weighted metrics. Figure 8 shows the Area Under the Curve (AUC) for the Bidirectional LSTM across the three main classes; the AUC for the legitimate class is 0.9913, the AUC for the Revshell class is 0.9775, and the AUC for the "Unknown" class is 0.9812.

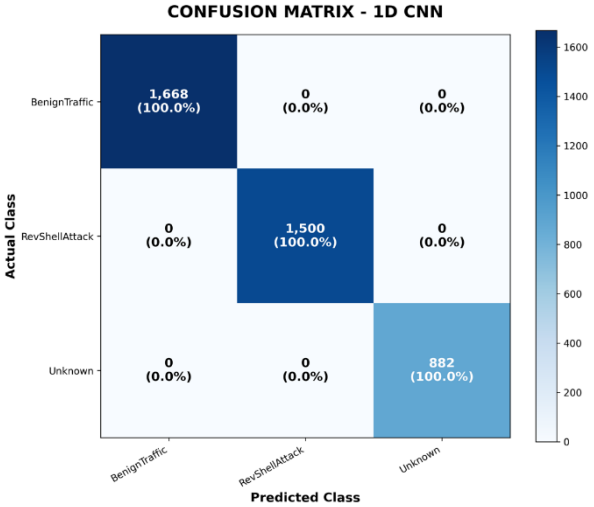


Figure 3: Confusion matrix for the 1D CNN sniffer – Experiment No. 2.

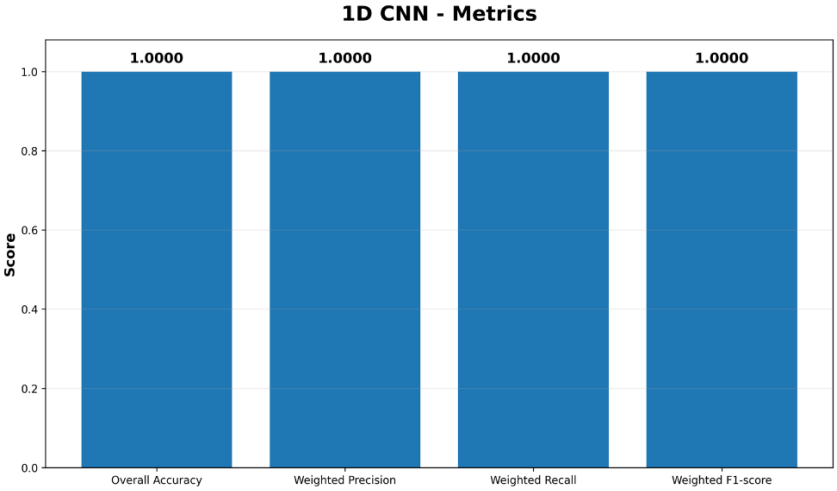


Figure 4: Evaluation of results presented via metrics: overall accuracy, weighted precision, weighted recall, weighted F1-score – Experiment No. 2.

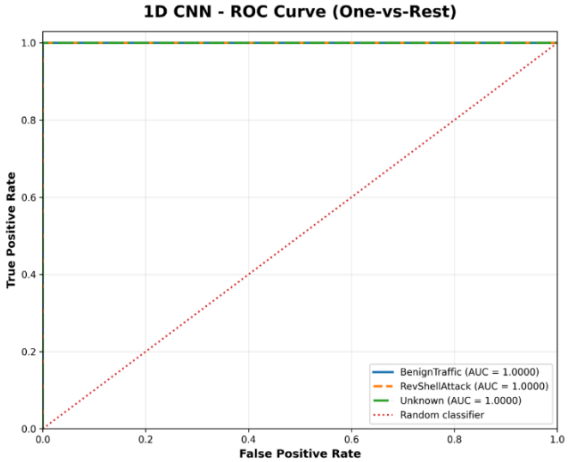


Figure 5: ROC curve evaluation of the three main classes, based on a "one-vs-rest" approach – results from the 1D CNN sniffer – Experiment No. 2.

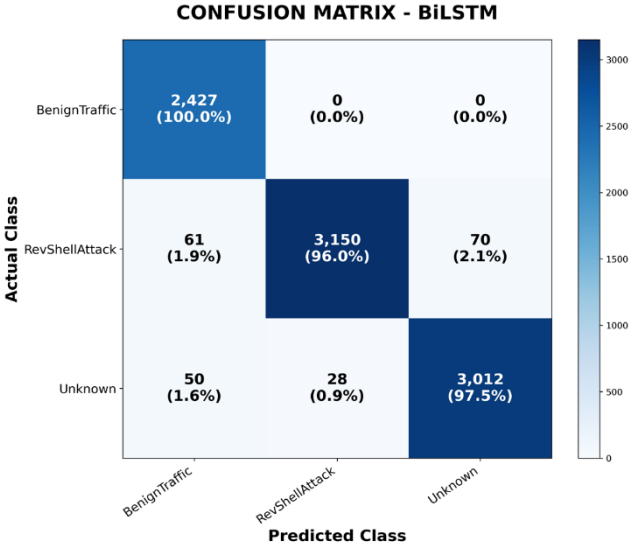


Figure 6: Confusion matrix obtained after the completion of the Bidirectional LSTM sniffer's operation – Experiment No. 4.

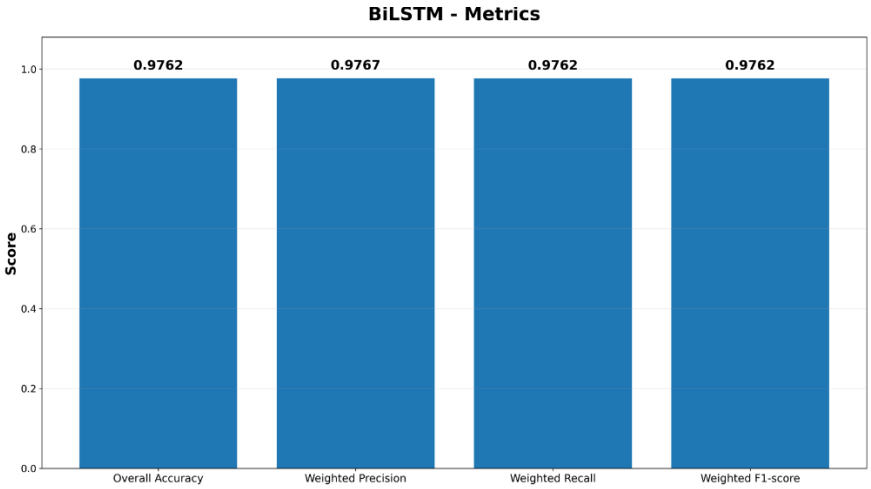


Figure 7: Evaluation of the BiLSTM sniffer results, presented via metrics: overall accuracy, weighted precision, weighted recall, and weighted F1-score – Experiment No. 4.

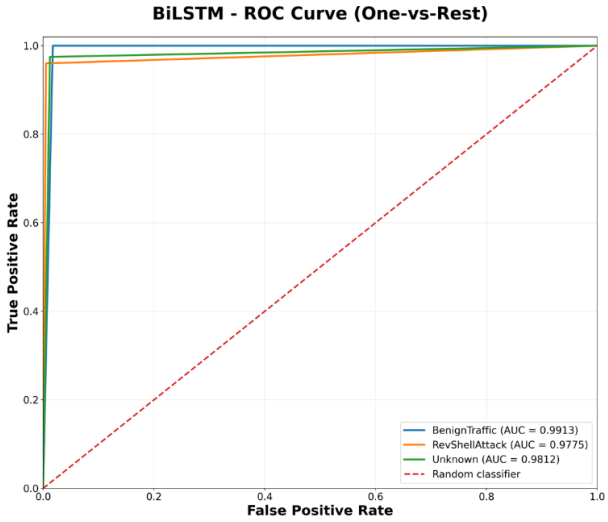


Figure 8: ROC curve evaluation of the three main classes, based on a "one-vs-rest" approach – result from the Bidirectional LSTM sniffer – Experiment No. 4

Table 1. Results of tests conducted on 1D CNN and BiLSTM models, involving adjustments to selected hyperparameters and network data scaling mechanisms.

One-dimentional Convolution Neural Network											
	batch size and epochs	Lr and patience, factor for lr	L1, L2 reg., patience for **es**	dropout reg., pool size	*optimizer* and loss function	Scaler, **dilation**	overall accuracy	weighted precision	weighted recall	weighted f1-score	AUC
Experiment №1	128, 120	0.01, 7, 0.5	Both 10^{-5}, 10^{-4}, **15**	(0.2-0.3), attention 0.1, 2	*AdaDelta*, Categorical Cross-Entropy	Robust, **2,3,4**	0.8931	0.8893	0.8931	0.8886	0.8614
Experiment №2	64, 130	0.0001, 8, 0.4	Both 10^{-6}, 10^{-5}, **12**	(0.3-0.4), attention 0.2, 3	*Adam*, Focal Loss	Standard Scaler, **1,2,3**	1.000	1.000	1.000	1.000	1.000
Experiment №3	32, 110	10^{-5}, 9, 0.6	Both 10^{-7}, 10^{-6}, **10**	(0.15-0.25), attention 0.1, 2	*SGD*, RMSE Loss	MaxAbs Scaler, **1,2,3**	0.9763	0.9765	0.9763	0.9763	0.9817
Experiment №4	16, 140	10^{-6}, 10, 0.7	Both 10^{-4}, 10^{-3}, **20**	(0.22-0.25), attention 0.15, 2	*RMSprop*, Log-Cosh Loss	MinMaxScaler, **1,2,2**	0.9783	0.9788	0.9783	0.9779	1.000
Experiment №5	256, 100	10^{-7}, 11, 0.3	Both 10^{-3}, 10^{-2}, **17**	(0.35-0.45), attention 0.3, 3	*Adagrad*, Kullback-Leibler Divergence	Normalizer, **2,1,3**	0.3748	0.3074	0.3748	0.2849	0.4568
Bidirectional Long Short-Term Memory											
	batch size and epochs	Lr and patience, factor for lr	L1, L2 reg., patience for **es**	dropout reg., ~~pool size~~	*optimizer* and loss function	Scaler, ~~**dilation**~~	overall accuracy	weighted precision	weighted recall	weighted f1-score	AUC
Experiment №1	128, 120	0.01, 7, 0.5	Both 10^{-5}, 10^{-4}, **15**	(0.2-0.3), attention 0.1	*AdaDelta*, Categorical Cross-Entropy	Robust	0.9666	0.9674	0.9666	0.9658	0.9823
Experiment №2	64, 130	0.0001	Both 10^{-6}, 10^{-5}, **12**	(0.3-0.4), attention 0.2	*Adam*, Focal Loss	Standard Scaler	0.9714	0.9724	0.9714	0.9710	0.9729
Experiment №3	32, 110	10^{-5}, 9, 0.6	Both 10^{-7}, 10^{-6}, **10**	(0.15-0.25), attention 0.1	*SGD*, RMSE	Max Abs Scaler	0.9529	0.9553	0.9529	0.9525	0.9613

Experiment №4	16, 140	10^{-6}, 10, 0.7	Both 10^{-4}, 10^{-3}, **20**	(0.22-0.25), attention 0.15	*RMSprop*, Log-Cosh Loss	MinMaxScaler	0.9762	0.9767	0.9762	0.9762	0.9826
Experiment №5	256, 100	10^{-7}, 11, 0.3	Both 10^{-3}, 10^{-2}, **17**	(0.35-0.45), attention 0.3	*Adagrad*, Kullback-Leibler Divergence	Normalizer	0.3457	0.3639	0.3457	0.3186	0.4873

Table 1 and Figures 3–8 show that the best results were achieved in Experiment 2 for the 1D CNN and in Experiment 4 for the BiLSTM. The overall accuracy for the 1D CNN reaches the maximum possible value of 1, while the overall accuracy for the BiLSTM reaches 0.9762.

Conclusion

The results of the second experiment with the 1D CNN sniffer and the fourth experiment with the bidirectional LSTM show good effectiveness and performance for both models, whereas the fifth experiments demonstrate the exact opposite.

In the second experiment, the ideal result for the 1D CNN (100% accuracy) was achieved using the following configuration: optimizer – "Adam"; scaling module – "StandardScaler"; loss function – "Categorical Focal Cross-Entropy"; batch size – 64; total number of epochs – 130; learning rate – 0.0001; learning rate "patience" – 8; learning rate "factor" – 0.4; L1 regularization value – 10^{-6}; L2 regularization value – 10^{-5}; early stopping "patience" – 12; dropout regularization in main layers – 30%; dropout regularization before the final output layer – 40%; dropout regularization in the attention layer – 20%; pool size – 3; dilation in the three convolutional layers – 1, 2, 3. In the fourth experiment, the best result for BiLSTM (97.62% overall accuracy) was achieved using the following configuration: optimizer – RMSprop; scaler – MinMaxScaler; loss function – Log-CoshLoss; batch size – 16; total epochs – 140; learning rate – 10^{-6}; learning rate "patience" – 10; learning rate "factor" – 0.7; L1 regularization – 10^{-4}; L2 regularization – 10^{-3}; early stopping "patience" – 20; dropout regularization in main layers – 22%; dropout regularization before the final output layer – 25%; and dropout regularization in the attention layer – 15%. The lowest results—representing the least suitable combination of parameters and settings for both deep neural network models—were recorded in the fifth experiments. The overall accuracy for the one-dimensional CNN is 0.3748 (37.48%), while the overall accuracy for the bidirectional LSTM is 0.3457 (34.57%). The following configurations were used for Experiment 5: optimizer – "Adagrad"; scaling module – "Normalizer"; loss function – "Kullback-Leibler Divergence"; batch size – 256; total number of epochs – 100; learning rate – 10^{-7}; learning rate "patience" – 11; learning rate "factor" – 0.3; L1 regularization value – 10^{-3}; L2 regularization value – 10^{-2}; early stopping "patience" – 17; dropout regularization in the main layers – 35%; dropout regularization before the final output layer – 45%; dropout regularization in the attention layer – 30%; pool size – 3; dilation in the three convolutional layers – 2, 1, 3 (pool size and dilation apply only to the 1D CNN).

Selecting suitable configurations, appropriately scaling input data, and correctly choosing optimization and architectural hyperparameters are fundamental to building an effective network anomaly detection system.

References

1. Alashjaee, A.M. Deep learning for network security: an Attention-CNN-LSTM model for accurate intrusion detection. Sci Rep 15, 21856 (2025). https://doi.org/10.1038/s41598-025-07706-y.
2. Alsubaei, F.S. Smart deep learning model for enhanced IoT intrusion detection. Sci Rep 15, 20577 (2025). https://doi.org/10.1038/s41598-025-06363-5
3. Farhan, M., Waheed ud din, H., Ullah, S. et al. Network-based intrusion detection using deep learning technique. Sci Rep 15, 25550 (2025). https://doi.org/10.1038/s41598-025-08770-0.
4. Iturbe-Araya, J. I., & Rifa-Pous, H. Hyperparameter optimization and evaluation metrics for unsupervised anomaly-based cyberattack detection in imbalanced smart home datasets. Journal of Network and Systems Management, 33, Article 99 (2025). https://doi.org/10.1007/s10922-025-09973-6
5. Neto, E.C.P., Iqbal, S., Buffett, S. et al. Deep learning for intrusion detection in emerging technologies: a comprehensive survey and new perspectives. Artificial Intelligence Review, 58, 340 (2025). https://doi.org/10.1007/s10462-025-11346-z
6. Ruffo, V. G. da S., Lent, D. M. B., Komarchesqui, M., Schiavon, V. F., de Assis, M. V. O., Carvalho, L. F., & Proenca Jr., M. L. Anomaly and intrusion detection using deep learning for software-defined networks: A survey. Expert Systems with Applications, 256, 124982 (2024). https://doi.org/10.1016/j.eswa.2024.124982
7. Scikit-learn developers. (n.d.). Normalizer. Retrieved from: https://scikit-learn.org/stable/modules/generated/sklearn.preprocessing.Normalizer.html#sklearn.preprocessing.Normalizer. [Accessed: 2026-10-02].
8. Scikit-learn developers. (n.d.). sklearn.preprocessing — scikit-learn documentation. Scikit-learn. Retrieved from: https://scikit-learn.org/stable/api/sklearn.preprocessing.html. [Accessed: 2026-09-30].
9. XU, K., WANG, H., LI, Ch., LIU, H., XING, Ch. A CPU–NPU Heterogeneous Edge Fault Diagnosis Framework for Industrial Sensor Data. Sensors [online]. 2026, Vol. 26, No. 16, 5125. ISSN 1424-8220. DOI: https://doi.org/10.3390/s26165125.
10. Wang, Q., Jiang, H., Ren, J., Liu, H., Wang, X., & Zhang, B. An intrusion detection algorithm based on joint symmetric uncertainty and hyperparameter optimized fusion neural network. Expert Systems with Applications, 244, 123014 (2024). https://doi.org/10.1016/j.eswa.2023.123014.
11. Zhang, Y., Muniyandi, R. C., & Qamar, F. A Review of Deep Learning Applications in Intrusion Detection Systems: Overcoming Challenges in Spatiotemporal Feature Extraction and Data Imbalance. Applied Sciences, 15(3), 1552 (2025). https://doi.org/10.3390/app15031552.

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

ARTIFICIAL INTELLIGENCE-BASED FACIAL RECOGNITION SYSTEM FOR DIGITAL IMAGES

Emil T. Ivanov

Ministry of Defence, Bulgarian Defence Institute, Sofiq, Bulgaria, emotsiv@gmail.com
ORCID: #0000-0003-1658-9588

***Abstract**: Biometric technologies are increasingly used in identification, access control, information security and automated image-processing systems. Among them, facial recognition provides the ability to extract and compare distinctive facial characteristics without direct physical contact. This paper presents a conceptual model, an algorithm and a prototype implementation of a system for recognizing pre-registered individuals in digital images through artificial intelligence methods. The identity decision is made using the minimum Euclidean distance and a predefined similarity threshold. The algorithm is implemented in Python using the face_recognition, dlib, OpenCV and NumPy libraries.*

***Keywords:** artificial intelligence, biometric data, face recognition, digital images, deep learning, Python, information security*

СИСТЕМА ЗА РАЗПОЗНАВАНЕ НА ЛИЦА ОТ ЦИФРОВИ ИЗОБРАЖЕНИЯ ЧРЕЗ МЕТОДИ НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ

Емил Ц. Иванов

Министерство на отбраната, Институт по отбрана, София, България, emotsiv@gmail.com
ORCID: #0000-0003-1658-9588

***Резюме**: Биометричните технологии намират все по-широко приложение в системите за идентификация, контрол на достъпа, информационна сигурност и автоматизирано обработване на изображения. Сред тях разпознаването на лица се отличава с възможността за безконтактно извличане и сравняване на характерни признаци на човешкото лице. Настоящата статия представя концептуален модел, алгоритъм и прототипна реализация на система за разпознаване на предварително регистрирани лица в цифрови изображения чрез методи на изкуствения интелект.Решението за идентичност се взема въз основа на минималното Евклидово разстояние и предварително зададен праг на сходство. Алгоритъмът е реализиран на езика Python чрез библиотеките face_recognition, dlib, OpenCV и NumPy.*

***Ключови думи:** изкуствен интелект, биометрични данни, разпознаване на лица, цифрови изображения, дълбоко обучение, Python, информационна сигурност*

Въведение

Бързото развитие на изкуствения интелект и компютърното зрение създава възможности за автоматизирано извличане на информация от цифрови изображения и видеопотоци. Едно от най-разпространените направления в тази

област е автоматичното откриване и разпознаване на човешки лица. Човешкото лице съдържа множество сравнително постоянни характеристики, свързани с геометрията и пространственото разположение на очите, носа, устата, скулите и контура на лицето. Тези признаци могат да бъдат преобразувани в математическо представяне и използвани за сравнение между различни изображения [1], [2].

Разпознаването на лице обаче не следва да се разглежда като единична операция. То представлява последователност от взаимосвързани процеси, включващи - въвеждане на цифровото изображение, откриване на лице или лица, локализиране на основни лицеви ориентири, геометрично подравняване на лицето, извличане на биометрични характеристики, сравняване с предварително регистрирани образци, разпознаване и представяне на резултата [1], [2].

Разграничението между откриване и разпознаване е особено важно. Откриването на лице, или face detection, определя дали в изображението присъства лице и къде се намира то. Разпознаването на лице, или face recognition, има за цел да определи дали откритото лице съответства на конкретно лице, регистрирано в системата.

Прилагането на подобна технология е свързано и с редица ограничения. Точността може да бъде повлияна от осветлението, резолюцията, положението на главата, изражението, възрастови промени, частично закриване на лицето и качеството на регистрационните изображения. Независимите оценки на NIST използват показатели като False Match Rate, False Non-Match Rate, False Positive Identification Rate и False Negative Identification Rate [3], [4], което показва необходимостта биометричните системи да бъдат оценявани не само чрез обща точност, а и чрез вероятността за неправилно приемане или отхвърляне.

Допълнителен съществен въпрос е защитата на обработваните данни. Съгласно Общия регламент (ЕС) 2016/679 относно защитата на данните, биометричните данни, използвани за уникално идентифициране на физическо лице, попадат в специална категория лични данни и тяхното обработване подлежи на засилени правни и организационни изисквания [5].

Настоящата разработка е насочена към създаване на ограничен изследователски прототип, който обработва предварително подбрани изображения на доброволно участващи лица в контролирана среда. Системата не е предназначена за скрито наблюдение, масова идентификация или вземане на автоматизирани решения с правни или други значими последици за засегнатите лица.

Цел и задачи на изследването

Целта на настоящото изследване е да се разработи и опише прототипна система за автоматизирано разпознаване на предварително регистрирани лица в цифрови изображения чрез методи на изкуствения интелект.

Системата трябва да осигурява:

- регистриране на известни лица чрез примерни изображения;
- автоматично откриване на лица във входна снимка;
- преобразуване на всяко открито лице в биометричен вектор;

- сравняване с векторите на известните лица;
- определяне на най-вероятното съвпадение;
- класифициране на лицето като известно или неизвестно;
- визуализиране и записване на резултатите.

За постигане на поставената цел са определени **следните задачи**:

- Да бъдат анализирани основните етапи на автоматизираното разпознаване на лица;
- Да бъде предложена модулна архитектура на прототипната система;
- Да бъде разработен алгоритъм за регистриране и разпознаване на лица;
- Да бъде формулиран математически модел за сравняване на лицевите вектори;
- Да бъде реализиран алгоритъмът на езика Python;
- Да бъдат предвидени механизми за обработване на изображения без лице, с повече от едно лице или с недостатъчно качество;
- Да бъде разработена методика за експериментално оценяване;
- Да бъдат анализирани технологичните, етичните и правните ограничения.

Обект на изследването е процесът на автоматизирано биометрично разпознаване на човешки лица в цифрови изображения.

Предмет на изследването са моделите, методите и алгоритмите за откриване, кодиране и сравняване на лицеви изображения чрез средства на изкуствения интелект.

Теоретични основи на лицевото разпознаване

Биометрична идентификация

Биометричната идентификация използва измерими физиологични или поведенчески характеристики за установяване или проверяване на идентичността на дадено лице. Физиологичните характеристики могат да включват лице, пръстови отпечатъци, ирис, ретина или геометрия на ръката, докато поведенческите могат да включват глас, почерк, походка или начин на взаимодействие с информационна система [6].

При системите за разпознаване на лица основният биометричен източник е цифровото изображение на лицето. То не се сравнява задължително директно на ниво пиксели. Вместо това изображението се обработва от специализиран модел, който извлича характерно числово представяне [1], [2].

Биометричната система може да изпълнява две основни задачи:

Верификация „едно към едно"

При верификацията се проверява дали представеното лице съответства на предварително заявена идентичност.

Примерен въпрос е: „Това лице принадлежи ли на лицето с идентификатор X?"

Сравнението се извършва между един входен биометричен образец и един регистриран шаблон [3].

Идентификация „едно към много"

При идентификацията входното лице се сравнява с множество регистрирани лица [4]. Примерен въпрос е: „Кое от лицата в базата данни съответства на това

изображение?". Разработената в настоящата статия система реализира опростен вариант на идентификация „едно към много", при която се търси най-близкият биометричен шаблон.

Откриване на лица

Преди да бъде разпознато, лицето трябва да бъде локализирано в изображението. Резултатът от този процес обикновено се представя чрез правоъгълна област с координати:

$$B = (x_{min}, y_{min}, x_{max}, y_{max}) \quad (1)$$

където:

- x_{min} и y_{min} определят горния ляв ъгъл;
- x_{max} и y_{max} определят долния десен ъгъл.

В зависимост от използвания модел откриването може да бъде реализирано чрез:

- Haar каскади [8];
- Histogram of Oriented Gradients;
- Support Vector Machines;
- Convolutional Neural Networks;
- Multi-Task Cascaded Convolutional Networks;
- специализирани детектори от типа Single Shot Detector.

В прототипа се използва HOG-базиран детектор от библиотеката dlib в Python. Този вариант е подходящ за експерименти върху стандартен централен процесор и изображения, в които лицата са относително фронтално разположени. При наличие на графичен ускорител може да бъде използван CNN-базиран детектор, който обичайно е по-устойчив при по-сложни условия, но изисква повече изчислителни ресурси [1], [7].

Лицеви ориентири и подравняване

След откриването на лицето е необходимо да бъдат определени характерни точки, наричани лицеви ориентири. Те могат да описват положението на очите, веждите, носа, устните, челюстта, контура на лицето.

Чрез тези точки изображението може да бъде подравнено така, че очите, носът и устата да заемат приблизително сходни позиции независимо от ограничено завъртане или наклон на главата. Подравняването намалява вариациите, които не са свързани със самоличността, и подобрява последващото сравняване [1].

Официалните примери на dlib използват детектор, модел за лицеви ориентири и невронен модел за създаване на 128-мерен лицев дескриптор [1], [2].

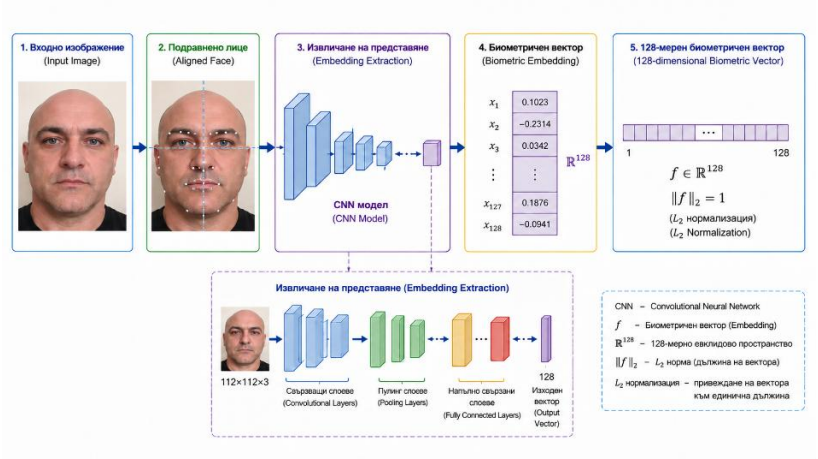
Извличане на характеристики

След подравняването лицето се подава към невронен модел, който генерира векторно представяне:

$$x = [x_1, x_2, \dots, x_{128}]^T \quad (2)$$

Полученият вектор се нарича лицева кодировка, лицев дескриптор, embedding или биометричен шаблон [1], [2].

Процесът на преобразуване на лицевото изображение в 128-мерен биометричен вектор е представен на фиг. 1. След геометричното подравняване лицето се обработва от невронен модел, който извлича отличителните характеристики и формира компактно векторно представяне (embedding), използвано при последващото сравняване на биометричните шаблони.



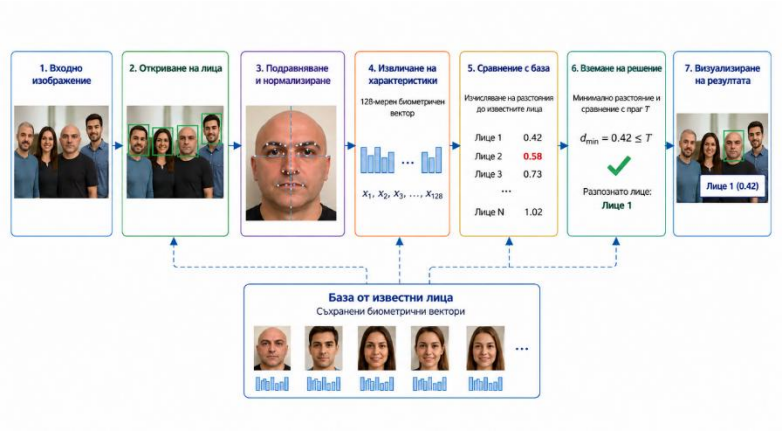
Фигура 7: Процес на извличане на 128-мерен биометричен вектор на лицево изображение

Основната идея на дълбокото метрично обучение е изображенията на едно и също лице да бъдат разположени близо едно до друго във векторното пространство, а изображенията на различни лица - на по-голямо разстояние [2]. Официалната документация на dlib описва преобразуването на всяко лице в 128-мерен дескриптор и използването на разстоянието между дескрипторите за сравнение [1], [2]. Това означава, че системата не извършва сравняване единствено по цвят на очите, форма на носа или отделен геометричен параметър. Невронният модел създава комплексно представяне, получено от съчетанието на множество визуални зависимости.

Концептуален модел и архитектура на системата

Концептуална последователност

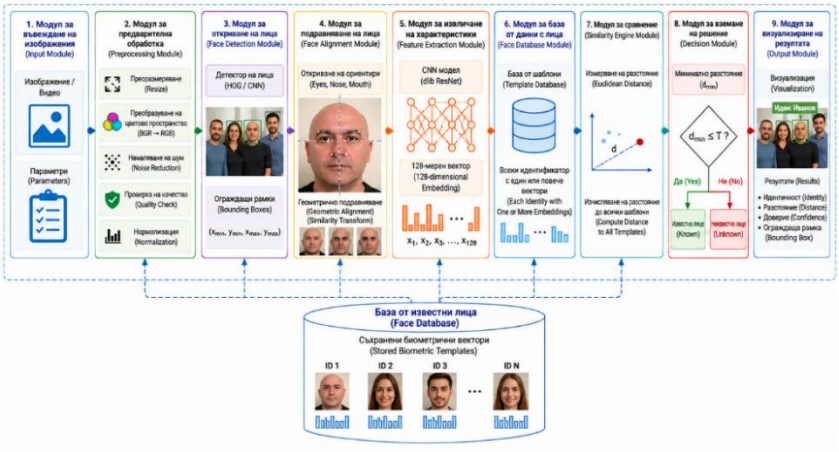
Общият процес на функциониране на системата може да бъде представен чрез последователността, представена на фиг. 2.



Фигура 8: Концептуална схема на система за разпознаване на лица

Функционални модули

Функционалната архитектура на разработената система е представена на фиг. 3. Тя се състои от девет основни взаимосвързани модула, които реализират последователно процесите по предварителна обработка, откриване на лица, извличане на биометрични характеристики, сравняване с базата от известни лица и вземане на решение за идентификация. Подробното описание на всеки модул е представено в следващите подраздели.



Фигура 9: Функционална архитектура на модулите на системата за разпознаване на лица.

В модула за предварителна обработка OpenCV зарежда стандартно цветните изображения в BGR формат, докато използваните функции за лицево разпознаване очакват RGB представяне. Поради това се извършва преобразуване

$$I_{RGB} = C(I_{BGR}) \tag{3}$$

където (C) е операцията за преобразуване на цветовото пространство.

Модулът за откриване на лица локализира всички лица и връща координатите им. Ако не бъде открито лице, изображението се отхвърля или се маркира за допълнителна проверка.

След откриването на лицето е необходимо неговото геометрично подравняване. Модулът за подравняване на лицето използва предварително определени лицеви ориентири (Facial Landmarks), като например позициите на очите, носа и устата, за да изчисли необходимата геометрична трансформация.

Математически процесът може да бъде представен чрез функцията

$$I_{aligned} = T(I_{face}) \tag{4}$$

където:

- I_{face} е откритата лицева област;
- $T(\cdot)$ е геометричната трансформация, включваща завъртане, мащабиране и транслация;
- $I_{aligned}$ е подравненото изображение, използвано за извличане на биометричния вектор.

За всяко открито лице се създава 128-мерен вектор. Този вектор представлява биометричния шаблон, използван при последващото сравняване [1], [2].

Следващата стъпка е създаването на базата от известни лица. В прототипа базата е реализирана като два свързани списъка:

$$E = \{e_1, e_2, \dots, e_N\}$$
$$L = \{l_1, l_2, \dots, l_N\} \tag{5}$$

където:

- e_i е кодировката на (i)-тото лице;
- l_i е съответното име или идентификатор;
- (N) е броят на регистрираните образци.

Следващият етап е изчисляване на разстоянието между неизвестния вектор и всички регистрирани вектори в модула за сравнение. Намира се най-близкият регистриран образец. Ако разстоянието е под определения праг, системата приема съвпадение. В противен случай лицето се класифицира като неизвестно от модула за вземане на решение.

В последния етап се представят резултатите. Върху изображението се изчертават – правоъгълник около лицето, име или текст „Неизвестно лице“, изчисленото разстояние, като се прави различно визуално представяне за известно или неизвестно лице.

Математически модел

Представяне на лицето

Нека входното лицево изображение е (I). След откриване, подравняване и обработване чрез модела за извличане на характеристики се получава функцията:

$$f : X \overset{\square}{\rightarrow} R^{128} \tag{6}$$

Следователно:

$$x = f(I) \tag{7}$$

където:

$$x = \{x_1, x_2, \dots, x_{128}\} \tag{8}$$

е биометричният вектор на входното лице.

За всяко известно лице в базата е наличен поне един предварително изчислен вектор:

$$y_i = \{y_{i1}, y_{i2}, \dots, y_{i128}\} \tag{9}$$

Евклидово разстояние

Сходството между два лицеви вектора се определя чрез Евклидово разстояние [2]:

$$d(x, y_j) = \sqrt{\sum_{j=1}^{128} (x_j - y_{ij})^2} \tag{10}$$

По-малката стойност на (d) означава по-висока степен на сходство. Разстоянията до всички известни образци образуват множеството:

$$D = \{d(x, y_1), d(x, y_2), \dots, d(x, y_N)\} \tag{11}$$

Определяне на най-близкия образец

Най-близкият образец се определя чрез:

$$i^* = \underset{i \in \{1,\dots,N\}}{\arg\min}\, d(x, y_{i^*}) \tag{12}$$

Минималното разстояние е:

$$d_{min} = d(x, y_{i^*}) \tag{13}$$

Функция за вземане на решение

Нека (T) е прагът за приемане на съвпадение. Решението на системата може да бъде представено като:

$$R(x) = \begin{cases} l_{i^*}, & d_{min} \le T, \\ \text{неизвестно лице}, & d_{min} > T. \end{cases} \tag{14}$$

Изборът на праг оказва пряко влияние върху поведението на системата. При по-ниска стойност на (T):

- съвпадението се приема по-трудно;
- намалява рискът неизвестно лице да бъде прието като известно;
- увеличава се рискът известно лице да бъде отхвърлено.

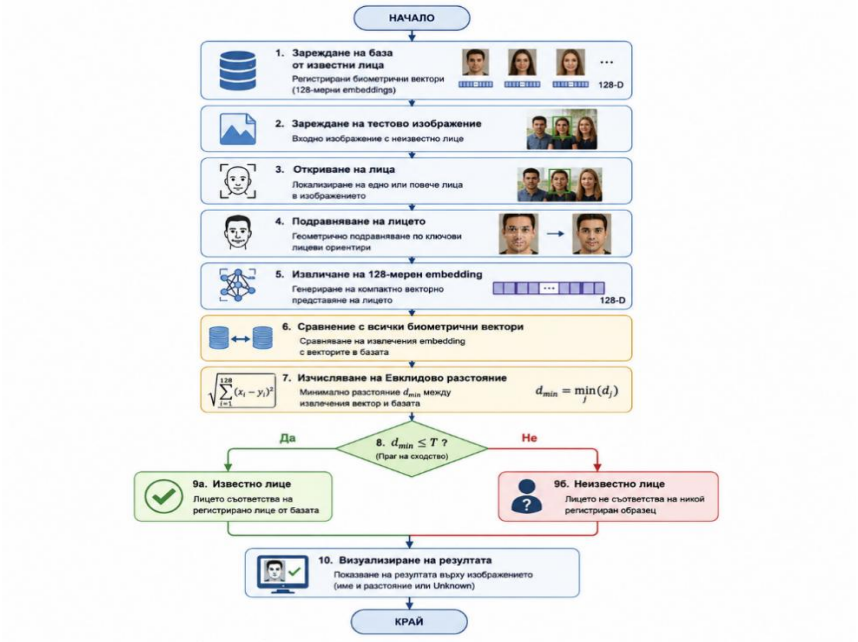
При по-висока стойност на (T):

- съвпадението се приема по-лесно;
- намалява броят на отхвърлените известни лица;
- увеличава се рискът от неправилно приемане [3].

Следователно прагът не трябва да бъде разглеждан като универсална константа. Той трябва да бъде калибриран спрямо използвания модел, качеството на изображенията, броя на лицата, допустимото ниво на риск и оперативния сценарий [3], [4].

Алгоритъм на системата и програмна реализация

Последователността на изпълнение на предложения алгоритъм е представена на фиг. 4. Блок-схемата илюстрира основните етапи на обработка – от зареждането на регистрационната база и входното изображение до извличането на биометричния вектор, сравняването с регистрираните шаблони и вземането на решение за идентичността на лицето.



Фигура 10: Блок-схема на алгоритъма за разпознаване на лица

Изчислителна сложност

Нека:

- (M) е броят на лицата в тестовото изображение;
- (N) е броят на регистрираните шаблони;
- (K=128) е размерността на вектора.

За всяко открито лице се извършва сравнение с (N) известни вектора. Сложността на сравнението е: (MNK) . Тъй като K =128 е постоянна величина, сравнителната част може да бъде представена опростено като: $O(MN)$. При малка база този подход е достатъчен.

Програмна реализация

Реализацията използва:

- **Python** — основен програмен език;
- **OpenCV** — зареждане, преобразуване, визуализиране и записване на изображения;
- **NumPy** — операции с числови масиви;
- **dlib** — детекция, лицеви ориентири и невронен модел [1], [7];
- **face_recognition** — опростен Python интерфейс към използваните функции на dlib [1].

Моделът на dlib създава 128-мерни лицеви дескриптори, които могат да бъдат сравнявани чрез Евклидово разстояние [1], [2].

```
face_recognition_project/
│
├── known_faces/
│   ├── Emil_Ivanov.jpg
│   ├── Person_2.jpg
│   └── Person_3.jpg
│
├── test_images/
│   └── test_photo.jpg
│
├── results/
│
└── face_recognition_system.py
```

Името на регистрационния файл може да бъде използвано като идентификатор:

```
Emil_Ivanov.jpg → Emil Ivanov
```

При по-развита система е препоръчително идентификаторите да не се извличат директно от файловите имена, а да се управляват чрез конфигурационен файл или база данни.

```
pip install numpy opencv-python face-recognition
```

Инсталирането на dlib може да изисква наличието на C++ компилатор и CMake, особено при някои версии на Windows. За възпроизводимост на експеримента е препоръчително да бъдат записани точните версии на Python и използваните пакети.

Регистриране на известните лица

Функцията `load_known_faces()` обхожда файловете в директорията known_faces. За всеки поддържан файл се изпълняват следните операции: Зареждане на изображението; Откриване на лицата; Проверка дали има нула, едно или повече лица; Създаване на лицева кодировка; Извличане на името от файловото име; Добавяне на кодировката и името към системната база.

Ако не бъде открито нито едно лице, файлът се пропуска. Това предотвратява създаването на невалиден шаблон.

Обработване на тестовото изображение

Функцията `process_test_image()` зарежда входната снимка чрез OpenCV и я преобразува от BGR в RGB. След това се откриват всички лица и за всяко се създава лицев вектор.

Тъй като координатите и кодировките се връщат в съответстващ ред, те могат да бъдат обработени чрез:

```
zip(face_locations, face_encodings)
```

Сравняване на лицата

Функцията `recognize_face()` изчислява разстоянията чрез [1]:

```
distances = face_recognition.face_distance(
    known_encodings,
    unknown_encoding,
)
```

Най-малкото разстояние се намира чрез:

```
best_match_index = int(np.argmin(distances))
```

Ако то е по-малко или равно на прага, се връща съответното име. В противен случай резултатът е „`Неизвестно лице`".

Визуализация

Функцията `draw_result()` изчертава правоъгълник около лицето и добавя: името; стойността на разстоянието; визуално разграничаване между известно и неизвестно лице.

Стойността на разстоянието се показва, защото предоставя повече информация от двоичното решение. Например две лица могат да бъдат приети като известни, но

едното да има значително по-ниско разстояние и съответно по-висока степен на сходство.

Изследване на прага

Препоръчва се системата да бъде изпитана с няколко стойности:

$$T \in \{0.40, 0.45, 0.50, 0.55, 0.60, 0.65\} \quad (15)$$

За всяка стойност трябва да бъдат изчислени: правилните съвпадения; неправилните съвпадения; правилните отхвърляния; неправилните отхвърляния. Това позволява да бъде определен праг, който осигурява приемлив баланс между сигурност и използваемост [3], [4].

Показатели за оценяване

Матрица на объркванията

Резултатите могат да бъдат организирани чрез следните категории [6]:

- True Positive — TP: известно лице е правилно разпознато;
- True Negative — TN: неизвестно лице е правилно отхвърлено;
- False Positive — FP: неизвестно лице е неправилно прието като известно;
- False Negative — FN: известно лице не е разпознато правилно.

ACCURACY

$$Accuracy \frac{TP+TN}{TP+TN+FP+FN} \quad (16)$$

Показателят представя общия дял на правилните решения.

PRECISION

$$Precision = \frac{TP}{TP+FP} \quad (17)$$

Precision показва каква част от приетите положителни решения са правилни.

RECALL

$$Recall = \frac{TP}{TP+FN} \quad (18)$$

Recall показва каква част от действително известните лица са разпознати.

F1-SCORE

$$F1 = 2 \cdot \frac{Precision \cdot Recall}{Precision+Recall} \quad (19)$$

F1-score е полезен при необходимост от баланс между Precision и Recall.

FALSE MATCH RATE

$$FMR = \frac{FP}{FP+TN} \quad (20)$$

FMR представя дела на опитите на различни или неизвестни лица, при които системата неправилно установява съвпадение [3].

FALSE NON-MATCH RATE

$$FNMR = \frac{FN}{TP+FN} \tag{21}$$

FNMR представя дела на опитите на действително регистрирани лица, при които системата не установява правилно съвпадение [3]. NIST използва FMR и FNMR като основни показатели при оценяване на алгоритми за биометрична верификация, а при идентификация „едно към много" използва съответни показатели за неправилна положителна и отрицателна идентификация [3], [4].

Време за обработване

Средното време за обработване може да бъде изчислено чрез:

$$\bar{t} = \frac{1}{Q} \sum_{q=1}^{Q} t_q \tag{22}$$

където:

- (Q) е броят на изпитванията;
- (t_q) е времето за обработване при конкретното изпитване.

Анализ на очакваното поведение

При стандартни фронтални изображения и достатъчно осветление може да се очаква системата да генерира сравнително устойчиви лицеви кодировки [1], [2]. Това не означава, че ще бъде постигната абсолютна точност. Дори при добри условия резултатът зависи от качеството на изображенията, броя на наличните образци и избрания праг.

Промененото осветление може да доведе до промяна на контраста и видимостта на отделни лицеви области. При силна сянка част от характерните признаци могат да бъдат представени недостатъчно ясно.

Завъртането на главата намалява видимостта на едната страна на лицето и изменя проекцията на лицевите характеристики. HOG-базираният детектор е по-подходящ за относително фронтални лица, поради което по-голямото отклонение може да доведе още до неуспешно откриване, преди да бъде достигнат етапът на разпознаване [1].

Частичното закриване може да има различно влияние според областта. Закриването на устата и носа от маска премахва част от наличната визуална информация и може да повлияе върху точността на лицевото разпознаване [10].

При неизвестните лица основният риск е неправилното приемане на най-близкия образец. Алгоритъмът винаги намира минимално разстояние, дори когато никое лице не е действително съвпадение. Поради това решението не трябва да се основава само на избора на най-близък образец, а задължително да включва праг за отхвърляне [3], [4].

Научни и приложни приноси

В резултат от изследването могат да бъдат формулирани следните приноси:

1. Предложена е модулна архитектура на система за разпознаване на предварително регистрирани лица в цифрови изображения.
2. Разработен е последователен алгоритъм, обхващащ регистрация, откриване, кодиране, сравнение и вземане на решение.
3. Формулиран е математически модел за идентификация чрез минимално Евклидово разстояние и праг за отхвърляне.
4. Алгоритъмът е реализиран като работещ прототип на Python.
5. Определени са подходящи показатели за оценяване, включително Accuracy, Precision, Recall, FMR и FNMR.

Анализирани са технологичните ограничения и рисковете от неправилно автоматизирано решение.

Заключение

В настоящата статия е представен прототип на система за разпознаване на лица от цифрови изображения чрез методи на изкуствения интелект. Разработеният подход включва последователно откриване на лицевата област, извличане на биометрични характеристики, формиране на 128-мерен вектор, сравняване с база от известни лица и вземане на решение чрез минимално Евклидово разстояние.

Предложеният математически модел показва, че разпознаването не се свежда единствено до намиране на най-близкия образец. Необходимо е минималното разстояние да бъде сравнено с праг, позволяващ отхвърляне на лица, които не присъстват в базата. Изборът на този праг определя баланса между неправилното приемане и неправилното отхвърляне.

Програмната реализация демонстрира, че с достъпни библиотеки на Python може да бъде създаден функционален изследователски прототип. В същото време готовият модел не премахва необходимостта от внимателно проектиране, експериментално валидиране и анализ на ограниченията. Качеството на изображенията, положението на главата, осветлението, закриването и размерът на базата могат да окажат съществено влияние върху резултатите. Допълнително, независимите оценки на NIST показват, че демографските фактори също могат да бъдат свързани с различия в поведението на алгоритмите за лицево разпознаване [9].

Особено важно е биометричният резултат да не се интерпретира като безусловно доказателство за идентичност. При реални приложения системата трябва да включва оценка на качеството, проверка за жизненост, защитено съхраняване на шаблоните, регистриране на действията и човешки контрол. При сценарии с висока критичност лицевото разпознаване следва да се комбинира с допълнителни средства за удостоверяване.

Acknowledgement:

This work was supported by the NSP "Security and Defence" program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

References

1. Dlib. Face Recognition Model and Python Examples.
2. Dlib. High Quality Face Recognition with Deep Metric Learning.
3. National Institute of Standards and Technology. Face Recognition Technology Evaluation — 1:1 Verification.
4. National Institute of Standards and Technology. Face Recognition Technology Evaluation — 1:N Identification.
5. European Parliament and Council of the European Union. Regulation (EU) 2016/679 — General Data Protection Regulation. Official Journal of the European Union, 2016.
6. Phillips, P. J., Martin, A., Wilson, C. L., Przybocki, M. An Introduction to Evaluating Biometric Systems. IEEE Computer, Vol. 33, No. 2, 2000, pp. 56–63.
7. King, D. E. Dlib-ml: A Machine Learning Toolkit. Journal of Machine Learning Research, Vol. 10, 2009, pp. 1755–1758.
8. OpenCV. Cascade Classifier — Face and Eye Detection.
9. Grother, P., Ngan, M., Hanaoka, K. Face Recognition Vendor Test Part 3: Demographic Effects. NISTIR 8280, National Institute of Standards and Technology, 2019.
10. Ngan, M. L., Grother, P. J., Hanaoka, K. K. Ongoing Face Recognition Vendor Test Part 6B: Face Recognition Accuracy with Face Masks. National Institute of Standards and Technology, 2020.

SOCIAL STUDIES

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

THE LOOK AND THE SMILE AS A MEANS OF COMMUNICATION

Valya M. Simeonova

Logistic support command, valiasimeonova_sweet@abv.bg

***Abstract**: The report examines the essence of the smile and the gaze and their importance in the communication process. With his gaze, a person can express everything - praise, reprimand, reproach, warning, approval, admiration, surprise, astonishment, joy, pain and many other nuances of emotions, moods and feelings. The smile is the most powerful non-verbal tool in modern civilization. It is a sign with universal meaning and expresses a complex complex of signals.*

***Keywords**: Non-verbal communication, gaze, smile*

ПОГЛЕДЪТ И УСМИВКАТА КАТО СРЕДСТВО ЗА КОМУНИКАЦИЯ

Валя М. Симеонова

Командване за логистична поддръжка, valiasimeonova_sweet@abv.bg

***Резюме**: В доклада са разгледани същността на усмивката и погледа и значението им в комуникационния процес. С погледа си един човек може да изрази всичко - похвала, порицание, упрек, предупреждение, одобрение, възхищение, изненада, учудване, радост, болка и много други нюанси на емоции, настроения и чувства. Усмивката е най-мощното невербално средство в съвременната цивилизация. Тя е знак с универсално значение и изразява сложен комплекс от сигнали.*

***Ключови думи**: невербална комуникация, поглед, усмивка*

Невербалната комуникация е процесът, при който хората чрез разменяне на телесно-пластични сигнали и конкретно организиране на пространството осъществяват връзка по между си, предават си информация, чувства и мисли, или казано по друг начин – общуват и се разбират без думи, само с помощта на знаците и фигурите.

Според психологията влиянието, което се оказва върху околните, зависи 7% от това, което казваме, 33% от начина, по който го казваме, 55% от езика на тялото ни. Човешкото тяло е в състояние да пресъздаде над 700 000 различни движения, които могат да бъдат разделени на 60 различни и символни сигнали, както и на около 60 жеста. Алън Пийз и Алън Гарнър [5] в своя труд пишат, че като цяло учените, занимаващи се с невербална комуникация са констатирали и регистрирали близо един милион несловесни сигнали и знаци.

Лицевото изражение е един от основните канали за въздействие в несловесното общуване. Карнеги пише, че "изражението на лицето е много по-важно от дрехите, в които сме облечени." [3] Именно чрез него най-вече се предава информация за емоционалното състояние и отношение на човек. В научната литература са

известни около 20 000 изражения. Екман говори за три вида изражения - неволеви (спонтанни и несъзнателни), волеви (предумишлени и в резултат на контрол над лицето) и заучени (които са станали автоматични и се задействат несъзнателно).

С погледа си на практика можем да изразим всичко - похвала, порицание, упрек, предупреждение, одобрение, възхищение, изненада, учудване, радост, болка и много други нюанси на емоции, настроения и чувства. По погледа често ние се опитваме да разберем дали човекът срещу нас е честен. Нормалният, постоянен контакт с очите обикновено се възприема като знак, че човек казва истината, докато неспособността да се поддържа контакт с очите се възприема като показател за лъжа или измама.

Усмихвайки се човек изразява своите емоции и чувства. Съществуват три основни типа приятелски усмивки - обикновена, приповдигната и широка. Разликата между тях е степента на интензивност, като по-интензивните усмивки предават и по-силни послания. Освен тях съществуват враждебни, неискрени и тревожни усмивки, като всяка една говори много за човека, който стои зад нея.

Усмивката

Устните също отразяват характера на човека. Тънките устни са знак за човек, който работи много усърдно и също така е отговорен. Малката уста показва, че човек е способен на високи нива на концентрация. По-пълните устни са индикация за хора, които обичат да се забавляват и имат по-спокоен подход към живота. Широката устата разкрива човек, който обича да открива нови преживявания.

Усмивката е най-мощното невербално средство в съвременната цивилизация. Тя изразява сложен комплекс от сигнали. Лицето изразява многобройни и разнообразни емоции. Контролът на емоциите, владеенето на поведението е задължително за военнослужещите. Безизразното лице, известно като „лице на покерджията“ или „каменно лице“, се използва за прикриване на неприятни емоции, т.е. маска, която предпазва от саморазкриване на личността. За военнослужещите усмивката е част от невербалното поведение, показва енергичност, желание за ползотворна среща. Най-често тя се използва в началото и в края на срещи, както и за изразяване на добронамереност и удовлетвореност. Широка или дискретна, усмивката не бива да се изолира от останалите езикови средства, особено от мимиките на лицето, както и от погледа. Една заучена усмивка се декодира безпогрешно като фалшиво отношение на доброжелателност или учтивост, когато погледът е студен или няма никаква подвижност на лицевите мускули или те изразяват коренно различни емоции. Затова специалистите по невербална комуникация съветват да се усмихваме винаги от сърце – тогава се появяват фини бръчици около очите и устата, а цялото лице се оживява. Това е искрената усмивка, която печели симпатии и доказва специално отношение.

Усмивката е най-изчистеният сигнал за топлота. [1] Когато се усмихваме ни възприемат за 9,7 пъти по-топли и приветливи. Но усмивките не издават само топлота и щастие. Те включват в себе си и ангажираност. Усмивките ни правят по-лесно запомнящи се. Усмивките ни очароват, защото предизвикват активност в собствените ни възнаградителни центрове в мозъка и е по-лесно да запомним хората и нещата, които ни карат да се чувстваме добре. Изследователи са

установили, че усмивките увеличават притока на кръв към мозъка. Това е един от невербалните сигнали, които активизират цялата нервна система, задействайки освобождението на хормони, които ни карат да се чувстваме страхотно. По този начин получаваме повече енергия и се чувстваме по-оптимистично настроени. Казано накратко: усмивката предизвиква както вътрешен, така и външен ефект „Еха!". Освен социални, тя има и вътрешни предимства.

Изкуствените усмивки не са запомнящи се. Има една много важна разлика между истинските и фалшивите усмивки – истинската винаги достига до ъгълчетата на очите и предизвиква миниатюрни бръчици „пачи крак".

Ето защо усмивката е толкова важна – само истинските усмивки оказват влияние на хората, които ги виждат. Щом забележим нечия искрена усмивка, тя предизвиква свиване и на собствените ни лицеви мускули. Всъщност изследователи са установили, че е много трудно да се мръщим, ако някой насреща ни се усмихва.

Една истинска усмивка често води до смях. Повечето хора смятат смеха за сигнал на хумора, който сигнализира, че нещо е смешно. Смеенето заедно с някого обаче е и чудесен начин за осъществяване на връзка. Учени са установили, че да се смееш с някого е един от най-добрите катализатори на връзка. Това е така, защото смехът е споделено позитивно преживяване, което стимулира производството на ендорфини, от които се чувстваме добре. Смехът ни прави по-открити и насърчава другите да бъдат по-открити с нас.

Усмихването и смехът всеобщо се възприемат като сигнали, които показват, че човек е щастлив. Забележителното при усмивката е, че когато се усмихнете на някого, това го кара да ви отвърне, като също ви се усмихне.

Започвайте и завършвайте общуването си с бавна усмивка. Усмивките са най-важни, когато виждаме някого за пръв път, както и когато завършваме взаимодействие с някого.

Отговаряйте на усмивките. Не се усмихвайте иззад затворени врати или зад гърба на хората. Вместо това запазете усмивките си, за да им се радвате в компанията на хора. Недейте просто да се усмихвате заради някого – усмихвайте се заедно с него. Усмихвайте се, когато някой се включи в разговора или в момента, в който погледите ви се срещнат.

Важно е в репертоара на езика на тялото да включите редовно усмихване, дори когато не ви е до смях, тъй като усмихването директно влияе върху нагласите на другите хора и начина, по който те ще реагират. Способността да се разшифроват усмивките, е кодирана в мозъка като средство за оцеляване. Тъй като усмивката е в същината си сигнал за подчинение, пра-, прачовекът е трябвало да може да разпознава дали приближаващият непознат е дружелюбен, или агресивен. Ако не е успявал, е загивал.

Не се усмихвайте, когато трябва да демонстрирате неодобрение или когато искате някой да се отдръпне.

Усмивката е знак с универсално значение. Тя представлява непреднамерено и неволно движение на лицевите мускули и най-вече разтягане на устните и показване назъбите, което е външен израз на оживление върху лицето, чувства на

симпатия, радост, веселост, доволство, както и горчивина, сарказъм, т.е. язвителност, жлъч, злоба. [2]

Според британски учени най-често срещаните усмивки са: проста усмивка, горна усмивка, широка усмивка.

Кратък анализ на тези три вида усмивки показва следното:

Простата усмивка, при която зъбите не се показват, се наблюдава често у хора, които са сами или не се занимават с определена работа, в която участват други хора. Те до известна степен се усмихват на себе си.

При горната усмивка се разкрива горният ред зъби и усмихващият се има пряк очен контакт с другия индивид. Тази усмивка се използва често като усмивка за поздрав. Това е така наречената „как се чувствате" – усмивка.

Широката усмивка може да се наблюдава при игра и често преминава в смях. При нея се откриват както горният ред зъби, така и долният, но пряк очен контакт при тази усмивка имаме сравнително рядко. [2]

Усмивката не изразява непременно чувство за щастие. „Пазете се от усмивка с десния ъгъл на устата" е казал един психолог. Този израз той използва за усмивка, която не се прави от учтивост. Устните така се изпъват, че се получава десен ъгъл. Тази усмивка няма дълбочина. С това изражение човек показва, че това, което му се говори, е „добро поведение". Така се усмихва момиче, на което се досажда или бъде поставено от шефа си в двусмислена ситуация.

Така наречената устна усмивка наподобява горната усмивка, само че при нея долната устна се впива навътре между зъбите. Устната усмивка показва, че усмихващият се чувства по-нискостоящ от този, към когото я отправя.

Разглеждайки лицето на човек, да се взимат предвид и устните на човек, чиято челюстна мускулатура се намира в спазматично враждебно състояние, устните също се свиват и вземат леко нацупен израз. Лекото нацупване сигнализира защитно поведение. Съответното лице иска колкото се може по-малко да се проявява и реагира. Затвореният, необщителният, мълчаливият израз на лицето всъщност се основава на притиснатите устни.

Поглед и движение на очите

Очите на даден човек също са показателни за много неща, могат да разкрият много за индивида. Както вече знаете, те са прозорец към душата и един внимателен поглед в очите на човек може да разкрие повече от това, което той би искал да каже за себе си. Човек с малки очи е много прецизен и отдава голямо значение на дребните детайли. Хората с големи очи са по принцип нежни по природа, също така много внимателни и любвеобилни. Ако наблюдавате хора с очи, които са близко едно до друго, ще забележите, че те имат способността да се концентрират много добре и са много последователни. Тези хора са също много динамични по природа. Лице с очи, които са разположени далеч едно от друго е с либерален характер.

Очите са нашият зрителен портал към света. От момента на раждането ни ние започваме да сканираме обкръжението си в търсене на познати лица, движения, непознати обекти, цветове, нюанси и симетрия, както винаги предпочитаме естетичното и красивото. Нашият поглед търси нови гледки и преживявания.

Очите могат да изразяват както любов и състрадание, така и страх и презрение. Радушният и весел поглед на някой човек може да направи деня ни по-хубав. По него можем да разберем кога нещо не е наред и дали човекът има грижи и проблеми. Погледът може да обгърне цяла зала или да се сниши сред тълпата от непознати. Очите обикновено са първото, което забелязваме у другите. [4]

Погледът и движенията на очите са важно комуникативно средство при общуването. Чрез погледа се установява пряк визуален контакт, дават се различни знаци, изразяват се емоции, чувства и отношение. Различните видове погледи и характерни движения с очите участват и в мимиката, и в жестовете, играят ролята на „тих език". Откритият, ясен поглед е първата предпоставка за установяване на сериозни и благонадеждни отношения между комуникиращите страни. Блуждаещият или сведен поглед е сигнал за нещо нередно – разсеяност, прикриване на неприятна вест, нехаресване на събеседника. Негова противоположност е втренченият поглед, впит в събеседника непрекъснато.

При междуличностната комуникация човешките очи излъчват най-показателните и точни сигнали за вътрешната нагласа, защото са централна, ключова точка на тялото и зениците им функционират независимо от останалите му части. [5]

Съвременните изследвания доказват, че 87% от информацията постъпва в мозъка през очите.

Зениците на очите се разширяват или свиват – както според силата на светлината, така и съобразно вътрешната нагласа и настроението на човека, когато те се променят от положителни към отрицателни и обратното. Когато някой се развълнува, зениците на очите му се разширяват, като размерът им може да стане до четири пъти по-голям от нормалния. Гневът и отрицателните емоции карат зениците да се свиват и очите стават „като маниста" или „като на змия".

Само когато сме „очи в очи" с друг човек, може да бъде създадена основа за истинска комуникация. Но докато по време на разговор някои хора ни карат да се чувстваме напълно удобно и непринудено, други ни притесняват, а за трети чувстваме, че не можем да им имаме доверие. Тези усещания са свързани най-вече с продължителността на времето, през което съответният човек ни гледа или приковава погледа ни, докато говори. [5]

Когато някой е неискрен или прикрива някаква информация, погледът му среща вашия само за около една трета от цялото време на разговора. Когато нечий поглед среща вашия за повече от две трети от цялото време на разговора, това би могло да означава едно от следните неща: първо, съответният човек ви намира за много интересна и привлекателна личност, като в този случай погледът е съчетан с разширени с разширени зеници; второ, съответният човек е настроен враждебно или поне недоброжелателно към вас и може би ви отправя несловесно предизвикателство, като в този случай погледът ще е съчетан със свити зеници.

Алън Пийз посочва четири вида поглед:

- Делови /гледане в триъгълника между двете зеници и фронталния синус/;
- Социален /насочване на погледа под нивото на очите в триъгълника между двете зеници и устата;

- Интимен /след кратко поглеждане в очите погледът се насочва към гърдите или още по-надолу/;
- Кос /изпод вежди – при проява на силен интерес или при демонстративно недоверие/.

Джо Наваро [4] в своя речник посочва още някои особености за очите. Отпуснатите очи са сигнал, че се чувстваме удобно и спокойно. Когато сме спокойни, мускулите около очите, както и тези на челото и бузите, са отпуснати, но в момента, в който се разтревожим или напрегнем, те също се напрягат. Преди да опитате за интерпретирате какъвто и да е жест или мимика, винаги поглеждайте очите за твърд и надарен. Мускулите на очите и на околоочния контур реагират на дразнителите много по-бързо от останалите лицеви мускули и почти мигновено издават вътрешното състояние на индивида.

Честотата на примигване зависи от заобикалящата среда и количеството стрес или възбуда, които човекът преживява. Всеки индивид е различен, но типичната честота на примигване е между 16-20 примигвания в минута, в зависимост от осветеността и влажността на средата. Хората, които работят на компютър, примигват по-рядко докато онези, които работят в среда с прах или полени, примигват по-често.

Изследвания по цял свят показват, че индивидите с по-висок социален статус поддържат по-продължителен визуален контакт с другите, както докато говорят, така и докато слушат. Индивидите с по-нисък социален статус по-често гледат в очите по-висшестоящите, докато слушат, и по-рядко, докато говорят. Склонни сме да харесваме индивиди, които осъществяват директен визуален контакт с нас, особено ако те са по-висшестоящи.

Целта на настойчивия поглед е да привлече вниманието на другия по един сърдечен или романтичен начин. Този вид поведение се отличава с меката благосклонност, която е изписана на лицето на заинтересования, и се чете в очите и устните му, както и в постоянните опити, които той прави, за да намери погледа на другия. Настойчив поглед отправяме, когато искаме да кажем на някого, че се интересуваме от него и че бихме искали да го опознаем по-отблизо.

Продължителен поглед и втренчване. Има голяма разлика между това да задържите поглед върху някого и да се втренчите в него. Втренчването обикновено е по-хладно и дистанцирано или открито предизвикателно и сигнализира, че намираме човека или неговото поведение за подозрително, тревожно или странно. От друго страна, продължителният поглед издава, че сте благосклонни към човека отсреща и че той или неговото поведение ви успокоява. Втренчването означава, че сме нащрек, докато продължителният поглед означава, че сме заинтригувани и дори добронамерени. Втренчването може да бъде изтълкувано като оскърбление, особено в затворена среда като автобус или подлез.

В. Руменчев отбелязва, че е възможно по-голямото количество поглед да изразява защитно поведение, при което насрещната страна се следи визуално много внимателно. Според него това е добре, когато се цели предотвратяване на физическа агресия, но не се препоръчва при делово общуване, тъй като от една страна издава слабост, а от друга, кара противника да засили самоконтрола и да

преустанови или сведе до минимум изтичането на невербална информация. Руменчев не изключва подобно поведение да се възприеме и като стремеж за доминиране и агресия. [6]

Почти във всички езици съществува изразът „скрит поглед", който всъщност е израз на страничен поглед. Той се използва от хора, които искат да видят нещо, без да бъдат засечени.

Друг поглед е този, при който клепачите са полуспуснати, така че да не закриват погледа, а само да го фиксират върху даден интересен предмет или личност.

Очните ябълки се движат в различни направления от очнодвигателните мускули. При психическо напрежение като уплаха, нерешителност или страх погледът не е насочен към един обект и е налице движение на очните ябълки в различни посоки (погледът се мести от обект на обект). При наличие на увереност погледът е целенасочен и няма движение на очните ябълки. При силна умора или панически страх понякога се нарушават съдружните движения и на моменти се появява разногледство.

Очните зеници също търпят значителни промени при психическо напрежение. Зеничните реакции са сравнително автономни и независимо че се намират под регулиращото действие на главния мозък, търпят значителни промени под влияние на емоционалните състояния, в които изпада човешката личност.

Вербалните и невербалните средства за комуникация предоставят възможност за формиране на определено мнение от първите минути на общуването. Съзнателното наблюдение на собствените действия, пози и жестове, както и тези на другите хора е най-добрият начин за постигане на задълбочено разбиране на значението на отделните невербални знаци.

В заключение може да се каже, че умението да се разчитат правилно съвкупността от невербалните сигнали, които се предават по време на комуникационния процес е ключово умение за всеки ръководител, но и за всеки, който иска да провежда ефективна комуникация.

Използвана литература

1. Едуардс, В. (2023). Тайните сигнали на общуването. София, Хермес. 400с.
2. Йорданов, Николай. (2006). Психология на комуникацията. И мълчанието говори. София, Военно издателство ООД. 111 с.
3. Карнеги, Д. (1996). Как да печелим приятели и да влияем на другите. София, Кибеа.
4. Наваро, Д. (2019). Речника на езика на тялото. София, Изток-запад. 192 с.
5. Пийз, А., Алън Гарнър. (2000). Езикът на тялото. Скритият смисъл на думите. София, Сиела.
6. Руменчев, В. (2006). Невербална комуникация в публичната реч и деловото общуване. София, УИ "Св. Кл. Охридски".

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**, Faculty of Artillery, Air Defense and Communication and Information Systems

INFORMATION PROVISION OF MACROCONFLICT MANAGEMENT

Asen Zahariev

University of Library studies and information technologies, a.zahariev@unibit.bg

Abstract: *The article examines the security environment , which is characterized by increasing complexity of macro-conflicts, determined by the processes of globalization, technological development, increasing interdependence between states and the emergence of new forms of hybrid confrontation . Basic theories of conflict management are presented, noting their advantages, limitations and applicability in the conditions of the modern environment. Special attention is paid to information provision as a strategic resource in the process of macro-conflict management. Some studies are noted that consider information as a key factor for strategic decision-making. The role of international organizations like the UN, the EU and NATO and their abilities to influence the different stages of conflict dvelopment are examined. The growing role of security services as key participants in the gathering, processing and analysis of information is also examined. Special emphasis is placed on the model of Johan Galtung, which is generally applicable and offers a concept for conflict transformation by overcoming contradictions between parties and creating prerequisites for sustainable solutions. The main goal is to present the role and importance of information provision in the process of macro-conflict management, analyzing the influence of information factors on strategic decision-making in the prevention and resolution of macro-conflicts. The article justifies the thesis that in the conditions of modern conflicts, information provision should be considered not as an auxiliary function, but as a strategic component determining the effectiveness of conflict management*

Keywords: *conflicts, management, information*

ИНФОРМАЦИОННО ОСИГУРЯВАНЕ НА УПРАВЛЕНИЕТО НА МАКРОКОНФЛИКТИ

Асен Захариев

Катедра „Национална и международна сигурност", факултет „Информационни науки", Университет по библиотекознание и информационни технологии

Резюме: *В доклада се разглеждат средата на сигурност, която се характеризира с нарастваща сложност на макроконфликтите, обусловена от процесите на глобализация, технологично развитие, нарастваща взаимозависимост между държавите и появата на нови форми на хибридно противопоставяне. Представени са основни теории за управление на конфликти, като са отбелязани техните предимства, ограничения и приложимост в условията на съвременната среда. Специално внимание е отделено на информационното осигуряване като стратегически ресурс в процеса на управление на макроконфликтите. Посочени са някои изследвания, които разглеждат информацията като ключов фактор за вземане на стратегически решения. Разгледана е ролята на международни организации като ООН, ЕС и НАТО и техните възможности да въздействат на различните етапи на развитието на конфликтите. Разгледана е и нарастващата роля на службите за сигурност, като основни участници в придобиването, обработката и анализа на информацията.*

Особен акцент е поставен върху модела на Йохан Галтунг, който е общоприложим и предлага концепция за трансформация на конфликтите чрез преодоляване на противоречията между страните и създава предпоставки за устойчиви решения. Основната цел е да се представят ролята и значението на информационното осигуряване в процеса на управление на макроконфликтите, като се анализира влиянието на информационните фактори върху вземането на стратегически решения при предотвратяването и разрешаването на макроконфликти. Докладът обосновава тезата, че в условията на съвременните конфликти, информационното осигуряване следва да се разглежда не като спомагателна функция, а като стратегически компонент, определящ ефективността на управлението на конфликти.

Ключови думи: *конфликти,управление, информационно осигуряване*

Въведение

На настоящия етап съвременната среда на сигурност се характеризира с изострени геополитически противопоставяния, ескалиращи в някои случаи до остри форми на кризи и конфликти в различни точки по света. Новите реалности формират среда с висока степен на неопределеност и пораждат нови рискове и заплахи, които силно рефлектират върху стабилността в глобален и регионален мащаб. Прилаганите силови подходи за постигане на определени политически и стратегически цели се отразяват и в сферата на международните отношения като допринасят за намаляване на доверието и отслабване на международните институции. Прилагането на концепцията „Мир чрез сила“ или дискусиите за „силата на правото или правото на силата“, както и анализът на историческия опит невинаги дават очакваните резултати. Показателен за това е фактът, че не бяха избегнати редица остри международни конфликти и агресивни намеси във вътрешните работи на много държави в различни региони по света. Според данни на Департамента за изследване на мира и конфликтите към университета в Упсала – Швеция, към момента в света активните въоръжени конфликти са 61(UCDP). Най – значимите големи въоръжени конфликти с международно значение са в Европа и Близкия изток после в статискитата следват вътрешни конфликти с огромни хуманитарни последици в Судан, Мианмар, множество конфликти в Африка и Азия. Съществуват и множество конфликти с потенциал да прерастнат във въоръжени. В стремежа за постигане на ефективно управление на конфликтите са провеждани редица изследвания и анализи на историческия опит.

Съвременните теории за управление на международни конфликти предлагат различни обяснителни модели за причините, динамиката и възможностите за въздействие върху конфликтите. Тяхната стойност се проявява най-вече с практическата им приложимост на етапите на ранно предупреждение, превенция, деескалация, посредничество, мироопазване и следконфликтно възстановяване. Сред най-разпространените концептуални подходи в научната литература се открояват теорията за управление на конфликти, теорията за разрешаване на конфликти, теорията за трансформация на конфликтите, реалистичният и либералният подход в международните отношения, както и по-новите концепции за човешка сигурност, хибридни конфликти и обществена устойчивост. На

настоящия етап особено значение заемат концепциите за хибридните конфликти и информационното противопоставяне, които се обуславят от развитието на информационните технологии и дигиталната свързаност и разширяват обхвата на противопоставяне отвъд традиционните военни действия.

Всяка от посочените теории има своите приноси и дефицити в управлението на конфликтите, но сложната им многоаспектна природа изисква да се прилагат комбинирани подходи съобразно етапите на развитие. Какъвто и да е характерът на конфликтното взаимодействие, информационното осигуряване изпълнява ролята на свързващ елемент между различните управленски подходи. Независимо дали става въпрос за превенция, кризисно управление, посредничество или следконфликтно възстановяване, ефективността на управленските действия е пряко зависима от наличието на своевременна, достоверна и аналитично обработена информация.

Съвременните изследвания на информационното осигуряване при макроконфликти се свеждат основно до ранното предупреждение и превенцията на конфликти. Друго направление акцентира върху ситуационната осведоменост и аналитичната поддръжка на вземането на решения. Разглежда се информационната среда като поле на противопоставяне, напр. информационни операции, операции по дезинформация, кибератаки и т.н. Следващо направление разглежда стратегическите комуникации като инструмент за управление на възприятията. Подходът, свързан с устойчивостта на държавите и обществата, предполага не само реакция, но и предварителна подготовка. Общото в различните направления е, че като цяло информационното осигуряване има съществено значение във всички фази на конфликти от различен характер. В редица изследвания, очакванията за цялостния процес по информационно осигуряване на управлението са свързани със сектор сигурност и най-вече разузнавателните и контраразузнавателните служби. В тази връзка следва да се има предвид, че службите за сигурност са само част от системата, наред с дипломатическите мисии, международните организации, институти, откритите източници и медийните и социални платформи. Тяхната роля е да осигуряват достоверна информация за подпомагане на вземането на стратегически решения и управлението на макроконфликти. В този смисъл те се явяват ключов фактор на информационната система не само в кризи и конфликти.

Методология на изследването

Основният инструментариум, използван в доклада, е анализ на монографии, книги, научни статии, статистически данни, както и синтез на знания и опит.

Резултати

Същността, характеристиките, генезисът и механизмите на конфликтите винаги са стояли на вниманието на изследователите. Изследванията на макроконфликтите се основават на теорията на една сравнително нова научна област – „Конфликтология". В теорията е заложено разбирането, че конфликтът е проява на социални връзки и отношения между хората, способ за взаимодействие при

сблъсък на несъвместими възгледи, позиции и интереси, противоборство на взаимосвързани, но преследващи свои цели две или повече страни. (Гоцев с.66). В стремежа за ефективно управление на социалните конфликти изследователите в предметната област представят различна категоризация, в зависимост от същността и причините за тяхното възникване и форми на проявление и на тази основа са се формирали и различни способи за тяхното предотвратяване, регулиране и разрешаване.

Въпреки натрупания опит в разрешаването на редица конфликти, изследванията в тази насока все още се отличават със значителни различия в крайните теоретични обобщения и практически решения. Прилагането на различни критерии при категоризацията, в зависимост от сферите на обществения живот, оформя най – общо следната категоризация:

- Икономически, свързани с пазарните отношения. Съществено влияние оказват конкуренцията за енергийни ресурси и транспортни коридори, както и икономическите зависимости, уязвимости и потенциални последици от санкционни режими;
- Политически, които възникват в сферата на политическите отношения и могат да прераснат във въоръжен сблъсък. Тук в тясна връзка са военностратегическите причини за конфликти, като надпреварата във въоръжаването и трансформацията на системите за сигурност.

В зависимост от участниците:

- Междуличностни и междугрупови, при които острите форми на проявление най-често са на етническа и религиозна основи и междудържавни, т.е. макроконфликти, които прерастват във военни. (Генова с.29).

Управлението на конфликтите във всички сфери е необходимо за възстановяване на баланса и поддържане на социалната стабилност. От изброените видове конфликти като особено значими са макроконфликтите, които трудно се поддават на регулиране, характеризират се с бърза ескалация, разрастване и огромни последствия, свързани с човешки жертви и хуманитарни кризи.

Въпреки, че има различни теории и подходи за управлението на конфликти, един модел се отличава със своята универсалност, приложимост и ефикасност. Към съвременните изследвания, съществен принос има моделът „TRANSEND“ на Йохан Галтунг. Моделът е разработен като алтернатива на традиционните модели за управление и разрешаване на конфликти, който трансформира конфликта и преодолява несъвместимостта. В основата е заложено разбирането, че основните причини за противопоставяне на държавите са различията в националните интереси, транснационалните въпроси, създаващи редица предизвикателства пред националните правителства и политически системи, изразяващи се в глобализация на ресурсите и екологичните проблеми, отваряне на пазарите и появата на плаващи валутни курсове. (Галтунг с.64). Приносът на този подход е, че матричното решение предоставя повече алтернативи и дава възможности на конфликтуващите да погледнат в бъдещето. На основата на гореизложеното може да се обобщи, че макроконфликтите са сложни социално-политически процеси с широк пространствен, времеви и функционален обхват, които засягат международната

система като цяло или значителни нейни подсистеми. Те се характеризират с участие на множество участници, висока степен на интензивност и устойчивост във времето, както и със значителни последици за регионалната и глобалната сигурност. Обикновено надхвърлят рамките на отделни държави, въвличат се и други участници и оказват дълготрайно влияние върху международните политически, икономически и информационни процеси. Това конфликтно взаимодействие се развива на стратегическо ниво и освен конфликтуващите държави могат да се включат и коалиции. В основата на тези конфликти стоят фундаментални противоречия, свързани с ресурсите, с контрола върху територии и стратегически пространства, както и със сблъсъка на ценности, интереси и модели на развитие.

В управлението на такива конфликти следва да се имат предвид ролята, значението и влиянието на международни и регионални организации, транснационални корпорации, неправителствени организации и в определени случаи недържавни въоръжени групировки. Друг значим фактор, който трябва да се отчита, е дигитализацията, глобалната свързаност и информационните въздействия върху обществото, които придобиват все по-голямо значение. Появиха се нови заплахи като хибридни операции, дезинформационни кампании и кибератаки, които оказват влияние върху обществените нагласи. При тези обстоятелства става все по-трудно да се преценява достоверността на информацията.

Новите реалности, свързани с геополитическите противоречия, произтичащи от стремежа към ревизия на установения международен ред, изискват ефективно информационно осигуряване на стратегическото вземане на решения. Непълната, недостоверната, несвоевременната или манипулираната информация може да доведе до погрешни оценки на намеренията и способностите на опонентите, което значително повишава риска от ескалация на междудържавните конфликти.

Ключова роля в разрешаването на различни по характер конфликти имат международните организации. При разглеждане на ролята на международните структури при управлението на макроконфликти възникват основателни въпроси относно възможностите за въздействие на противоречията. Възникват въпроси защо, след като има организации, нормативна уредба и механизми за управление, редица конфликти не бяха предотвратени.

В тази връзка на основата на международни правни актове ще представим възможностите на ООН, НАТО и ЕС и съответно техните ограничения.

Безспорно ООН заема централно място в системата на международната сигурност и колективното управление на конфликти, но нейната ефективност следва да се оценява във връзка с институционалните ограничения и променящата се природа на съвременните конфликти. Предимствата се свеждат до висока степен на международна легитимност, универсално членство и нормативна рамка, основана на международното право и Устава на ООН. В арсенала за въздействие са превантивна дипломация, посредничество, мироопазващи операции, санкционни режими и хуманитарна координация. Въпреки че общото впечатление е, че не е достатъчно бърза и гъвкава, в редица случаи е успявала да предотврати ескалация

или да подпомогне постигането на примирие между конфликтуващите. При високо интензивни макроконфликти, включващи големи сили или стратегически интереси, ефективността значително намалява. Основният проблем е правото на вето на постоянните членове на Съвета за сигурност. Друг проблем е трансформацията на конфликтната среда. Съвременните конфликти имат хибриден характер, включват недържавни участници, информационни и киберизмерения. Тези особености затрудняват прилагането на традиционните инструменти, които са проектирани основно за класически междудържавни конфликти. Съществен проблем е и осигуряването на своевременна, надеждна и интегрирана информация, необходима за ранно предупреждение и стратегическо вземане на решения. Предвид посочените предимства и ограничения може да се обобщи, че организацията е ефективен, но ограничен инструмент за управление и разрешаване на макроконфликти. Тя е най-успешна като платформа за легитимиране на международни действия, посредничество и координация, но не разполага с достатъчен капацитет и автономия за самостоятелно разрешаване на конфликти с висока стратегическа значимост.

Европейският съюз има по-ограничен, но по-функционален мандат, насочен към управление на кризи, превенция на конфликти и стабилизация, основно в съседните региони. Легитимността на ЕС се основава на съчетанието между икономически възможности, нормативно влияние и политико-дипломатически инструменти.

НАТО е организация с ясно дефиниран колективно-отбранителен мандат. Легитимността на Алианса е ограничена до държавите членки, но в неговите рамки съществува висока степен на политическа и военна съгласуваност, което позволява бързо вземане на решения в условията на кризи.

Общото между посочените по-горе организации в процеса на управление на макроконфликти, в зависимост от техните етапи, може да се резюмира накратко по следния начин:

Дейностите по предотвратяването на конфликти са насочени към ранно идентифициране на рисковете и ограничаване на факторите, които могат да доведат до ескалация. Управленското въздействие при конфликти следва да е ориентирано към предотвратяване използването на насилие и принуда. Изследванията показват, че 80% от конфликтите се решават на този етап. През следващите фази възможностите значително намаляват. (Недялков)

В етапа на предотвратяването ролята на ООН се свежда до мониторинг на напрежения и сигнализиране за потенциални конфликти, но ефективността ѝ е ограничена, поради зависимостта от информация, предоставяна от държавите членки, и от липсата на консенсус в Съвета за сигурност.

Възможностите на ЕС в предотвратяването се свеждат до стратегическо наблюдение, санкционна политика и подкрепа за институционално развитие. ЕС може да въздейства върху първопричините за конфликти, особено в съседните региони.

Северноатлантическият съюз има ограничена, но нарастваща роля в предотвратяването на конфликти, главно чрез стратегическо възпиране,

ситуационна осведоменост и споделяне на разузнавателна информация. Превантивната функция на Алианса е насочена преди всичко към предотвратяване на военна ескалация между държави.

В етапа на регулиране, чиято основна цел е ограничаване на насилието, стабилизиране на ситуацията и предотвратяване на по-нататъшна ескалация, ООН традиционно играе водеща роля чрез мироопазващи мисии, посредничество и мониторинг на примирия. Тя е особено ефективна при регулиране на конфликти с ниска до средна интензивност и при наличие на международен консенсус. Европейският съюз също участва активно на етапа на регулирането чрез цивилни и смесени мисии, дипломатически посредничества и координация на хуманитарни усилия. Информационното осигуряване на ЕС подпомага интеграцията между политическите решения и действията на място.

НАТО е най-ефективен при регулиране на конфликти с висок военен интензитет, когато се налага бързо стабилизиране на обстановката чрез военни средства. Високото интегрирано информационно осигуряване на Алианса дава оперативно превъзходство, но не адресира дълбоките политически причини за конфликта.

Разрешаването на конфликти предполага трайно политическо уреждане и постигането на устойчив мир чрез елиминиране на структурните причини за противопоставянето. Тук ООН е ключов участник чрез създаване на правна и политическа рамка за мирни споразумения и следконфликтно възстановяване. Нейната сила е в легитимирането на мирните процеси, но практическата реализация често зависи от ангажираността на други международни и регионални структури. При разрешаването на конфликти ЕС има сравнително най-силен принос в дългосрочното разрешаване на конфликти чрез икономическа помощ, институционално изграждане и интеграционни перспективи. На този етап НАТО има ограничена роля в разрешаването на конфликти, тъй като неговият мандат е предимно военен. Въпреки това Алиансът може да допринесе индиректно чрез гарантиране на сигурността в следконфликтна среда.

Направената съпоставка показва, че ефективното управление на макроконфликти изисква последователно и координирано използване на механизмите за предотвратяване, регулиране и разрешаване на конфликти. ООН, ЕС и НАТО разполагат с различни, но взаимнодопълващи се инструменти, чиято ефективност зависи в решаваща степен от качеството на информационното осигуряване и междуинституционалната координация през всички фази на конфликтния цикъл. Анализът на дейността на представените организации показва, че нито една организация не разполага с пълен и универсален инструментариум за самостоятелно управление на макроконфликти. ООН осигурява международна легитимност и нормативна рамка, ЕС допринася с комплексни политически, икономически и цивилни механизми, а НАТО предоставя надежден военен и отбранителен капацитет. Тяхната ефективност значително нараства при координирано използване на ресурсите, което гарантира съгласуваност на действията.

Наред с всички механизми за разрешаване на конфликти най-съществена роля е на информационното осигуряване. Предвид широкия обхват на информационната дейност, тук няма да бъдат загегнати характеристиките на информацията, критериите за оценка, етапите на обработка и стойността на крайния информационен продукт. Необходимо е да се направи и уточнението, че не всички стратегически решения са в съответствие с експертните оценки. Целта на информационното осигуряване е да намали неопределеността. Информационната дейност е важен аспект на управлението на социалните системи и представлява целенасочен и систематизиран процес на събиране, обработка, анализ и разпространение на информация, необходима за ефективното вземане на решения в условията на сложна и динамична среда на сигурност. В контекста на съвременните макроконфликти този процес придобива особена значимост, поради нарастващата роля на хибридните заплахи, които комбинират военни, политически, икономически, кибернетични и информационни средства за постигане на стратегически цели.

Основните функции на информационното осигуряване включват информационно-аналитична, прогностична, координационна и защитна функция. Чрез тях се осигурява своевременно и надеждно познание за средата на сигурност, за намеренията и възможностите на основните участниците, както и за потенциалното въздействие на дезинформационни и хибридни операции. В този смисъл информационното осигуряване се превръща в ключов инструмент за ранно идентифициране и неутрализиране на заплахи. С най-големи възможности в тази област са службите за сигурност.

Тяхната дейност е предимно информационна, работят с широк набор информация от открити и закрити източници и са в състояние да регистрират опити за манипулиране на информационната среда.

В условията на хибридни заплахи и целенасочени дезинформационни кампании, информацията играе решаваща роля за осигуряване на устойчивостта на процеса на вземане на решения на държавното ръководство. Хибридните въздействия често са насочени към създаване на информационна несигурност, размиване на границата между истина и манипулация и формиране на погрешни възприятия у ръководството и обществото. Пропагандата и манипулацията чрез използването на откритите източници на информация са едни от най-сериозните световни проблеми (Йотова с. 145). Това значително увеличава риска от неправилни стратегически оценки и решения.

Ефективното информационно осигуряване допринася за ограничаване на тези рискове чрез системен анализ на информационната среда, проверка на достоверността на източниците и интегриране на данни от различни канали. По този начин се създават предпоставки за вземане на информирани решения, които отчитат не само обективните факти, но и възможните манипулативни въздействия върху информационния поток.

Информационните потоци в условията на съвременните макроконфликти са многопосочни и динамични, като обхващат взаимодействието между държавни институции, международни организации, медии и обществеността.

Комуникационните канали включват официални, дипломатически и военни механизми, както и дигитални платформи, социални мрежи и киберпространството, които често се използват като инструмент за дезинформация и психологическо въздействие.

В този контекст управлението и защитата на информационните потоци се превръщат в съществен елемент от информационното осигуряване. Ограничаването на дезинформационните въздействия изисква координирани действия за мониторинг на информационната среда, повишаване на информационната устойчивост на институциите и обществото, както и развитие на стратегическа комуникация, насочена към изграждане и поддържане на доверие.

В съвременната среда за сигурност информацията се утвърждава като стратегически ресурс за превенция и деескалация на макроконфликти. Навременното събиране и анализ на достоверна информация създават предпоставки за ранно идентифициране на потенциални конфликтни ситуации и за предприемане на адекватни политически, дипломатически и други невоенни мерки. В този смисъл информационното осигуряване изпълнява ключова роля за ограничаване на риска от ескалация и за управление на напрежението между държавите.

Съществен елемент от цялостното информационно осигуряване са системите за ранно предупреждение. Системата за ранно предупреждение включва няколко верижни комплекса: мониторинг на съответните процеси; изграждане на система от параметри и критерии за отчитане влиянието на дадени процеси върху зараждането и развитието на кризисните ситуации; изграждане на система от превантивни действия, които могат да предотвратят интензифицирането на даден кризисен процес; създаване на надежден и ефикасен механизъм за защита на съвременната държава, използвайки както политически и дипломатически, така и военни средства. (Манев, М., Русева, Р). В България с Наредбата за ранното предупреждение и оповестяването при бедствия е създадена организация за мониторинг на приближаваща или непосредствена заплаха, но създаването и съществуването на отделни компоненти за наблюдение и информиране за различни рискови за сигурността фактори, въпреки тяхното успешно функциониране, още не означава, че има изградена национална система за ранно предупреждение. (Приета с ПМС № 70 от 27.03.2009 г.) В тази връзка е необходимо цялостно концептуално изясняване на този проблем, разработване на дългосрочна стратегия и конкретни програми за надграждане на системата.

Системата следва не само да информира държавното ръководство, но и да предлага многовариантност на решенията. Оценката на рисковете и разработването на сценарии представляват важен инструмент за подпомагане на стратегическото планиране и вземането на решения. Чрез систематичен анализ на вероятността и на потенциалните последици от различни варианти на развитие на конфликта се осигурява възможност за предварителна подготовка и избор на адекватни мерки за реагиране.

Широко прилаганият сценариен подход позволява да се моделират различни траектории на развитие – от ограничена ескалация до пълномащабен

макроконфликт, като се отчитат както обективните фактори, така и влиянието на информационната среда. В условията на хибридни заплахи оценката на рисковете следва да включва и анализ на въздействието на дезинформационни кампании, кибератаки и други невоенни инструменти, които могат да ускорят или да възпрепятстват процесите на деескалация.

В условията на съвременните макроконфликти информационното осигуряване се утвърждава като ключов фактор за ефективното формулиране и реализиране на политически и дипломатически решения. В този контекст информационното осигуряване подпомага политическото ръководство и дипломатическите структури при оценката на ситуацията, избора на стратегически приоритети и определянето на адекватни инструменти за въздействие.

Като инструмент за подкрепа на политическите решения, информационното осигуряване осигурява анализ на интересите, позициите и поведението на основните международни субекти, както и оценка на потенциалните последици от различни политически и дипломатически ходове. Чрез систематизиране и интерпретация на данни от разузнавателни, дипломатически, икономически и информационни източници се създава аналитична основа за формулиране на политики, насочени към превенция, деескалация или разрешаване на макроконфликти. По този начин се намалява рискът от прибързани или неадекватни решения, основани на непълна или манипулирана информация.

В дипломатическата дейност информационното осигуряване играе съществена роля за подготовката и провеждането на преговори, посредничество и многостранни формати на взаимодействие. Анализът на информационната среда и на обществените нагласи позволява на дипломатическите представители да адаптират своите послания и стратегии, като отчитат както официалните позиции на партньорите, така и неформалните фактори, влияещи върху процеса на вземане на решения. В условията на активни дезинформационни кампании това подпомага защитата на дипломатическите инициативи от информационни атаки и подкопаване на доверието.

Особено значение има ролята на информационното осигуряване за подобряване на координацията и взаимодействието между различните институции, ангажирани с управлението на макроконфликти. Ефективният обмен на информация между политически, дипломатически, военни и аналитични структури създава предпоставки за единно разбиране на ситуацията и за съгласуваност на предприетите действия. Липсата на координация и фрагментираността на информационните потоци могат да доведат до противоречиви решения и да отслабят общата стратегия за управление на конфликта.

Анализът на ефективните модели на информационно осигуряване показва, че в условията на съвременните макроконфликти информацията се утвърждава като стратегически ресурс, чиято роля надхвърля традиционното подпомагане на вземането на решения. Централизираните, децентрализираните, интегрираните и технологично ориентираните модели предлагат различни възможности за управление на информационните потоци, като всеки от тях притежава специфични предимства, но и съществени ограничения. Практиката на ЕС и НАТО

демонстрира, че най-висока ефективност се постига чрез комбиниран и адаптивен подход, съобразен с конкретния контекст на сигурност.

В тази връзка могат да се очертаят следните насоки за повишаване на ефективността на информационното осигуряване:

Прилагане на интегриран модел на информационно осигуряване. Предимството е, че позволява постигането на цялостна ситуационна осведоменост и гъвкавост при реагиране.

Подобряване на междуинституционалната координация чрез ясно дефинирани механизми за споделяне на информация, единни стандарти за анализ и защита на данните, както и регулярни съвместни оценки между политически, дипломатически, военни и аналитични структури.

Повишаване на капацитета за противодействие на хибридни заплахи и дезинформация чрез постоянен мониторинг на информационната среда.

Балансирано използване на технологични решения, като анализ на големи масиви от данни и автоматизирани системи, съчетано със силен експертен и човешки контрол, с цел ограничаване на рисковете от алгоритмични пристрастия и погрешни интерпретации.

Обучение и подготовка на експерти в областта на анализа на информация, управлението на кризи и конфликти, което е предпоставка за ефективното функциониране на всеки модел на информационно осигуряване.

В обобщение на горното се налагат следните изводи:

Информационното осигуряване при управлението и разрешаването на макроконфликти е изправено пред нарастващи предизвикателства, произтичащи от трансформацията на международната среда на сигурност и ускореното развитие на технологиите. Съвременните конфликти се развиват в условията на висока динамика, информационна пренаситеност и целенасочени хибридни въздействия, което поставя нови изисквания към процесите на събиране, анализ и използване на информацията.

Едно от основните предизвикателства пред информационното осигуряване е свързано с бързата дигитализация и нарастването на обема и скоростта на информационните потоци. Дигиталните платформи, социалните мрежи и киберпространството значително разширяват източниците на информация, като едновременно с това усложняват процеса на проверка на достоверността и надеждността на данните. В условията на макроконфликти дигиталната среда се превръща и в поле за активни информационни и психологически операции, което изисква повишен капацитет за мониторинг, анализ и защита на информационните системи.

В перспектива дигитализацията предоставя възможности за по-бърз обмен на информация, по-добра координация между институциите и създаване на интегрирани платформи за ситуационна осведоменост. Реализирането на тези възможности обаче е пряко свързано с нивото на киберсигурност и от способността за управление на рисковете, свързани с цифровите уязвимости.

Използването на изкуствен интелект (ИИ) и технологии за анализ на големи масиви от данни открива нови перспективи за повишаване на ефективността на

информационното осигуряване. Автоматизираният анализ позволява обработката на огромни обеми информация в реално време, откриването на скрити зависимости и ранни индикатори за ескалация на конфликти, както и идентифицирането на дезинформационни кампании. Данните, придобити от открити източници значително разширяват възможностите на анализа и имат съществено значение при различните етапи на управлението на конфликти.

Наред с тези предимства, ИИ поставя и сериозни предизвикателства, свързани с прозрачността на алгоритмите, възможните пристрастия в анализа и зависимостта от технологични решения. Без адекватен човешки контрол и експертна интерпретация, съществува риск автоматизираните системи да генерират неточни или подвеждащи оценки, които да повлияят негативно върху процеса на вземане на решения.

Заключение

В заключение може да се отбележи, че информационното осигуряване представлява стратегически ресурс за управление и разрешаване на макроконфликти. Дава възможност не само за непосредственото управление, но и за изготвянето на прогнози. Неговата ефективност обаче зависи от качеството на информацията, степента на координация между институциите и способността за адаптация към динамичната и хибридна среда за сигурност.

На основата на анализа и добрите практики, като най- ефикасно е прилагането на интегриран модел на информационно осигуряване, инвестиране в човешки и технологичен капацитет, засилване на международното сътрудничество и разработване на ясни етични и правни рамки за използване на новите технологии. Само чрез такъв подход може да се постигне ефективно предотвратяване, регулиране и устойчиво разрешаване на съвременните макроконфликти.

Анализът на причините за възникването на съвременните междудържавни конфликти ясно показва, че ефективното информационно осигуряване представлява необходима предпоставка за адекватното управление и разрешаване на макроконфликти. Интегрираният подход към събирането, анализа и използването на информацията създава условия за ограничаване на ескалацията и за постигане на устойчиви решения в рамките на международната система.

В заключение, ефективното информационно осигуряване, при разрешаването на макроконфликти, изисква системен, координиран и адаптивен подход, който да отчита динамиката на международната среда и нарастващата роля на информационните и хибридните въздействия. Реализирането на посочените препоръки би допринесло за повишаване на качеството на политическите и дипломатическите решения и за ограничаване на рисковете от ескалация на съвременните конфликти.

Литература

1. Галтунг, Й, 2005 Разрешане на конфликти. С. ISBN 954-649-705-3 с. 64
2. Генова, В., 2012 Полиция и социални конфликти. С. НИКК – МВР
3. Гоцев, Г. 2021 Управление при кризи. С. ISBN 978-619-239-543-8

4. Йотова, Р. 2023 Открити източници на информация събиране, класификация и обработка С. ISBN 978-619-185-605-3, с. 145
5. Манев,М., Русева, Р. 2005 Управление при кризи и конфликти ISBN: 954-334-050-2;
6. Недялков, П. 2017 Основи на управлението С. ISBN 978-619-160-754-9
7. Departament za izsledvane na mira i konfliktite kam universiteta v Upsala – Shvetsia https://ucdp.uu.se/.

CULTURAL NATIONALISM AS A POLICY FOR THE PRESERVATION AND SUSTAINABLE DEVELOPMENT OF THE BULGARIAN IDENTITY AND STATESHIP

Petar Givkov, Stoyan G. Stoychev

Abstract: *In their report, the authors examine the connections between cultural nationalism, the security environment, the risks and threats that it poses both to this nationalism and to the erosion of the national identity, the ethnocultural core of our nation. In a broader sense, both the significance and the role of cultural nationalism in upholding, developing and filling with content categories such as language, writing, religion, common history, symbolic system, monuments, heroic pantheon, holidays, folk customs and traditions are presented. Last but not least, the initial thesis of the report is defended that cultural nationalism represents a necessary policy for the preservation and sustainable development of the Bulgarian identity - an active, consciously implemented mechanism for the consolidation of the ethnocultural core of the nation and for the sustainability of the nation.*

Keywords: *Cultural nationalism; National identity; Statehood; Politics: National sustainability.*

КУЛТУРНИЯТ НАЦИОНАЛИЗЪМ КАТО ПОЛИТИКА ЗА ОПАЗВАНЕ И УСТОЙЧИВО РАЗВИТИЕ НА БЪЛГАРСКАТА ИДЕНТИЧНОСТ И ДЪРЖАВНОСТ

Петър Живков[1], Стоян Г. Стойчев[2]

[1]Магистър, кандидат-докторант към катедра „Национална и международна сигурност, факултет „Информационни науки“, Университет по библиотекознание и информационни технологии (УниБИТ), София, България,
E-mail: piterjivkov@gmail.com
[2]Професор в катедра „Национална и международна сигурност, факултет „Информационни науки“,
Университет по библиотекознание и информационни технологии (УниБИТ), София, България,
E-mail: s.stoychev@unibit.bg; sstoychev_ss@abv.bg

Резюме: *В доклада си авторите разглеждат връзките между културния национализиъм, средата за сигурност, рисковете и заплахите, които тя носи както за този националзиъм, така и за ерозия на националната идентичност, на етнокултурното ядро на нацията ни. Представено е в един пои-широк смисъл както значението, така и ролята на културния национализъм за отстояване, развиване и изпълване със съдържания на категории като език, писменост, религия, обща история, символна система, паметници, героически пантеон, празници, народни обичаи и традиции. Не на последно място е защитена началната теза на доклада, че културният национализъм представлява необходима политика за опазване и устойчиво развитие на българската идентичност - активен, съзнателно провеждан механизъм за консолидация на етнокултурното ядро на нацията и за устойчивост на нацията.*

Ключови думи: *Културен национализъм; Национална идентичност; Държавност; Политика: Национална устойчивост.*

Въведение

В условията на динамична и непредсказуема международна среда, белязана от процесите на глобализация, технологични трансформации и нарастваща геополитическа нестабилност, въпросът за националната устойчивост придобива нови и все по-важни измерения. Сред множеството фактори, определящи стабилността и жизнеспособността на съвременната държава, културно-историческото наследство (КИН) заема особено място - не като пасивен обект на опазване, а като активен стратегически ресурс.

Настоящото изследване защитава тезата, че културният национализъм представлява необходима политика за опазване и устойчиво развитие на българската идентичност - активен, съзнателно провеждан механизъм за консолидация на етнокултурното ядро на нацията. За разлика от политическия национализъм, съсредоточен предимно върху държавните институции, властта и границите, културният национализъм извежда своята същност от органичната връзка, поддържаща общността жива във времето - език, писменост, религия, обща история, символна система, паметници, героически пантеон, празници, народни обичаи и традиции. Именно тази органична връзка го превръща в жизненоважен инструмент не само за опазване на българската идентичност, но и за самата устойчивост на българската държавност, доколкото институционалната цялост на всяка държава в крайна сметка се опира на съществуването на консолидирана, себепознаваща се и себеорганизираща се нация.

Методология

При изготвянето на своя доклад автортите са използвали системният подход, като най-подходящ за изследване на взаимосвързани и сродни дейности. Реализирането на доклада е постигнато и с използването на методите на литературния обзор, на изследванията и сравненията, на системния анализ, на теоретичните изследвания, историческия метод, както и с използването на системния анализ.

Резултати

Правейки връзка с въведението на доклада, можем да посочим като продължение, че актуалността на тезата произтича пряко от конкретните предизвикателства, пред които е изправена българската държава днес - демографска криза, продължаваща емиграция и имиграция, засилващи се опити за исторически ревизионизъм, натиск върху българската езикова, историческа и етническа идентичност. Именно в отговор на тези предизвикателства културният национализъм се явява не просто защитна реакция на миналото, а активна, ориентирана към бъдещето политика за устойчиво развитие на нацията и държавата.

Понятието или терминът „културен" в концепцията за „културен национализъм" се използва в настоящето изследване в смисъл, различен от обичайната му, ежедневна употреба, приета малко на готово от английският език, тоест, от английското значение на терминът „културен"[2] – авторите дават своя принос като представят в изследването терминът „културен" в чисто българският му прочит и аспекти, а именно: Българският термин „културен", покрива в тесния си, битов смисъл само едната страна на културата, от което произлиза реално – сгради, архитектура, изкуство, естетика, музика, литература, навици, традиции, причвички на живот (съвкупността от материалната, духовната и социалната култура), докато „историческо", „етническо" и „религиозно" остават самостоятелни категории.

От друга страна, изразът „културен национализъм", който се използва в настоящото изследване, „културен" следва вече и по-широката съставна на българската логика: включва в неразделно единство език и писменост, историческа памет и приемственост на етноса, духовна и религиозна традиция, държавнотворчески опит и героически пантеон - съставки, които английското "cultural" побира по подразбиране, тоест, в една единствена дума, а българската традиция изговаря и съзнава поотделно. Именно това изрично назоваване на всяка съставна част превръща българския културен национализъм в съзнателно артикулирана защитна система обхващаща едновременно опазването, консолидацията и устойчивото развитие на българската идентичност и държавност.

Същност, цели и принос на културния национализъм.

Произходът на културния национализъм като теоретична категория е тясно свързан с етносимволистката школа в изследванията на национализма, разработена от Антъни Д. Смит (Anthony D. Smith). Според тази концепция съвременните нации не са просто модерни политически конструкции, а стъпват върху предварително съществуващи етнически ядра (*ethnie*) - общности, обединени от споделени митове за произход, обща история, културни практики, език и връзка с конкретна територия. Доразвивайки тази традиция в своя фундаментален труд „Динамиката на културния национализъм", Джон Хътчинсън (John Hutchinson), посочва ключова разлика между културния и политическия национализъм: докато политическият национализъм се стреми към граждански права и държавни институции, културният национализъм преследва вътрешно себепознание и духовно обновление на общността, разбирана не като механичен сбор от граждани, а като етническа, морална и историческа общност с уникален цивилизационен профил. Комбинация, която според него се дава или носи от т.нар. ***морални иноватори*** – художниците, писателите, историците, поетите, лингвистите, тоест, от интелигенцията.

[2] Английското "cultural" носи широк, антропологически смисъл - то обхваща практиките, ценностите и историческата памет на общността в едно, единно понятие, без нужда от отделна дума за "историческо".

Оттук произтичат и конкретните цели на културния национализъм: ***съхранение на езика и историческата памет като носители на националното самосъзнание, изграждане на устойчива социална кохезия чрез споделени културни кодове и символи, и защита на когнитивния и културен суверенитет на нацията пред нарастващия натиск за унификация в условията на глобализация и дигитална трансформация.***

Механизмът, чрез който подобно себепознание исторически прераства в масово движение, е прецизно описан от Мирослав Хрох (Miroslav Hroch) в книгата му „Социални предпоставки за националното възраждане в Европа", в която той излага своя модел на трифазовото национално възраждане, приложим пряко за Централна и Източна Европа. Моделът очертава последователност от начална фаза на научно и антикварно любопитство към езика и историята, през фаза на патриотична агитация, до формирането на масово национално движение. Българското Възраждане следва почти буквално тази логика - от филологическия и историографски устрем на ***будителите***, през борбата за просвета и църковна независимост, до масовото националноосвободително движение.

Основният принос на културния национализъм, изведен от тази теоретична основа, е изграждането на устойчива платформа за колективна принадлежност - усещане за общност, простираща се отвъд индивидуалния живот и отвъд текущия политически конюнктурен момент. Езикът, историческата памет, символите и героическият пантеон изграждат фундаменталната емоционална инфраструктура на нацията. Когато гражданите споделят общи културни кодове и памет, нивото на взаимно доверие и социална кохезия нараства, превръщайки нацията в устойчива система срещу вътрешни разделения и външни кризи.

Практическото изражение на този принос личи ясно в конкретни държавни практики. Полша предлага показателен пример за институционализирана политика на паметта. След 1989 г., и особено чрез дейността на Института за национална памет (IPN), полската държава активно финансира изследването, документирането и общественото почитане на исторически фигури и събития, свързани с националното съпротивление. В същия контекст литературното наследство на полското Възраждане, въплътено в творчеството на Адам Мицкевич, продължава да служи като жив символен ориентир за нацията - пряк паралел с ролята, която Христо Ботев и Иван Вазов играят в българската национална памет.

Израел представлява още по-категоричен пример за съзнателно и целенасочено културно-национално изграждане. Възраждането на иврита като говорим, всекидневен език - дело, свързано преди всичко с усилията на Елиезер Бен-Йехуда в края на XIX и началото на XX век е класически пример в изследванията на национализма за това как един предимно литургичен език може да бъде превърнат в жива основа на модерна идентичност. Институции като „Яд Вашем" и централното място на паметта за Холокоста в държавния наратив демонстрират как историческата памет може да бъде пряко институционализирана в служба на националната кохезия и оцеляването на държавността.

Предизвикателства и рискове пред културния национализъм.

Утвърждаването на културния национализъм като необходима политика за опазване на идентичността не се случва в неутрална среда. Напротив той е изправен пред редица обективни предизвикателства, рискове и заплахи, идващи както отвън, така и отвътре - от самото общество, застрашаващи основите, върху които тази политика стъпва: езика, историческата памет, институциите и обществения консенсус.

Външни заплахи

Основната външна заплаха произтича от глобализационно-технологичния натиск към културна унификация. Глобалните платформи и алгоритмичните механизми за подбор на съдържание налагат универсализирани културни модели и езикови съкращения, еродиращи локалните исторически контексти, върху които се крепи именно онази „емоционална инфраструктура на нацията", разгледана по-горе в доклада.

Тази заплаха се проявява и в по-остра, целенасочена форма: опити за исторически ревизионизъм намират в дигиталната, алгоритмично фрагментирана информационна среда особено благоприятна почва за разпространение. В условията на затворени „информационни балони" ревизионистки и деформирани версии на историята достигат до значителна аудитория без възможност за своевременна научна проверка, подкопавайки директно споделения фонд от факти и памет, върху който културният национализъм изгражда цялата своя защитна функция.

Вътрешни заплахи

Най-осезаемата вътрешна заплаха е демографската криза. Ниската раждаемост, застаряването на обществото и продължаващата емиграция на активното население пряко подкопават живата основа, върху която стъпва културният национализъм. Той разчита на възпроизвеждащата се общност, предаваща език, обща памет и традиции между поколенията. Тази вътрешна демографска ерозия има и своя външна проекция: значителна част от българската нация вече живее извън пределите на държавата, изложена на постепенен асимилационен натиск от приемащите общества - риск, чието овладяване изисква активна и последователна държавна политика към диаспората.

Успоредно с демографската криза действа и недостатъчният институционален и финансов ресурс, отделян за опазване на културно-историческото наследство, езиковата политика и просветната инфраструктура - фактор, пряко ограничаващ капацитета на музеите, архивите, читалищата и училищата, натоварени практически с пренасянето на българския идентичностен код между поколенията, а и с възпитаването на подрастващите в националните традиции, ценности, морал.

Най-съществена сред вътрешните заплахи остава политическата инструментализация, произтичаща от собствената дълбока афективност на културния национализъм - именно защото борави с категориите на идентичността и паметта, той лесно се превръща в обект на присвояване от политически актьори за постигане на тесни партийни цели. Когато историческата памет и символният апарат бъдат монополизирани от една политическа класа, чийто представители

(една част от тях все пак) нямат пряко отношение към българската идентичност и културният национализиъм и използват тези категории (историческа памет и национални символи) като оръжие срещу вътрешнополитически опоненти, вместо да служат на цялата нация, културният национализъм губи именно онова качество, което вече определихме, като негов основен принос - способността да обединява, а не да разделя. Това изкривяване носи двойна опасност: поддържането на взаимно изключващи се версии за историята и героическия пантеон разгражда обществената кохезия отвътре, а неправилно приложен, културният национализъм може да се изроди в изключващ наратив спрямо малцинствените общности в страната, вместо да насърчава модел на интеграция и съвместно съществуване. Към тези рискове и заплахи се добавя и комерсиализацията на наследството - натискът за бърза печалба в туристическия и медийния сектор често свежда дълбочината на културно-историческото наследство до повърхностен кич, подменяйки истинското себепознание с псевдопатриотичен - консуматорски подход.

Именно тези кумулативни рискове и заплахи - вътрешни и външни, правят въпроса за устойчивото, отговорно провеждане на политика за културен национализъм не просто актуален, а неотложен, доколкото самото бездействие пред тях би означавало постепенна загуба на онзи принос, който посочихме по-горе – при същността и ролята на културния национализъм. А както видяхме, той е жизненоважен за нацията и държавността. Именно на този въпрос за устойчивостта и отговорността при проявеждане на политиката в тази посока са посветени част от изследванията, които авторите представят по-надолу в доклада си.

Устойчиво развитие на културния национализъм

Заплахите, разгледани в предходния раздел, не отменят необходимостта от културен национализъм като политика - напротив, именно пред лицето на демографската криза, институционалния недостиг, риска от политическа злоупотреба и дигиталната фрагментация на паметта, въпросът за неговото устойчиво, отговорно провеждане става още по-неотложен. Настоящият раздел разглежда конкретните основи и механизми, чрез които тази политика може да бъде провеждана градивно и в синхрон с утвърдените европейски практики.

Културно-историческото наследство като стратегически ресурс

Устойчивото развитие на културния национализъм изисква преди всичко разбиране на самото културно-историческо наследство. Да изградим разбиране към него не като статичен, музеен обект на пасивно опазване, а като активен стратегически ресурс. Тази позиция премества акцента от чисто консервационна логика (опазване на паметника заради самия него) към функционална логика (наследството като действащ фактор за устойчивостта на нацията и държавата), без при това да намалява грижата за автентичността и научната коректност на самото опазване.

Стратегическата стойност на наследството произтича именно от неговата двойна функция, разгледана в предходните раздели: то е едновременно носител на историческата памет, консолидираща нацията отвътре, и защитен буфер срещу

външния натиск за унификация и вътрешния риск от фрагментация. Инвестицията в дигитализация, поддръжка и активна популяризация на музеи, архиви и читалища следователно не е второстепенен разход, а пряка инвестиция в самата устойчивост на държавата - насока, особено релевантна предвид институционалния недостиг, установен като риск в предходната част на доклада.

Европейски политики и Рамковата конвенция от Фаро (2005)

Провеждането на политика за културен национализъм не противоречи на съвременните европейски практики - напротив, то намира пряка нормативна подкрепа в международни документи на Съвета на Европа. Рамковата конвенция за стойността на културното наследство за обществото (Фаро, 2005) признава всички форми на културно наследство като споделен извор на памет, разбирателство, идентичност и социална кохезия, а член 7 от конвенцията изрично призовава страните да развиват знанието за културното наследство именно като ресурс, улесняващ мирното съвместно съществуване чрез насърчаване на доверие и взаимно разбирателство.

Конвенцията добавя и съществено уточнение, което пряко подкрепя разграничението, направено по-горе в доклада между градивна и изключваща употреба на културния национализъм: тя настоява територията и общността да се разбират като място на срещи между култури, а не като затворена, изключваща цялост. С други думи, международната нормативна рамка не просто позволява защита на националната идентичност чрез културно наследство - тя изрично изисква тази защита да бъде провеждана по начин, съвместим със социалната кохезия и мирното съвместно съществуване, а не в противоречие с тях. Именно защото Конвенцията от Фаро едновременно легитимира защитата на националната идентичност чрез културно наследство и поставя граница пред нейната евентуална злоупотреба, тя се превръща в естествена нормативна опора за тезата на настоящото изследване.

Механизми за устойчива и приобщаваща практика

От съчетаването на стратегическото разбиране за наследството и нормативната рамка на Фаро произтичат конкретни насоки за устойчива практика. Гражданите и местните общности следва да станат преки участници в опазването на паметта, а не пасивни получатели на веднъж отгоре зададен наратив - подход, който едновременно засилва автентичността и обществената легитимност на самата политика и намалява риска от политическа монополизация, посочен като вътрешна заплаха в настоящото изследване. Образователната и просветната политика, насочена към младото поколение, остава основният канал за предаване на националния код между поколенията, а активната държавна грижа за българските общности зад граница - чрез учебни програми, културен обмен и достъп до образование в България - директно противодейства на демографската и асимилационната заплаха, установена по-рано.

Демографската динамика на съвременна България включва и обратния на емиграцията процес - нарастващи имиграционни потоци, включително трудова миграция от Азия и бежански вълни от Африка и Близкия изток. Тази динамика поставя пред политиката за културен национализъм отделен, различен по природа

въпрос от вътрешната демографска криза: не свиване на общността, а темпото и капацитета за интеграция на новопристигналите в рамките на съществуващата културна и езикова идентичност. Когато темпото на имиграция надхвърля реалния капацитет на образователната система, езиковата политика и социалните институции за пълноценна интеграция, рискът не е самата демографска промяна, а възможната фрагментация на общото езиково и културно пространство, върху което кохезията, разгледана в началото на доклада, разчита. Тук отговорът, съвместим с приобщаващия модел, установен по-рано в изследването, не е отхвърляне или изключване, а активна интеграционна политика, гарантираща, че новите граждани стават реални участници в общата културна и езикова рамка, а не паралелна, несвързана с нея общност.

Устойчивото развитие на културния национализъм в крайна сметка изисква баланс между два привидно противоположни императива - твърдата защита на националната идентичност и приемствеността, и отвореността към диалог и съвместно съществуване с други общности и култури. Именно в поддържането на този баланс, а не в избора на единия за сметка на другия, се крие разликата между културен национализъм като градивна политика и неговото израждане в изключваща идеология, разгледано също в изследването, макар и не достатъчно задълбочено.

Заключение

Защитавайки тезата, че културният национализъм представлява необходима политика за опазване и устойчиво развитие на българската идентичност не е отживелица или носталгично отклонение от неизбежния ход на глобализацията, а активен, съзнателно провеждан механизъм за консолидация на етнокултурното ядро на нацията, чиято стойност нараства, а не намалява, пред лицето на съвременните предизвикателства, авторите на настоящото изследване са убедени, че страната ни има и възможности, а и политичесдка воля (поне в някои от политическите сили, които имат доста ясна и видима подкрепа от народа на България на настоящия етап от развитието ни) и е въпрос на време тази важна политика – полтиката на културен национален, да бъде поставена недвусмислено и категорично на дневен ред. Да се развие тази политика и предвид, но не само, провеждането на конкурсът Евровизия в страната ни през предстящата 2027 година – да се използва обаче този импулс, когато страната ни ще бъде посетена от много повече туристи от една „нормална“ година, от много повече от нормалното страни и да се засили в годините напред. Защото страната ни определено има какво да покаже на света, на Европа, и да намери още по-добре, и по още по-достоен начин своето място сред нациите дали културен тласък, а и принос за развитие на обществата в региона ни, а и в Европа като цяло.

Чрез съчетаването на етносимволистката концепция на Антъни Смит (Smith), разграничението на Джон Хътчинсън (Hutchinson) и модела на националното пробуждане на Мирослав Хрох (Hroch), изследването изведе основния принос на културния национализъм - изграждането на устойчива платформа за колективна принадлежност, онагледена и чрез практиките на Полша и Израел. Важно е да се

подчертае, че думата „културен" в израза „културен национализъм" не се отнася само до изкуство и естетика - тя носи в себе си много повече, както беше изяснено, а обхваща в неразделно единство език и писменост, историческа памет, етническа принадлежност, духовна и религиозна традиция, и държавнотворчески традиции и опит.

Изследването посочва обаче и част от предизвикателствата, рисковете и заплахите пред тази политика: демографската криза, институционалния недостиг, риска от политическа инструментализация и комерсиализация, глобализационно-технологичния натиск и алгоритмичната фрагментация на историческата памет. Тези рискове и заплахи обаче не отслабват, а засилват аргумента в полза на съзнателно провеждана политика на културен национализъм. Колкото повече основите на националната идентичност са застрашени, толкова по-необходима става тяхната защита.

Устойчивото развитие на тази политика, изисква разбиране на културно-историческото наследство като активен стратегически ресурс, а не пасивен обект на опазване - разбиране, намиращо пряка нормативна опора в Рамковата конвенция на Съвета на Европа от Фаро (2005), която едновременно легитимира защитата на националната идентичност чрез културно наследство и поставя границата пред нейната злоупотреба: територията и общността като място на срещи между култури, а не като затворена, изключваща цялост. Именно в поддържането на този баланс - твърда защита на идентичността, съчетана с приобщаваща, а не изключваща практика се крие бъдещето на българския културен национализъм като жизнеспособна и легитимна политика.

Пред България, в настоящият сложен, намиращ се в преход Свят, предстои да намери собствения си, устойчив път в тази посока - път, който съчетава активна грижа за езика, историческата памет и диаспората у нас и по света, с институционална и финансова инвестиция в наследството като стратегически ресурс, и с осъзнатост към собствените вътрешни рискове от политизация и изключване. Културният национализъм, разбиран и провеждан по този начин, остава не просто защита на миналото, а активна, ориентирана към бъдещето политика за устойчивото съществуване на българската нация и държава в 21ви век.

Литература:

1. Мащаби на демографската криза в България и Европа. [viewed 01 September 2026]. Available from: https://www.iki.bas.bg/english/CVita/angelov/No277.htm
2. Смит, А., 2000. Националната идентичност. София: издателство Кралица Маб.
3. Рамкова конвенция за съвета на европа зазначението на културното наследство за обществото, Фаро, 2005. [viewed 01 September 2026]. Available from: https://seecorridors.eu/filebank/file_1014.pdf
4. Cultural: 1. relating to the habits, traditions, and beliefs of a society; 2. relating to music, art, theatre, literature, etc.: 3. of or referring to the way of life of a

particular people, esp. as shown in their ordinary behavior and habits, their attitudes toward each other, and their moral and religious beliefs; 4. of or referring to the literature, art, music, dance, theater, etc., that represent the traditions or the way of life of a particular people or group. [viewed 01 September 2026]. Available from: https://dictionary.cambridge.org/dictionary/english/cultural

5. Hutchinson, J., 1987. The Dynamics of Cultural Nationalism. London: Publisher Group Routledge – Taylor and Francis Group.
6. Hroch, M., 1985. Social Preconditions of National Revival in Europe. Cambridge: Cambridge University Press.
7. Timeline of Polish History. [viewed 02 September 2026]. Available from: https://eng.ipn.gov.pl/en/brief-history-of-poland#1795-1918

ARCH SYNDROME AND CRITICAL THINKING IN A MILITARY ENVIRONMENT

Viktor T. Dobrev

Department of „Radar and communication systems" Faculty of Artillery, Air Defense and CIS, Vasil Levski National University of Science and Technology, Shumen, Bulgaria

Abstract: *The current problems related to the training of cadets in military schools and cognitive dissonance in relation to training in critical thinking in a military environment are examined. The etiology of the observed phenomenon and its development are described. The characteristics of the ARCH syndrome formulated in the allied armies of the alliance are presented. With the main adaptation forms for the implementation of the training*

Keywords: *critical thinking, concept of knowledge in a military environment, the ARCH phenomenon*

СИНДРОМА „ARCH" И КРИТИЧЕСКОТО МИСЛЕНЕ ВЪВ ВОЕННА СРЕДА

Виктор Т. Добрев

катедра „Радарни и комуникационни системи" факултет „Артилерия ПВО и КИС" на НВУ „Васил Левски" гр. Шумен, България

Резюме*: Разглеждат се актуалните проблеми свързани с обучението на курсанти във военните училища и когнитивният дисонан, спрямо обучението във критично мислене във военна среда. Описана е етиологията на наблюдавания феномен и неговото развитие. Представени са характеристиките на синдрома ARCH формулиран във съюзническите армии на алианса. С основните адаптационни формиза реализирането на обучението.*

Ключови думи*: критическо мислене, понятие за познание във войска среда, феномена ARCH*

„Критика" произлиза от гръцкото κρΐνω (krīnō) да различаваш, отбираш, съдиш, решаваш.

Критиката е изкуството да се извеждат съждения и това неизбежно поражда противоречия и разногласия в йерархията на всяка организирана структура. В съвременната артикулация тя се свързва негативна анотация. По-развитата форма на интерпретация е свързана с обяснение на каузалност и така се появяват предпоставките на анализа. В литературата критиката се интерпретира като коментар, обзор, оценка. В професионалната област се свежда до спазването на правила и схеми. В този ракурс „критика" се проявява като граници на нещо на фона на общото — полемика насочена към обект представен през съждения и съотнесен към съществуващото положение. Критиката не е скрупулизно мрънкане и никога не може да се определи като грубост – тя е излагане на алтернативна

аргументация на основа доказателства и логика. Сама по себе си тя разпознава какво е действено и функционално и какво не.

Критическото мислене е необходима предпоставка за критиката, но само тя е в състояние да променя организацията. Това се случва в структури, където критиката се поощрява в посока от „долу нагоре" – търсят се т нар. „предприемачи на нормите" или „програмни актьори" които задвижват процеса на иновациите и променят професионалните общности. Този тип хора интерпретират събития, формират дискурс, конструират нов консенсус. Принципно бюрокрацията изисква стандартизация и без установен процес за промяна, автоматично няма място за критика на съществуващия ред.

Широко разпространение има мнението, че военните организации са слабо ориентирани към иновации поради факта че са ориентирани към процедурите, оказват съпротива към промените и се обучават бавно – неща, които са характерни за всяка бюрократична система. Прилагането на иновации във военна организация определено дават възможност за постигане на преимущество по време на война – показателно е поведението на Украйна в текущия конфликт.

Отчитайки потенциала на подобен вектор кара военните организации в мирно време да инвестират огромни средства за постигането на по-добра организация и образователни реформи, създавайки нови институти и структури във военните университети за генериране на иновации струващи огромни финансови средства. В същия момент масово е мнението, че военните структури са индиферентни към иновации и адаптация към новите реалности. Неуспехът на военните организации по отношение на иновациите се крие в бюрократичната инерция, липсата на покритие по отношение на аксиологичния потенциал на войнската доблест с характера на конкретните иновации, липсата на обучение и влиянието на войнската култура и идентичност в различните видове въоръжени сили.

Неоспорим факт е, че проявата на критично мислене от страна на офицер може да му докара проблеми в кариерното развитие и формирания вече стереотипен критерии за „качествени знания" при подготовката. Друг интересен факт е, че повечето методологични изследвания се градят на единични случаи на иновативен скок на някой велики армии – липсата на Крос културно корелации пречи на изследването причинните фактори за проблематика по отношение на иновации.

Най-рационалното и прагматично обяснение на феномена се крие в „идеала за знание" движещ се около формулировката ARCH, който е акроним на четири взаимносвързани склонности: action, relevance, conflict, hierarchy – стремеж към действие, целесъобразност, конфликт и йерархия работещи синергично в посока на смислообразуващ механизъм създаващ роли и отношения между различните понятия и категории на знанията във военната сфера.

Феноменът ARCH демотивира критиката идваща отдолу, затормозява алтернативните представи за бъдещето на войната и критичното мислене като ефективен начин за самоактуализация отвътре на военната организация. Задължително трябва да отбележим непреднамереността на създаването и функционалността на идеала за познание във военните организации. Феноменът ARCH функционира върху определено разбиране за войната, където критичното

мислене се възприема, като страничен ефект от опитите да се оптимизира военната организация под някаква определена версия за реалното военно действие. В случая сработват някой нематериални фактори регламентиращи критичността като пречка на основата на властовите отношения и кариерата в условия на бюрократичен режим.

Как ARCH потиска критическото мислене?

Въпреки липсата на преки или двусмислени забрани за потискане на критическото мислене в такава тенденция е очевидна. Най-ясно видима е в устава FM 3 0 на сухопътните войски на САЩ (аналогично и в повечето европейски доктрини). И двете системи императивно се изградени на йерархията. Израстването в кариерната стълбица е свързано с прогресивно свиване на мисловната рамка и нарастване на четирите функционални дименсии на ARCH, които възпрепятстват критичното мислен.

Първият фактор това *склонността към действие* – то е за предпочитане пред това да си прав. Военната организация разглежда знанията за войната като нещо изискващо действие. „Офицерът е мениджър на организираното насилие". Приоритетът е върху оперативната и бойна подготовка спрямо образованието, инструктажите пред семинарите, като се фаворизира личния опит.Нерешителността се възприема като главен проблем:

Американската армия заявява, че „подредената инициатива изисква склонност към действие" (FM 3 0). Доктрината на някой европейски армии провъзгласява, че „нерешителността е по-лоша от погрешно действие". Всички принципи на войната наблягат на решителността. Пристрастието към действие потиска критичното мислене и легитимира грешките, стига да се предприемат действия. Скоростта в OODA цикъла (т.нар. цикъл на Бойд или управленски цикъл) се счита за по-важна от неточността. Западните армии са обсебени от идеята, че „бързината печели".

Вторият компонент на ARCH е ц*елесъобразността* – всичко трябва да се случва „тук и сега". Този компонент лежи на разбирането за това, че „се прави всичко необходимо за настоящата и бъдеща война" на основата на йерархичността и действието. Това е самостоятелен ключов механизъм в разбирането за познание във военната организация. Доктрината за целесъобразност е безалтернативна поради факта, че никоя друга не може да обхване всички възможни начини за водене на война – съвременната война отдавна се е сбогувала с идеята за фронтове и завземане на територии, като продукт на рефлексивното мислене и се гради на мрежово-центричната концепция изискващо дивергентно критическо мислене.

Удобство предизвиква и факта, че целесъобразността не изисква допълнително обосноваване и мотиви, с което намалява дълбочината и далновидността на мисленето изобщо – западните доктрини категорично заявява: „концепциите изложени тук не са само ръководство за водене на боя, а и начин на мислене" (US Marine Corps, 2018). Самата целесъобразност несъзнателно се възприема като нещо добро и важно за познаването на „текущата война" и усилва склонността към действеност.

Целесъобразността обаче блокира избора на конкуриращи се идеи и алтернативи – едно от изискванията за качествено знание е наличието на

рефлексивност и критика. В случая има приоритет на целесъобразността спрямо качеството от една страна, а едновременно с това се усилва и йерархизацията поради факта че командващия определя целесъобразността в дадения момент. Схемата на доминиране и подчинение изглежда полезна при вземането на решения и всяко знание се гради на действия – оттам и „не всеки има право на съждения".

Консервативният статус на целесъобразността се самопрезентира като единствен арбитър във военната организация затваряйки я за всякакви алтернативни перспективи.

Третият компонент на ARCH е *склонността към бивалентност*, а оттам и конфликтност. Тук противопоставянето се разбира в аксиоматичното в координатите на „ние и те". В западните концепции се цитира Клаузевиц с идеята му за войната като „акт с използване насила, за да се наложи на противника нашата воля" (Clausewitz, 1993). Така войната се възприема не като нещо включващо абстрактни актьори, а като противоборство между „ние" и „те". Самото мислене за войната автоматично включва мислещия като участник в нея – нещо, което унищожава рефлексивността и обективността на процеса. Критиката на воюващите и критическо мислене се отдават много по-лесно на човек, който е безпристрастен наблюдател. Западните доктрини акцентират върху йерархизацията на документите регламентиращи дейността на военните организации – стратегическите документи дават структурата и съдържанието на оперативните, а те от своя страна доктринално определят видовете въоръжени сили и вертикалите на тяхното управление.

Участието във война изисква организация и на Запад това изисква някаква форма на стандартизация - типа структури (корпуси, дивизии, бригади, батальони, роти, взводове, отделения). Стандартизацията укрепва управленческите вертикали. В тях задължително съществуват отдели за разузнаване и материално-техническо обезпечаване, но никога „отдели за критика"

Прегрупирането „по време на война" се поставя в прерогативите на по-старшите да вземат подобни решения, а самата война се свежда до воденето на бой по-остарялата формулировка на Клаузевиц: „войната по своята същност е водене на бой, тъй като той е единственият решаващ акт на многообразието на дейностите покриващи разбирането за войната".

Тази формулировка не предполага критическо мислене и критика, защото боят е свързан с дефицит на време и опасности изискващи подчинение и бързина, а не рефлексия и критика. Намирайки се във „врящия котел" на войната прави невъзможността да се абстрахираш без юридически последствия от неизпълнение на решенията на началника.

Оттам произтича и четвъртата склонност в концепцията за знание във военната организация – това е *йерархизацията.* Йерархическият връх решава кое е знание и може да определя неговото качество. Във всяко едно западно ръководство авторитетно се завява, че изложеното по-долу определя как трябва да се организира, мисли и действа на по-ниските нива. Генералите също призовават да се обсъждат доктрините, но налагат предварително рамка на допустимото мислене.

Вместо приемането на знанието като предмет на разширяване свързано с колегиално обсъждане, условно приемане и непрекъснати дискусии военните организации обвързват качеството на знанията с йерархия. Това отново опира до транслацията на доктрини, където опирайки се Клаузевиц постоянно се подчертава напрегнатостта и неопределеността на войната. Решенията трябва да се вземат въпреки това и всичко се случва през властта на пълномощията – военното звание определя кое е истина и кое не е!

Според Йенсен (Jensen 2016) търсенето на консенсус се случва не през търсенето на „правилно предсказана будеща теория на победата", а в търсенето на съгласуваност на версията. Така, каквато и да е реформа съдържаща „теория на победата" не зависи от истина – тя е непостижима, защото зависи от логика и емпирия, а на практика се води от легитимност и власт. Командващият решава кое е истинско знание приемайки, че то може да бъде окончателно: „Всичко вече е казано и точка!"

Йерархичността в разбирането на знанието предполага също така, че прогреса се гарантира от процеса, а не от резултата – акцента пада върху управлението и потискане на дискусионността. Това води до предрешеност на резултат. Такова мислене укрепва доминацията и подчинението. В тази ситуация винаги възниква въпроса „Кой ви даде право, да говорите или питате това?". Според публикация на Грисом от 2006 година военните структури се втвърдяват и закостеняват върху стари доктрини за воденето на войната от близкото минало, вместо да проявят футуристична визия как би изглеждала тя в бъдеще. По този начин се засяга една от основните стратегически формулировки заемащи академичната подготовка с теоретична преработка и емпирични данни.

Коен и Гуч (1991) анализирайки действията на британското командване през Първата световна война, остро критикуват отсъствието на критично мислене:

„Покорното послушание на подчинените на Хейг, доведе до това офицерите от средно ниво да предприемат настъпление без тактически или стратегически усет, независимо дали вярват в това, което правят или не, следвайки заповеди, те можеха да разчитат на повишение; ако постъпват иначе, със сигурност ще бъдат уволнени и опозорени".

Друг важен момент е възприемчивостта на организацията към иновации – изследванията показват, че дори да се появи нова „теория за победата" от страна на критиците то реформата може да се случи единствено при подкрепата на „мрежовите медиатори". Военната организация не трябва да е „функционално глупава" и да е отворена за критика.

„Функционално глупавата" организация не умее да използва рефлексивните си и когнитивни способности оставайки глуха към критическо мислене и обявявайки като несъстоятелни въпросите, които не са референтни.

Стандартният аргумент за организационната инерция се аргументира със смисъла на военната организация да решава определен проблем и сблъсъкът и с тези, които искат да се справят с нея. Самата организация в своя смисъл предполага устойчивост и консерватизъм на процесуалност и развитие, т. е. „проектирана е да не се променя". Големите структури формират устойчиви

навици достигащи до стандартизацията им и това неизбежно води до съпротива срещу измененията (Jensen, 2016). Прецедентът се издига в култ, като защита на собствените им прерогативи награждаващи навиците и знанията придобити при управлението на „старата машина". Обратно, критическото мислене създава възможности за иновации, защото провокира създаване на алтернативни артикулации на съществуващия ред. Това се случва изключително и само ако има рефлексивно мислене и детайлно разпознаване на текущата ситуация.

В алтернативните системи системи се разчита на „индивидуални хийтове или доктринални реформи свързани с „инкубатори" или „мрежови медиатори". В така наречените инкубатори на офицерите специално се възлага да мислят и разсъждават върху бъдещето на войната и да създават релевантни „теории за победата". Получавайки заповед да мислят свободно те заобикалят организационния натиск и „заинтересованите" структури, които могат да ги накажат за идеите не съвпадат с интересите на отделните подразделения. Британският генерал Рупард Смит признава, че се налага промяна в офицерския корпус:

„Това ще изисква подбор на хора с интелигентност и способност за иновации при неблагоприятни условия – вместо „действащите", които толкова често са обект на институционални системи за подбор, особено в армиите за „индустриална война"... Сега се нуждаем от новатори – умни, практични, находчиви и смели, способни да действат успешно при нови обстоятелства".

Достатъчен е бегъл поглед върху процедурите за планиране, за да се види как се предписва определен начин на мислен и се убива всеки порив за търсене на алтернативи. Онтологическата безопасност се гарантира през статуса на командващия като арбитър на истината. В доктрините изрично се подчертава критическото значение на командирските качества. Колкото по-дебело се подчертава значението на командирските качества, толкова повече се потиска критическото мислене – командирските качества автоматично се подкрепят от модела на доминиране и подчинение, даващи отговор кой трябва да определя кое е истина.

Използвана литература:

1. Alvesson, M., & Spicer, A. (2012). A stupidity-based theory of organizations. Journal of Management Studies, 49(7), 1194–1220. https://doi.org/10.1111/j.1467-6486.2012.01072.x
2. Angstrom, J., & Widén, J. J. (2015). Contemporary military theory: The dynamics of war. Routledge. https://doi.org/10.4324/9780203080726
3. Borell, K. (2004). Disciplinära strategier (2nd ed.). Militärhögskolan.
4. Boyd, J. R. (1987). A discourse on winning and losing [Unpublished briefing]. Air University Library, Maxwell Air Force Base. https://www.colonelboyd.com
5. Builder, C. (1989). The masks of war: American military styles in strategy and analysis. Johns Hopkins University Press.
6. Echevarria, A. (2014). Reconsidering the American way of war. Georgetown University

7. Farrell, T. (2005). The norms of war. Lynne Rienner. https://doi.org/10.1515/9781626370173
8. Farrell, T., Rynning, S., & Terriff, T. (2013). Transforming military power since the Cold War: Britain, France, and the United States, 1991–2012. Cambridge University Press. https://doi.org/10.1017/CBO9781107360143
9. Farrell, T., & Terriff, T. (Eds.). (2002). The sources of military change: Norms, politics, technology. Lynne Rienner. https://doi.org/10.1515/9781588261793
10. Finkel, M. (2011). On flexibility. Stanford University Press. https://doi.org/10.1515/9780804777155
11. Jensen, B. M. (2016). Forging the sword: Doctrinal change in the U.S. Army. Stanford University Press.
12. Jan Ångström „Criticism and Knowledge Ideals in Military Organizations" „Scandinavian Journal of Military Studies" 8 (1), January 2025
13. Jensen, B. M. (2018). The role of ideas in defense planning: Revisiting the revolution in military affairs. Defence Studies, 18(3), 302–317. https://doi.org/10.1080/14702436.2018.1497928
14. Jones, S. G., McCabe, R., & Palmer, A. (2023, February). Ukrainian innovation in a war of attrition. CSIS Briefs.
15. Kier, E. (1997). Imagining war: French and British military doctrine between the wars. Princeton University Press.
16. Koselleck, R. (1988). Critique and crisis: Enlightenment and the pathogenesis of modern society. MIT Press.
17. Levy, Y. (2016). What is controlled by civilian control of the military? Control of the military vs. control of militarization. Armed Forces & Society, 42(1), 75–98. https://doi.org/10.1177/0095327X14567918
18. Levy, Y. (2017). Control from within: How soldiers control the military. European Journal of International Relations, 23(1), 192–216. https://doi.org/10.1177/1354066116631807
19. Luttwak, E. N., & Shamir, E. (2023). The art of military innovation. Harvard University Press. https://doi.org/10.4159/9780674295148
20. Murray, W. (2011). Military adaptation in war. Cambridge University Press. https://doi.org/10.1017/CBO9781139005241
21. Murray, W., & Millett, A. R. (Eds.) (1996). Military innovation in the interwar period. Cambridge University Press. https://doi.org/10.1017/CBO9780511601019
22. U.S. Air Force. (2021). AFDP 1: The Air Force. Department of the Air Force.
23. U.S. Army. (2019). ADP 1: The Army. Department of the Army.
24. U.S. Army. (2022). FM 3-0 Operations. Department of the Army.
25. U.S. Joint Chiefs of Staff. (2017). Joint Publication 1. Department of Defense.
26. U.S. Joint Chiefs of Staff. (2023). Joint Warfighting. Department of Defense.
27. U.S. Marine Corps. (2017). MCDP 1-0: Marine Corps operations. Department of the Marine Corps.
28. U.S. Marine Corps. (2018). MCDP 1: Warfighting. Department of the Marine Corps.

VULNERABILITY ASSESSMENT IN THE VARNA REGION IN THE CONTEXT OF DISASTERS AND EMERGENCIES

Mariya Dimitrova

Abstract: *Urban areas are increasingly vulnerable to the impacts of natural and technological disasters, which necessitates systematic risk analysis and effective prevention strategies. This paper examines the challenges associated with disasters and emergency situations in the city of Varna, with a particular focus on identifying the key factors determining the vulnerability of the urban environment. As one of the largest economic and transport centers on the Bulgarian Black Sea coast, Varna is exposed to a variety of risks, including floods, landslides, extreme weather events, as well as technological accidents related to infrastructure and industrial activities.*

The study employs an analytical and comparative approach based on an analysis of regulatory documents, scientific literature, and empirical data on disasters that have occurred in the region. Particular attention is given to the 2014 flood in the Asparuhovo district as a representative example of the interaction between natural factors and anthropogenic impacts.

The main objective of the study is to assess the degree of vulnerability of the urban system and to propose measures for reducing risk through integrated disaster management, improving infrastructure resilience, and developing early warning systems. The findings may contribute to the formulation of policies aimed at enhancing the resilience of the urban environment to future crisis situations.

Keywords: *disasters, accidents, risk management, vulnerability, prevention, Varna*

АНАЛИЗ НА УЯЗВИМОСТТА ПРИ БЕДСТВИЯ И АВАРИИ В РАЙОНА НА ВАРНА

Мария Димитрова

Резюме*:Градските райони са все по-уязвими към въздействието на природни и техногенни бедствия, което изисква систематичен анализ на риска и ефективни стратегии за превенция. Настоящият доклад разглежда проблематиката на бедствията и аварийните ситуации в град Варна, като акцентът е поставен върху идентифицирането на ключовите фактори, определящи уязвимостта на градската среда. Варна, като един от най-големите икономически и транспортни центрове по българското Черноморие, е изложена на разнообразни рискове, включително наводнения, свлачищни процеси, екстремни метеорологични явления, както и техногенни аварии, свързани с инфраструктурата и индустриалната дейност.*

Изследването използва аналитичен и сравнителен подход, базиран на анализ на нормативни документи, научна литература и емпирични данни за настъпили бедствия в региона. Специално внимание е отделено на наводнението в квартал „Аспарухово“ през 2014 г. като показателен пример за взаимодействието между природни фактори и антропогенни въздействия.

Основната цел на изследването е да оцени степента на уязвимост на градската система и да предложи мерки за намаляване на риска чрез интегрирано управление на бедствията, подобряване на инфраструктурната устойчивост и развитие на системи за ранно предупреждение. Получените резултати могат да подпомогнат формулирането на

политики за повишаване на устойчивостта на градската среда към бъдещи кризисни ситуации.

Ключови думи: *бедствия, аварии, управление на риска, уязвимост, превенция, Варна*

Въведение

Поради интензивните урбанизация, климатични промени и нарастваща концентрация на население и инфраструктура в градските райони, през XXI век, рискът от природни и техногенни бедствия придобива все по-голямо значение. Градовете се превръщат в сложни социално-икономически системи, в които е все по-висока вероятността за възникване на кризисни ситуации. В този контекст изследването на бедствията и аварийните ситуации и разработването на ефективни мерки за тяхната превенция се превръщат в ключов елемент от устойчивото развитие на градската среда.

Град Варна е един от най-големите икономически, транспортни и туристически центрове на българското Черноморие. Това положение го излага на разнообразни рискове, включително наводнения, свлачища, екстремни метеорологични явления и техногенни аварии. Събитията, свързани с наводненията в квартал „Аспарухово" през 2014 г., са доказателство за необходимостта от прецизно анализиране и от разработване на ефективни механизми за управление на риска.

Управлението на риска от бедствия е системен процес, включващ идентифициране, оценка и намаляване на потенциалните заплахи за населението, инфраструктурата и околната среда. Ефективното управление на риска изисква интегриран подход, който съчетава пространствено планиране, развитие на инфраструктурата, институционална координация и повишаване на обществената информираност.

Основната цел на настоящия научен доклад е да анализира основните видове бедствия и аварии в град Варна, да оцени степента на уязвимост на градската среда и да предложи мерки за превенция и намаляване на риска.

Изследването се основава на интердисциплинарен подход, който комбинира методи от областта на управлението на риска, географията и урбанистиката. Анализирани са научна литература и нормативни документи, както и на настъпили бедствия и аварии. На системен анализ са подложени факторите, влияещи върху уязвимостта на градската среда.

Използвани са и методи за оценка на риска, които позволяват да се идентифицират ключовите заплахи и да се формулират препоръки за тяхното предотвратяване или ограничаване. Чрез този подход се цели да се изведат практически приложими насоки за подобряване на управлението на риска от бедствия в град Варна.

1. Теоретични основи на управлението на риска от бедствия

Управлението на риска от бедствия представлява съвкупност от политики, стратегии и практически действия, насочени към намаляване на вероятността от възникване на бедствия и ограничаване на техните негативни последици върху

обществото, икономиката и околната среда [8]. В науката бедствието се разглежда като резултат от взаимодействие между опасно природно или техногенно явление и уязвимостта на засегнатата система. Това означава, че самото природно явление не води непременно до бедствие, ако обществото разполага с достатъчен капацитет за превенция и реагиране [3, 4, 10].

В контекста на управлението на риска е важно разграничението между понятията **опасност (hazard)**, **уязвимост (vulnerability)** и **риск (risk)** [1, 4]. Опасността представлява потенциално разрушително природно или антропогенно явление, като например наводнение, свлачище, буря или индустриална авария. Уязвимостта се отнася до степента, в която население, инфраструктура или икономическа дейност са податливи на въздействие на опасности. Рискът се определя като вероятността дадено опасно явление да причини щети при наличието на определена уязвимост.

Градската среда се характеризира с висока концентрация на население, икономическа активност и критична инфраструктура, което я прави особено чувствителна към различни видове бедствия. Урбанизацията, промяната в земеползването и недостатъчната поддръжка на инженерната инфраструктура увеличават степента на уязвимост на градовете. В този контекст управлението на риска от бедствия изисква интегриран подход, между пространствено планиране, развитие на устойчива инфраструктура, мониторинг на опасните процеси и ефективни системи за ранно предупреждение.

Съвременните политики в областта на намаляването на риска от бедствия поставят акцент върху превенцията и необходимостта от интегриране на управлението на риска в националните и местните политики за развитие. Основните приоритети на тази рамка включват по-добро разбиране на риска, укрепване на институционалния капацитет за управление на бедствията, инвестиране в превантивни мерки и повишаване на готовността за ефективна реакция при кризисни ситуации [3].

Особено важно значение има интегрирането на научните изследвания в процеса на вземане на решения на местно и национално ниво [4].

За градовете като Варна, управлението на риска от бедствия следва да бъде разглеждано като непрекъснат процес, който обединява усилията на държавните институции, местната власт, научната общност и гражданското общество.

2. Географска и социално-икономическа характеристика на варна

2.1. Географско положение и природни особености

Град Варна е разположен в североизточната част на България, на западния бряг на Черно море, и е най-големият град по българското Черноморие. Административен център е на Област Варна и е стратегически важен транспортен, икономически и туристически център, със значителна роля в морската търговия, туризма и логистиката.

Релефът на района е разнообразен и включва крайбрежни тераси, хълмисти възвишения и долини, оформени от речни и ерозионни процеси. Особено характерни са дълбоко врязаните дерета, които се спускат към морския бряг. Те

играят важна роля в естественото оттичане на повърхностните води, но при интензивни валежи могат да се превърнат в потенциален източник на наводнения.

Важна природна особеност на града е наличието на Варненско езеро и Белославско езеро, които са свързани с морето чрез плавателен канал и образуват естествена лагунна система. Тези водни обекти имат важно значение за пристанищната дейност, транспорта и екологичното равновесие на региона.

В района на Варна се наблюдават и активни свлачищни процеси, характерни за крайбрежните склонове. Те се дължат на специфичните геоложки условия, наличието на глинести пластове и влиянието на морската ерозия. Тези природни фактори увеличават уязвимостта на определени части от градската територия.

2.2. Климатични фактори и хидрологични особености

Климатът на Варна е умереноконтинентален с ясно изразено влияние на Черно море. Морето оказва смекчаващо въздействие върху температурните колебания, като зимите са сравнително меки, а летата – топли и влажни. Въпреки сравнително умерените климатични условия, районът е подложен на периодични екстремни метеорологични явления: интензивни краткотрайни валежи, силни ветрове, бури и щормове в крайбрежната зона. Тези процеси могат да доведат до наводнения, ерозия на бреговата линия и щети върху инфраструктурата.

В района на Варна реките са малки и се комбинират с временни водни течения, които се активизират при силни валежи. Значителна роля играят и многобройните дерета, преминаващи през урбанизираната територия на града. При недостатъчна поддръжка или застрояване на тези естествени водоотводни канали се увеличава рискът от локални наводнения. Показателен пример за подобна ситуация е наводнението в квартал Аспарухово през 2014 г., при което интензивните валежи и натрупаните наноси в деретата довеждат до бързо приижданe на водни маси и значителни щети върху жилищната инфраструктура.

2.3. Урбанизация и развитие на инфраструктурата

Варна е третият по големина град в България и един от най-бързо развиващите се урбанистични центрове в страната. Като важен транспортен възел Варна разполага с голямо морско пристанище, което е ключов елемент от националната и международната транспортна система. Градът се обслужва от Летище Варна, което играе важна роля за развитието на туризма и международните връзки на региона.

Интензивното строителство и разширяването на градската територия обаче създават редица предизвикателства. Пример е застрояването на райони с потенциална природна опасност, включително дерета и свлачищни зони.

Нарастващият брой жители и туристи също поставят по-големи изисквания към инженерната инфраструктура – водоснабдяване, канализация, транспортни мрежи и системи за защита при бедствия. Поради тази причина устойчивото градско планиране и модернизацията на инфраструктурата са ключови фактори за намаляване на риска и повишаване на устойчивостта на град Варна към природни и техногенни бедствия.

Следователно град Варна е изложен на различни природни и техногенни рискове, които могат да окажат съществено въздействие върху населението, инфраструктурата и икономическата дейност. Възникването е възможно както

поради природни бедствия, така и поради аварийни ситуации, свързани с човешката дейност.

3. Бедствия

3.1. Наводнения

Наводненията са сред най-сериозните природни рискове за Варна. Те се причиняват най-често от интензивни краткотрайни валежи, които водят до бързо приижданe на водни маси по деретата и временните водни течения в района. Допълнителен фактор е застрояването на естествени водоотводни зони, което затруднява нормалното оттичане на водите.

Откроява се примерът с наводнението в квартал Аспарухово през 2014 г., когато вследствие на проливни дъждове и запушени дерета се образува мощен воден поток, причинил значителни материални щети и човешки жертви.

3.2. Свлачища

Свлачищните процеси също представляват сериозен риск за крайбрежните райони на Варна. Те се дължат на специфичните геоложки условия, включващи пластове от глинести и рохкави седименти, както и на ерозионното въздействие на морските вълни. Свлачища се наблюдават по крайбрежните склонове и в някои периферни райони на града, където интензивното строителство може да дестабилизира склоновете. Свлачищните процеси застрашават пътна инфраструктура, жилищни сгради и инженерни съоръжения [5, 6].

3.3. Бури и екстремни метеорологични явления

През есенно-зимния период често се наблюдават интензивни ветрове и морски бури, които могат да причинят щети по крайбрежната инфраструктура и пристанищните съоръжения. Възможни са и метеорологични явления като градушки, интензивни валежи и периоди на силна горещина през летните месеци [6, 7].

4. Техногенни аварии

4.1. Промишлени аварии

Като важен индустриален и транспортен център, Варна разполага с редица промишлени предприятия, складови бази и енергийни съоръжения. Такива обекти създават потенциален риск от промишлени аварии, включително пожари, експлозии и изтичане на опасни вещества. Особено значение имат индустриалните зони около Варненско езеро и пристанищната инфраструктура на Пристанище Варна, където се извършват дейности, свързани със съхранение и транспорт на различни видове товари.

4.2. Транспортни инциденти

Варна е ключов транспортен възел, включващ морски, въздушен и сухопътен транспорт. В града се намират важни транспортни съоръжения като Летище Варна и международното пристанище, които обслужват значителен пътнически и товарен поток.

Интензивният транспорт увеличава вероятността от пътнотранспортни произшествия, железопътни инциденти и аварии, свързани с морския транспорт.

Подобни събития могат да доведат до човешки жертви, материални щети и замърсяване на околната среда [10].

4.3. Аварии в критичната инфраструктура

Критичната инфраструктура включва системи, които са жизненоважни за функционирането на града – електроснабдяване, водоснабдяване, телекомуникации и транспортни мрежи. Аварии в тези системи могат да доведат до сериозни социални и икономически последствия.

Например прекъсвания в електрозахранването, аварии във водоснабдителната мрежа или повреди в канализационната система могат да нарушат нормалния живот на населението и да създадат условия за възникване на вторични кризисни ситуации [10, 11].

5. Готовност и капацитет на местната власт

Анализът на риска от бедствия във Варна показва, че устойчивостта на града зависи и от организационната готовност и капацитета на местната власт, от интегрирания подход, който обединява институционална структура, системи за ранно предупреждение и междуинституционално взаимодействие [9].

• Институционално организация на управлението при кризи

Местната власт във Варна включва с координирани звена за управление при бедствия – общински отдели за защита при бедствия, пожарна безопасност, полиция и здравни служби. На стратегическо ниво общината разработва планове за защита. Подходът е известен и осигурява ясна организация на действията при кризи, позволява бързо разпределение на ресурси и координира действията на отделните служби при различни сценарии на бедствия [8].

• Системи за предупреждение и комуникация

Варна използва метеорологични станции, наблюдение на водните нива, мобилни приложения, електронни съобщения и сирени за информиране на гражданите при опасност. Тези системи позволяват не само ранно предупреждение, но и координация на евакуацията, спасителните екипи и аварийните действия, като значително намаляват риска от човешки загуби и материални щети [8].

• Взаимодействие между институциите

Междуинституционалното сътрудничество включва общински органи, национални институции като Главна дирекция „Пожарна безопасност и защита на населението“, здравни служби, полиция и социални служби. Редовните оперативни срещи, съвместните учения и обменът на информация позволяват координирано реагиране при бедствия и предотвратяват дублиране на усилията.

Пример за критичното значение на взаимодействието при комплексни събития е наводнението в квартал Аспарухово през 2014 г., когато синхронизираната работа на институциите би могла да намали щетите и човешките загуби. Причина за бедствието са интензивни валежи, недостатъчна поддръжка на деретата, неправомерно застрояване и интензивна урбанизация. Последствията са сериозни – човешки жертви, разрушени сгради, повредена инфраструктура и замърсени водни обекти. Случаят подчертава необходимостта от: редовна поддръжка на

инженерните съоръжения, контрол върху строителството в рискови зони, развитие на системи за ранно предупреждение и повишаване на обществената информираност.

6. Мерки за превенция и намаляване на риска

На базата на анализа на природните и техногенните бедствия, готовността на институциите и казуса „Аспарухово", могат да се формулират ключови превантивни мерки:

- **Устойчиво градско планиране**
  - Ограничаване на строителството в зони с повишен риск;
  - Създаване на зелени пространства и водопоглъщащи площи;
  - Интегриране на оценката на риска в плановете за развитие на града [7].
- **Подобряване на инфраструктурата и дренажните системи**
  - Редовна поддръжка и почистване на дерета и канализации
  - Модернизация на водоотводните съоръжения
  - Изграждане на защитни съоръжения и контрол на водните потоци [10].
- **Системи за ранно предупреждение**
  - Автоматизирани метеорологични и водни станции;
  - Електронни и мобилни канали за разпространение на предупреждения;
  - Възможности за бърза координация на спасителните и евакуационни екипи [10].
- **Обучение и информираност на населението**
  - Информационни кампании и обучения за действия при бедствия;
  - Практически упражнения и симулации за населението и служителите;
  - Разработване на инструкции и ръководства за безопасност [10].
- **Междуинституционална координация**
  - Редовни учения;
  - Обмен на информация между общинско и национално равнище;
  - Съвместни планове за действие [10].

Заключение

Проблемът с природните и техногенните бедствия в съвременната градска среда придобива все по-голямо значение в контекста на нарастващата урбанизация, климатичните промени и увеличаващата се концентрация на население и инфраструктура. Анализът на рисковете в Варна показва, че градът е изложен на разнообразни природни и антропогенни заплахи, включително наводнения, свлачищни процеси, екстремни метеорологични явления и техногенни аварии, свързани с индустриалната и транспортната инфраструктура.

Изследването подчертава, че уязвимостта на градската среда е резултат от взаимодействието между природните условия и човешката дейност. Географското положение на Варна на брега на Черно море, наличието на дерета и свлачищни зони, както и интензивното градско развитие създават предпоставки за възникване на различни рискови ситуации. Казусът с наводнението в квартал Аспарухово през 2014 г. ясно демонстрира как съчетанието от екстремни валежи, недостатъчна

поддръжка на водоотводните системи и неподходящо застрояване може да доведе до сериозни човешки и материални загуби.

Анализът показва, че ефективното управление на риска изисква интегриран и дългосрочен подход, който съчетава устойчиво градско планиране, модернизация на инфраструктурата, развитие на системи за ранно предупреждение и активно участие на обществото.

Резултатът от анализа позволява заключението, че намаляването на риска от бедствия в градска среда изисква системни усилия, основани на научен анализ, ефективна политика и активна обществена ангажираност. Разработването и прилагането на комплексни превантивни мерки може значително да повиши устойчивостта на Варна към бъдещи природни и техногенни заплахи и да допринесе за устойчивото развитие на града и региона.

Литература:

1. Alexander, D. (2013). Resilience and disaster risk reduction: An etymological journey. Natural Hazards and Earth System Sciences, 13(11), 2707–2716.
2. Cutter, S. L., Burton, C. G., & Emrich, C. T. (2010). Disaster resilience indicators for benchmarking baseline conditions. Journal of Homeland Security and Emergency Management, 7(1).
3. European Commission. (2020). Overview of natural and man-made disaster risks the European Union may face. Publications Office of the European Union.
4. Ministry of Interior of the Republic of Bulgaria. (2019). National disaster risk profile of the Republic of Bulgaria. Sofia.
5. Romanova, H., Radeva, N., & Vasileva, R. (2019). Research of the awareness and preparedness for floods of foreigners temporarily residing in Varna. Land Forces Academy Review, 24(4), 326–331. DOI: 10.2478/raft-2019-0041.
6. Radeva, N. R., Panteleeva, M. N., & Romanova, H. A. (n.d.). Civil protection modern aspects in case of disasters — Bulgaria.
7. Romanova, H. (n.d.). Flood risk assessment in Bulgaria (and in particular in Varna Province). Varna Medical Forum.
8. United Nations Office for Disaster Risk Reduction. (2015). Sendai framework for disaster risk reduction 2015–2030. UNDRR.
9. Георгиев, Г. (2018). Управление на риска от бедствия в България. София: Университетско издателство.
10. Главна дирекция „Пожарна безопасност и защита на населението“. (2015). Годишен доклад за състоянието на защитата при бедствия. София.
11. Николов, Д. (2016). Природни рискове и бедствия в България. София: Издателство на БАН.

APPLICATION OF GRAPH THEORY IN THE ANALYSIS OF DEPOPULATED REGIONS

Milena H. Lambeva

*Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, milenalambeva_333@gmail.com*

***Abstract**: Depopulated regions exert a direct, profound, and multidimensional negative impact on national security. This report demonstrates how graph theory can be applied to analyze the demographic connectivity of regions, with the aim of improving it and reducing the number of areas with critically low population levels.*

***Keywords:** depopulated regions, national security, graph theory, free-scale networkt*

ПРИЛОЖЕНИ НА ТЕОРИЯ НА ГРАФИТЕ ЗА АНАЛИЗ НА ОБЕЗЛЮДЕНИ РАЙОНИ

Милена Х. Ламбева

*Факултет „Артилерия, ПВО и КИС“, Национален военен
университет "Васил Левски", Шумен, България, milenalambeva_333@gmail.com*

***Abstract**: Обезлюдените региони оказват пряко, дълбоко и многоизмерно отрицателно въздействие върху националната сигурност. Този доклад демонстрира как теорията на графите може да се приложи за анализ на демографската свързаност на регионите, с цел подобряването ѝ и намаляване на броя нарайоните с критично ниски нива на население.*

***Ключови думи:** обезлюдени райони, национална сигурност,теория на графите, без мащабни мрежи*

Увод

Значителна част от обектите, процесите и явленията, които представляват интерес от научен или научно-приложен характер проявяват системни свойства. За тяхното описание и изследване е адекватен подход, който ги разглежда като съвкупност от взаимосвързани същности и отношения между тях.

Мрежовият анализ предоставя теоретичната основа за изследване на структурните и функционалните зависимости между елементите на системата, докато теорията на графите предоставя математическите средства за формално представяне на реалните системи чрез възли, ребра и тегла и за анализ на техните ключови характеристики.

Този доклад демонстрира приложимостта на средствата на графите за моделиране на системите, които се формират от населените места в намиращи се в определен регион и пътищата, които ги свързват. Показва и как методите на

мрежовия анализ могат да бъдат използвани за изследване на демографската свързаност в регионите.

Предлага се решение на проблема за нарушената социална кохезия посредством преднамерено предизвикана ревитализация на определени обезлюдени населени места и се показва как граф базираните модели на селищните системи могат да бъдат използвани за да се определи към кое/кои населено място или места да бъдат насочения усилията за съживяване.

В първата секция е мотивирано твърдението, че обезлюдените райони представляват източник на заплаха за националната сигурност.

Във втората секция са въведени основни понятия от областта на графите, които имат отношение към моделирането и изследването на демографската свързаност в рамките на селищна система.

Трета секция съдържа граф-базиран модел на селищна система, върху който са симулирани локални (подобряване на условията за живот) и структурни (построяване на нови пътища, свързващи населеното място или подобряване качеството на съществуващите) изменения в географския регион.

1 Обезлюдените райони на територията на страната – източник на заплахи за националната сигурност

Сигурността е фундаментална необходимост, която в теорията на Маслоу е поставена в основата на йерархията на човешките потребности [1]. Темата за физическото оцеляване остава актуална в хода на развитието на обществото от зараждането на цивилизацията до съвременността. **Тази трайна значимост формира сигурността като сложна и многоаспектна съвкупност от индивидуални, обществени и национални** измерения.

Националната сигурност е по-тясно понятие от общата концепция за сигурност, но въпреки това представлява комплексна и многокомпонентна система. Тя интегрира в себе си ключови аспекти като политическа стабилност, военен капацитет, информационна сигурност, екологична устойчивост, икономическа устойчивост и социално сближаване и още много други.

Настоящият доклад се фокусира върху много тясна област от демографската компонента на националната сигурност, а именно обезлюдените територии и възможностите за тяхната ревитализация .

Числеността и пространственото разпределение на населението са сред ключовите демографски показатели, които влияят върху способността на държавата да поддържа стабилност и да упражнява ефективно управление.

Обезлюдяването на територии е структурен демографски процес, характеризиращ се с постоянен и значителен спад в популационните нива и е сред основните демографски фактори, влияещи пряко върху националната сигурност, като отслабва икономическата устойчивост, ерозира социалното сближаване и ограничава капацитета на държавата за ефективно управление и териториален контрол.

Следователно, намаляването на обезлюдените райони е стратегически приоритет, изискващ интегрирани политики в областта на демографията, регионалното развитие, сигурността и териториалното управление.

Комплексното въздействие на три фактора довежда до депопулация на селища и цели региони – ниска раждаемост, висока смъртност, обусловена предимно от високата степен на застаряване на населението и миграция на хора в детеродна и трудоспособна възраст към райони с благоприятни социални и икономически условия.

Поради биологично обусловените им особености, върху първите два фактора е невъзможно да се повлияе в кратки срокове. Ревитализация на обезлюдени райони за период от време между пет и десет години е мислима чрез въздействие върху фактора миграция.

Един възможен подход за промяна на миграционните показатели се състои в използването на подходящи механизми за насърчаване на повторното заселване на селища с малък брой жители, които да се превърнат в нови регионални центрове и да допринесат за съживяването на целия регион.

В свой доклад [1], Тадо Юрич синтезира набор от мерки, насочени към привличане на хора в икономически активна и репродуктивна възраст към обезлюдени райони. Те могат да бъдат обобщени по следния начин:

• Осигуряване на възможности за дистанционна работа, което изисква въвеждането на широколентов интернет в цялата страна.

• Подобряване на инфраструктурата, включително разширяване на транспортната мрежа.

• Достъп до основни услуги, като здравеопазване, образование и културни дейности.

Превръщането за кратко време на обезлюдено селище в притегателен център за активни млади хора изисква влагането на значителни по размер ресурси от страна на държавата.

В тази връзка на преден план излиза необходимостта да се определи населено място към което да бъдат насочени инвестициите, такова че то не само да увеличи числеността на населението си многократно, а и да окаже положително въздействие на социалната свързаност в целия регион.

Задачата за избор на прицелно населено място е многоразмерна и многокритериална, свързана с много предварителни разчети и прогнози.

В следващата част на доклада ще бъде показано, че средствата на теорията на графите могат да се използват в качеството на инструмент за определяне на районите, които са най-подходящи за инвестиции, така че да се постигне максимален ефект върху регионалната демографска динамика.

2 Теория на графите - математическа рамка за моделиране и анализ на селищни системи

Селищната система е произволна или административно организирана пространствено разположена съвкупност от взаимосвързани селища, населени

места и територии, чрез различни икономически, социални, инфраструктурни или информационни връзки.

Характеристиките на населените места – демографски показатели, транспортната инфраструктура, която ги свързва, и миграционните потоци – могат да бъдат адекватно описани чрез теорията на мрежите.

За моделиране на структурата и свойствата на мрежата от населени места в дадена територия е целесъобразно да се използва граф, върховете на който геометрично са представени като точки и се асоциират с отделните населени места, а свързаността между тях е представена чрез ребрата на графа, изобразени като дъги.

Графът е математически обект, състоящ се от множество от върхове V и множество от ребра E.

$$G = (V,E) \quad (1)$$

Свойствата на върховете, които са приложими за определяне на относителната свързаност на населеното място в рамките на селищната мрежа са известни в теорията на графите като „централност". С този термин се означават няколко свойства, най-широко използваните от които са: централност по степен (от англ. degree centrality), централност по посредничество (от англ. betweenness centrality) и централност по близост (от англ. closeness centrality).

Централност по степен на произволен връх (degree centrality) се определя като отношение между броят върхове, с които той е съседен и броят на всички върхове в графа.

В контекста на селищните системи това свойство се определя от отношението на броя населени места, с които даденото селище е пряко свързано, към общия брой селища в мрежата и показва доколко това селище играе ролята на локален хъб в мрежата.

Централност по посредничество (betweenness centrality) се базира на най – кратките пътища в графа. За всяка двойка върхове съществува най – кратък път, той е този с най–малко върхове или с най – малка сума на тежестите, ако графът е претеглен. Централността по посредничество показва броя на най – кратките пътища за различни двойки върхове, които минават през даден връх и помага да се идентифицират ключови транспортни и функционални „възли-мостове" и показва дали населеното място е определящо върху миграционни и транспортни потоци.

Централност по близост (closeness centrality) изследва средно аритметичното разстояние на връх до другите върхове.

Централността по близост измерва степента, до която дадено населено място е достъпно за всички останали в мрежата, като оценява сумата от най-кратките пътища. **В рамките на мрежовото представяне на селищата** показва пространствената интегрираност, инфраструктурната свързаност и потенциала за бързо разпространение на демографски и функционални ефекти.

Собственият вектор (eigenvector centrality) измерва колко важно е едно населено място, като отчита не само броя на неговите връзки, а колко важни са местата, към които е свързано. Ако един възел е свързан с много влиятелни

възли неговата собствена централност е висока. Ако е свързан с периферни възли централността му е ниска, дори да има много връзки.

Матрицата на дисперсията е динамична характеристика, която показва вероятността индивид, материал, ресурс, информация, сигнал да се премести от възел i към възел j. Тази матрица е важна за моделиране на миграция, движение на хора, транспортни потоци и др.

3 Граф базиран модел на селищна система

Задачата за избор на селището, към което да се насочи комплекса от икономически, административни и социални мерки може да бъде решена посредством изпълнението на следната последователност от стъпки:

1. Етап моделиране.

Регионалната селищна система се представя като претеглен неориентиран граф G=(V,E), където всеки връх $v_i \in V$ съответства на селище, а всеки ръб $e_{ij} \in E$ представлява съществуващ път или комуникационна връзка между селища i и j. На всеки връх са присвоени атрибути: име на населеното място, демографска категория от 1 до 6, отразяваща числеността на населението и параметър на привлекателност (пригодност), който отразява относителния капацитет на населеното място да привлича потоци от население. Етикетите на дъгите са цели числа от 1 до 5, които са съпоставими с най-краткото време за придвижване между селищата.

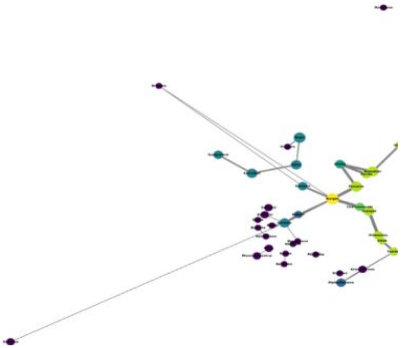
Към модела се поставя изискване да отразява пространственото разположение на селищата и свойството безмащабност на регионалните селищни системи: във всеки район съществува едно населено място с голяма численост на населението, непосредствено свързано с няколко значително по - малки населени места. В периферията на района са разположение няколко почти обезлюдени селища със затихващи икономически и социални функции. Селището с най-голяма численост привлича все повече жители от селищата от региона и извън него, а населението в малките населени места намалява все повече. Това обосновава използването на модел Бианкони –Барабаши (нарича се още фитнес модел) [2], който представлява разширение на класическия Барабаши–Албърт модел и притежава присъщите за него характеристики – безмащабност, степенно разпределение, наличие на хъбове, феномен на малкия свят, но дава възможност за присвояване на вътрешна „фитнес" стойност за всеки възел. Параметърът фитнес отразява присъщата способност на възела да привлича връзки независимо от текущата му степен. С него се кодират фактори като икономически възможности, инфраструктура, дигитална свързаност, туристически потенциал, административни стимули и т.н. Възел с висок фитнес-например град с развита инфраструктура и услуги, наличие на работни места ще привлича повече население и има по-голяма вероятност да формира връзки с други възли.

Фигура 1 представя граф на селищната система на Бургаска област, който отразява реалните GPS координати и характеристиките на населените места: числеността на популацията се изразява с големина на кръгчето, фитнеса – посредством цвета на кръгчето, които са в съответствие на стойности от

предварително определена скала, а дебелина на дъгата отразява качество на пътя. За целите на този доклад графът е генериран в среда на Python, но за визуализация на графи могат да се използва всеки от съществуващите езици.

Симулацията описана по-нататък, също е направена на езика Python в среда на JuputerLab.

2. Етап симулация на интервенции За да се прогнозира ефектът от целенасочените интервенции в едно или няколко селища се извършва промяна на атрибутите на възлите и ръбовете в данните, които са изходни за изчертаването на граф . Направен е експеримент със село Младежко, което по данни на Национален статистически институт [4] е с население 28 души, както е показано на фигура 2 и се нарежда сред селищата с най-малка численост в Бургаска област. Категоризацията (показател Category), определянето на стойностите на показателя фитнес (показател Fitness), както и категоризацията на пътищата (показателя Weight от изображението на фигура 3) на дъгите са направени от автора на доклада.



Фигура 1: Граф-базиран модел на селищната система на Бургаска област

	Id	Label	Populatior	Category	Fitness	lat	lon
30	Stoilovo	Stoilovo	60	1	0,01	42,03772	27,51656
31	Draka	Draka	49	1	0,01	42,3645	27,01805
32	GolyamoB	GolyamoB	48	1	0,01		
33	Bogdanov	Bogdanov	44	1	0,01	42,23358	27,26105
34	Kirovo	Kirovo	31	1	0,01	42,15782	27,18719
35	Mladejko	Mladejko	28	1	0,01	42,15329	27,37048
36	Belila	Belila	27	1	0,01	42,33073	27,10428
37	Rosenovo	Rosenovo	21	1	0,01	43,66458	27,78277
38	Bratovo	Bratovo	13	1	0,01	43,18484	26,41612
39	Belevren	Belevren	6	1	0,01	42,09362	27,17797
40	Varovnik	Varovnik	5	1	0,01	42,21722	27,23178
41	Vresovo	Vresovo	5	1	0,01	42,81211	27,19878

Фигура 2: Изглед от файла с данни nodes.csv, използван за генериране на изходния граф на Бургаска област.

За да се симулира увеличаването на привлекателността на Младежко с нарастването на броя на жителите с 100 души се генерира нов граф, със следните промени в изходните данни: категорията на селото е повишена от 1 на 2, на параметъра Population е присвоена стойност 128, привлекателността е повишена от 0,01 на 0,5. Добавени са нови ребра, които симулират изграждане на нови несъществуващи пътища, свързващи селото с областния център и други по-малки селища.

	Source	Target	Weight	Type
26	Ruen	Vresovo	2	Undirected
27	Tsarevo	Kiten	4	Undirected
28	Obzor	Nessebar	4	Undirected
29	Fakia	Momina ts	1	Undirected
30	Zagortsi	Sredets	1	Undirected
31	Bistrets	Valchanov	1	Undirected
32	Belila	Sredets	1	Undirected
33	Bogdanov	Sredets	1	Undirected
34	Draka	Zagortsi	1	Undirected
35	Suhodol	Zagortsi	1	Undirected
36	Zornitsa	Sredets	1	Undirected
37	Mladejko	Mladejko	1	Undirected
38	Stoilovo	Stoilovo	1	Undirected

Фигура 3: Изглед от файла с данни edges.csv, който е използва в качеството на изходни данни за построяване на графа на Бургаска област.

37	Source	Target	Weight	Type
38	Stoilovo	Stoilovo	1	Undirected
39	Mladejko	Burgas	5	Undirected
40	Mladejko	Kirovo	1	Undirected
41	Mladejko	Sredets	2	Undirected
42	Mladejko	Gramatikovo	1	Undirected
43	Mladejko	Kiten	4	Undirected
44	Mladejko	Tsarevo	2	Undirected

Фигура 4: Изглед от файла с данни edges.csv след добавени нови ребра

В новия граф се симулира появата на нови „агенти" - микро-обекти, инициативи, домакинства или отделен човек, които се прикачват към съществуващите селища според тяхната степен и фитнес. След изпълнението на симулацията графиката се отчитат параметрите „популация" и „фитнес" на изследвания възел. Вижда, че след интервенцията вероятността за прикрепване на „агенти" към Младежо нараства.

При провеждане на експеримента са използвани възможностите на библиотеките за работа с мрежи в Pyton за са се симулира навлизането в областта на определен брой нови агенти годишно за различен период от време.

В случая е реализирана с**имулация на поток от агенти върху графа** на областта за 20 години като всяка година се появяват **200 нови агенти.**

3. Етап анализ на резултатите и избор на селище

За избор на селище, чиято ревитализация в най-висока степен и за най-кратко време ще повлияе положително върху социалната свързаност на целия регион е необходимо да бъдат направени множество симулации с промяна на параметрите на различни възли от графа.

Графовите модели предоставят формален и гъвкав инструмент за анализ на пространствените и функционални връзки между населените места. В контекста на демографската политика те позволяват да се моделира не само текущото състояние на регионалната мрежа, но и потенциалните ефекти от различни интервенции. Чрез параметри като degree (свързаност) и fitness (атрактивност) графите улавят комплексни взаимодействия, които традиционните демографски модели не могат да опишат.

Възможността да се симулира процесът на заселване като механизъм на преференциално прикачване позволява да се идентифицират възли, които имат потенциал да се превърнат в локални хъбове при подходящи условия. Това превръща графовите модели в инструмент за стратегическо планиране: те могат да покажат къде инвестициите биха имали най-голям ефект, кои населени места могат да бъдат „активирани" чрез подобряване на инфраструктурата и какви сценарии биха довели до устойчиво развитие на периферните региони.

Примерът с Младежко показва че малко периферно населено място е възможно да бъде превърнато в един от най-привлекателните възли в мрежата и че „локални

хъбове" могат да бъдат създадени изкуствено, ако се приложат правилните политики.

Изводи

Изследването демонстрира, че графовият модел Bianconi–Barabasi предоставя инструмент за анализ на пространствените и функционални връзки между населените места. В контекста на демографската политика те позволяват да се моделира не само текущото състояние на регионалната мрежа, но и потенциалните ефекти от различни интервенции и могат да служат като инструмент за анализ и прогнозиране на демографски процеси.

Литература

1. A. H. Maslow,. A theory of human motivatio(1943)n. Psychological Review, 50(4), 370–396. https://doi.org/10.1037/h0054346
2. Bianconi, G., & Barabási, A.-L. (2001). *Competition and multiscaling in evolving networks*. Europhysics Letters
3. Tado Juric, Addressing Depopulation01.06.20226 г., достъпен на https://www.martenscentre.eu/wp-content/uploads/2024/12/Addressing-Depopulation.pdf
4. НСИ - Национален статистически институт, 01.06.20226 г., достъпен на https://www.nsi.bg/

GEODESY

THE IMPACT OF GRAVITY CORRECTIONS ON NORMAL HEIGHTS DETERMINED BY PRECISE GEOMETRIC LEVELLING

Marko Markov

Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levski"
markomarkov8@abv.bg

***Abstract**: The impact of gravity corrections on normal heights determined by precise geometric levelling is investigated. Results from actual levelling and gravimetric measurements were used. The results affected by the first and second gravity corrections were analysed. A comparison was made with results obtained from GNSS measurements, transformed using BGSTRANS software, the official software of the Bulgarian Geodesy, Cartography and Cadastre Agency.*

***Keywords:** gravity corrections, normal heights, precise geometric levelling, gravimetric measurements, GNSS*

Въведение

При реализация на дейностите, съпътстващи една прецизна геометрична нивелация, отчитането на влиянието на гравитационното поле е не само необходимо, но и задължително да бъде гарантирано получаване на физически обосновани височини. Измерените нивелачни превишения се влияят от изменението на силата на тежестта по направление на нивелачния ход, поради което за коректно определяне на нормалните височини на реперите се въвеждат, по необходимост, съответни гравиметрични „нормални" поправки [2,6].

Нормалната поправка към измереното нивелачн превишение се формира от две съставни. Първата отразява изменението на нормалното гравитационно поле, а втората отчита влиянието на аномалното гравитационно поле. Тяхното отчитане позволява резултатите от геометричната нивелация да бъдат освободени от ефекта на неуспоредност на ниво-повърхнина в система „нормални височини" и да бъдат приведени към използваната актуална височинна система (понастоящем EVRS 2007).

Практическата значимост на тези поправки зависи от изискуемата точност на нивелачните измервания и от вариациите на гравитационното поле. При една прецизна нивелация, дори поправки от субмилиметров порядък, биха били съпоставими с точността на получаваните („измерените") височинни разлики. Това поставя въпроса за оценка на влиянието на тези поправки в процеса на предварителна обработка на резултатите от директните измервания.

В настоящото изследване са използвани резултати от извършена прецизна нивелация, дублирана с гравиметрични измервания, върху избран участък от Държавната нивелачна мрежа. Въз основа на получените данни, са изчислени първата и втората гравиметрични поправки и е оценено влиянието им, върху стойностите на нормалните височини.

Целта на изследването е да се оцени влиянието на гравиметричните поправки, при определяне на нормални височини, в резултат от реализацията на прецизни нивелачни ходове. За целта са сравнени резултатите, получени след обработката, без въвеждане на поправките, с резултатите, на базата на предварително определени, получени чрез трансформация с програмен продукт BGSTrans елипсоидни височини.

Получените резултати са основа за оценка на практическата необходимост от паралелни гравиметрични данни при реализацията на прецизни височинни определения.

1 Методология на изследването

Изследването е проведено върху предварително избран участък от Държавната нивелачна мрежа. Реализацията на измерванията е осъществена с дигитален нивелир, с фабрична точност 0,3mm/1km двойно пронивелирано разстояние. Използвани са комплект - баркодови, несгъваеми лати, с инварна лента. Нивелачните измервания са извършени съобразно всички изисквания описани в *ИНСТРУКЦИЯ № РД-02-20-1 ОТ 15 ЯНУАРИ 2021 Г. ЗА СЪЗДАВАНЕ И ПОДДЪРЖАНЕ НА ДЪРЖАВНАТА НИВЕЛАЧНА МРЕЖА, Издадена от министъра на регионалното развитие и благоустройството*. Използваният гравиметър е „LaCoste&Romberg Model G", широкодиапазонен гравиметър, с "електронен отчет" на нулевото положение на махалото и електронни либели. ГНСС измерванията са реализирани посредством двучестотен ГНСС приемник и са съобразени с *ИНСТРУКЦИЯ № РД-02-20-25 ОТ 20 СЕПТЕМВРИ 2011 Г. ЗА ОПРЕДЕЛЯНЕ НА ГЕОДЕЗИЧЕСКИ ТОЧКИ С ПОМОЩТА НА ГЛОБАЛНИ НАВИГАЦИОННИ СПЪТНИКОВИ СИСТЕМИ)*.

При обработката на резултатите от нивелацията определянето на „измерените" нормални превишения е осъществено чрез въвеждане на първа и втора гравиметрични поправки [1]. В този контекст нормалното превишение между два съседни репера се определя като:

$$\Delta h_i^N = \Delta h_i + I_i + II_i, \tag{1}$$

където: Δh_i е измереното превишение, а I_i и II_i са съответно първата и втората гравиметрични поправки. В процеса на предварителната обработка на резултатите от директните измервания, поправките а I_i и II_i се изчисляват за участъка между два съседни междинни репери, тъй като за всяка отделна нивелачна станция разстоянията са малки и ефектът от пренебрегване на поправките би бил пренебрежимо малък [8, 11].

Първата поправка отчита влиянието на изменението на нормалната сила на тежестта, включително влиянието на височината на терена и особеностите на релефа, докато втората е повлияна от аномалната съставна на реалното гравитационно поле. В процеса на реализация на приложената методика, първата поправка е определена чрез разликата в нормалната сила на тежестта за краищата на разглежданата отсечка, а втората е свързана с интегралното влияние на разликата между реалната и нормалната сила на тежестта по височина (2 и 3):

$$I_i = -\frac{(\gamma_0^{i+1} - \gamma_0^i)}{\gamma_m^i} H_{i+1} \quad (2)$$

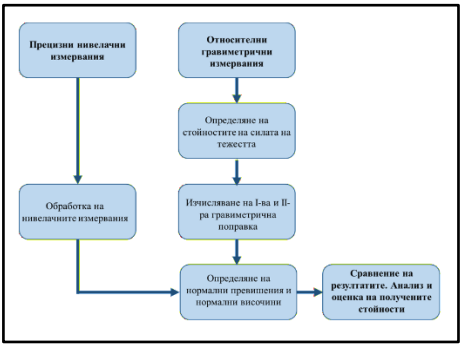
$$II_i = -\frac{1}{\gamma_m^i} \int_{i,i+1} (g - \gamma) dh \quad (3)$$

За определяне на необходимите гравиметрични величини (стойностите на ускорението на силата на тежестта) са реализирани паралелни относителни гравиметрични измервания. При този метод непосредствено се определят разликите в силата на тежестта между точка с предварително определена стойност над изследвана точка. Подобен подход е подходящ за изграждане и сгъстяване на гравиметрични мрежи, като при обработката им се прилагат схеми и процедури, ограничаващи влиянието на систематичните грешки [10] .

Получените гравиметрични резултати са използвани съвместно с нивелачните измервания за предварително изчисление на нормалните височини. За оценка на ефекта от получените гравиметрични данни е извършено паралелно изчисление на височините, в два варианта – без въвеждане и с въвеждане на първата и втората гравиметрична поправка.

На базата на получените резултати е извършена и независима съпоставка с нормалните височини, на идентични точки, получени в резултат на трансформация с програмния продукт BGSTRANS. Това сравнение има за цел да покаже различията между нормалните височини, определени въз основа на непосредствените нивелачни и гравиметрични измервания, и тези, получени чрез официално утвърден у нас трансформационен модел. В крайните резултати разликите между двата вида нормални височини достигат няколко сантиметра.

За допълнителна оценка на влиянието на гравиметричните поправки са използвани резултатите от изравнените стойности на височините, нормалните височини, с нанесени гравиметрични поправки и резултатите от трансформацията BGSTRANS. От наличните данни са подбрани представителни стойности, чрез които се оценяват както величината на гравиметричното влияние, така и изменението му по изследвания участък.



Фигура 1: Схема на избрана методика на изследване

2 Резултати и анализ

Оценката на влиянието на гравиметричните поправки е анализирана посредством данните от 93 точки от изследвания нивелачен участък. Съпоставени са изравнените височини (Низр), нормалните височини (HN), и нормалните височини, получени чрез трансформация с BGSTRANS (HNтр).

От пълния набор данни са подбрани седем характерни точки, ясно показващи различни по величина стойности, на гравиметричното влияние и на разликите спрямо трансформационния модел. Идентификационните номера и координатите на реперите не са включени, тъй като не са необходими за анализа.

Таблица 1. Представителни резултати от сравнението на нормалните височини на реперите

№	$H_{изр.}$, [m]	H^N, [m]	$H^N_{тр}$, [m]	$H^N - H_{изр}$, [m]	$H^N - H^N_{тр}$, [m]
1	25,65659	25,65221	25,66400	0,00438	-0,01179
2	71,70568	71,70570	71,73500	0,00002	-0,02930
3	136,90180	136,90329	136,99300	0,00149	-0,08971
4	155,69135	155,69388	155,73600	0,00253	-0,04212
5	240,79605	240,79662	240,88900	0,00057	-0,09238
6	243,35496	243,36002	243,41300	0,00506	-0,05298
7	276,93924	276,94563	276,99600	0,00639	-0,05037

Анализът на всичките 93 точки показва, че разликата $H^N - H_{изр.}$ е в интервала на абсолютни стойности от **0,0 до 6,4 mm**, при средна стойност **1,32 mm** и стойност на средната квадратна грешка от **1,83 mm**. Макар абсолютната величина на получените стойности да е малка, спрямо самите височини, тя е съпоставима с точността, която се изисква при прецизни височинни определения. Поради това, пренебрегването на гравиметричния ефект може да окаже влияние върху крайните резултати при задачи, изискващи милиметрова точност [12]. Дори сравнително малките гравиметрични поправки могат да бъдат съпоставими с допустимите разлики на крайния резултат. Поради това използването на едни и същи приближени стойности за целия нивелачен участък не би отчело в достатъчна степен реалното пространствено изменение на гравитационното поле.

Нормалната височина комуникира с геопотенциалните разлики (коти) и средната нормална сила на тежестта по височина, поради което определянето ѝ от

геометрична нивелация изисква отчитане на влиянието на гравитационното поле [1, 6]. Това влияние е установено чрез сравняване на стотици хиляди резултати преди и след въвеждането на гравиметричните поправки.

Втората част от анализа е свързана със сравнението на получените нормални височини с резултатите получени чрез BGSTRANS. За всички 93 точки разликата H^N - $H^N_{тр}$ варира от **1,3** до **92,4** mm, като средната стойност е **41,28** mm.

Разликата между двата резултата се дължи на различния подхпод при определяне на нормалните височини. В първия случай те са получени въз основа на реални нивелачни и гравиметрични измервания, докато при втория се използва трансформационен модел, свързващ наделипсоидните височини с нормалните височини посредством височинна референтна повърхнина. Следователно H^N - $H^N_{тр}$ не представлява пряка оценка на гравиметричните поправки, а характеризира различието между два различни подхода за получаване на нормални височини.

Резултатите недвусмислено показват, че сантиметровите различия породени от трансформациония модел, не могат да бъдат обяснени с влиянието на първата и втората гравиметрична поправка. Те са свързани преди всичко с различията между непосредствено определените височини и височинната референтна повърхнина, използвана при трансформацията.

Резултатите потвърждават практическото значение на високоточната паралелна гравиметрична информация при определяне на нормални височини. При геодезически задачи, за които се изисква милиметрова точност, гравиметричният ефект не може да бъде разглеждан като пренебрежимо малък. В конкретния случай този ефект достига 6,4 mm. Същевременно непосредственото използване на гравиметрични измервания позволява да бъде отчетено локалното изменение на гравитационното поле, което е съществено предимство при прецизни височинни определения [1,7].

Получените резултати са в съответствие с принципа, че качеството и достоверността на нормалните височини зависи не само от точността на геометричната нивелация, но и от адекватното описание на гравитационното поле [3,8]. Това е особено важно в процеса на изграждане и поддържане на височинни референтни системи, при които точността на гравиметричната информация и на височинните определения са взаимно свързани.

Заключение

Получените резултати показват, че влиянието на гравиметричните поправки върху определените нормални височини е малко по абсолютна стойност, но съществено от гледна точка на крайните резултати от прецизната нивелация. При височинни определения със субмилиметрова точност гравиметричният ефект не следва да бъде пренебрегван.

Резултатите получени, чрез ненадежни трансформационни модели не могат да бъдат използвани като пряк заместител на нормалните височини, получени от високоточни нивелачни и гравиметрични измервания.

Практическото значение на резултатите е свързано с възможността, чрез непосредствени гравиметрични измервания, да се отчете локалното изменение на

гравитационното поле. Това е особено важно при прецизни височинни мрежи и при задачи, при които натрупването на систематични грешки по направление на нивелачните ходове може да повлияе негативно върху крайния резултат.

Литература

1. Андреев А. Физическа геодезия и гравиметрия. Университетско издателство „Епископ Константин Преславски", Шумен, 2013, ISBN 978-954-577-681-6.
2. Господинов, Сл., Пенева, Е., Пенев, П., Ламбева, Т., Цановски, Ю., Джорова, С., Маринов, Г., Радев, И. Съвременни аспекти на геометричната нивелация. Годишник на УАСГ, 2016, бр. 4, том 49.
3. Господинов Сл., Пенева, Е., Беляшки, Т., Димитров, Д., Михайлов Г., Гравиметрични дейности за целите на Геодезията в Република България, Годишник на УАСГ, том XLIII, св.VI, 151-156, София.
4. ИНСТРУКЦИЯ № РД-02-20-25 ОТ 20 СЕПТЕМВРИ 2011 Г. ЗА ОПРЕДЕЛЯНЕ НА ГЕОДЕЗИЧЕСКИ ТОЧКИ С ПОМОЩТА НА ГЛОБАЛНИ НАВИГАЦИОННИ СПЪТНИКОВИ СИСТЕМИ
5. ИНСТРУКЦИЯ № РД-02-20-1 ОТ 15 ЯНУАРИ 2021 Г. ЗА СЪЗДАВАНЕ И ПОДДЪРЖАНЕ НА ДЪРЖАВНАТА НИВЕЛАЧНА МРЕЖА, В сила от 05.02.2021 г., Издадена от министъра на регионалното развитие и благоустройството, Обн. ДВ. бр.10 от 5 Февруари 2021г., изм. и доп. ДВ. бр.72 от 2 Септември 2025г.
6. Пенева, Е., Височини и височинни системи. София, 2017, ISBN: 9789549122503
7. Пенева Е., Разлика между ортометрични и нормални височини за територията на България. Геодезия, картография и земеустройство, бр.1, 2001.
8. Радичев, Р., Михайлов, Е. Гравиметрични измервания в България за периода от 1926 г. до 2011 г. Годишник на МГУ „Св. Иван Рилски", том 54, 2011.
9. Радичев, Р., Михайлов, Е., Кисьов, А. Гравиметрични поправки и фактори, влияещи на високоточните измервания на силата на тежестта. Годишник на МГУ „Св. Иван Рилски", том 56, 2013.
10. Славова, Т., ЛОКАЛИЗИРАНЕ НА ДЪЛБОЧИННО РАЗПОЛОЖЕНИ КУХИНИ, ПОСРЕДСТВОМ ГРАВИМЕТРИЧНИ МЕТОДИ, ИК „Свети Иван Рилски", София, 2026 г., ISBN 978-954-353-504-0
11. Djorova, S. & Nikolova, M., DETERMINATION OF DEPTH PARAMETERS OF SUBSURFACE VOIDS USING GRAVIMETRIC AND GLOBAL NAVIGATION SATELITTE SYSTEMS MEASUREMENTS, SGEM On Line Scientific Library from the 24th International Multidisciplinary Scientific GeoConference, 2024, 475-482. 10.5593/sgem2024/1.1/s05.60.
12. Peneva E., Georgiev I., Comparison of a gravimetric geoid model with data from GPS/leveling for the territory of South-western Bulgaria, Bulgarian Academy of Sciences, Geodezy 17, Sofia 2006.

GIS AS A TOOL FOR INTEGRATING, ANALYSING, AND VISUALISING SPATIAL DATA TO SUPPORT ROAD SAFETY DECISION-MAKING

Marko Markov

Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levski"
markomarkov8@abv.bg

***Abstract**: This study presents a practical approach to the use of GIS for integrating, analysing, and visualising spatial road safety data. The analysis is based on publicly available datasets describing the condition part of a road network and recorded road traffic accidents for certain period. Spatial analysis combined with statistical methods was used to investigate the relationship between pavement condition and the spatial concentration of road traffic accidents. The findings highlight the potential of GIS-based methods to support road safety analysis and informed decision-making.*

***Keywords:** GIS, road traffic accidents, road safety, statistical methods*

Въведение

Пътната безопасност е комплексна област, в която взаимодействат множество фактори, свързани с инфраструктурата, характеристиките на транспортния поток, поведението на участниците в движението и условията на околната среда [7]. Анализът на тези фактори изисква използване на надеждна и добре структурирана информация, която позволява не само описание на отделни събития, но и установяване на пространствени зависимости [9].

С развитието на геопространствените технологии, значително се увеличава количеството на наличните пространствени данни, свързани с транспортната инфраструктура и пътнотранспортните произшествия. Различни оторизирани държавни структури събират информация за отделни аспекти на пътната обстановка, като състояние на настилката, характеристики на пътната мрежа, местоположение и параметри на възникнали произшествия. Въпреки това, отделните набори от данни често съществуват самостоятелно, а тяхната реална, аналитична стойност, се проявява при комбинирането им и при техния съвместен анализ.

Географските информационни системи (ГИС) предоставят възможност за интегриране на различни източници на информация, извършване на пространствени анализи и визуално представяне на получените резултати [5]. Чрез използване на ГИС данни с различен характер могат да бъдат разглеждани в единна пространствена среда, което позволява откриване на зависимости, които трудно биха били установени чрез традиционни анализи [1]. В областта на пътната безопасност това дава възможност за съпоставяне на състоянието на пътната инфраструктура с пространственото разпределение на пътнотранспортните произшествия.

Самото визуализиране на пространствени данни обаче не е достатъчно за оценка на наблюдаваните зависимости. Необходимо е прилагането на различни статистически методи, които служат за получаване на количествени оценки и тенденции. Комбинацията между пространствен анализ и статистически подходи позволява преминаване от обикновено картографско представяне, към по-задълбочено изследване на факторите, свързани с пътната безопасност [8].

В този аспект, интерес би представлявало приложението на ГИС-базиран подход за интегриране на данни за състоянието на пътната настилка и данни за пътнотранспортни произшествия, с цел анализ на възможни пространствени зависимости. Използвани са публично достъпни данни за републиканската пътна мрежа и регистрирани пътнотранспортни произшествия за периода 01.01.2024–13.07.2026 г. Чрез изчисляване на показатели за концентрация на произшествията спрямо дължината на пътните участъци и прилагане на статистически методи, се оценява възможността за идентифициране на участъци, които могат да станат обект на допълнителен анализ.

Основната цел не е установяване на една единствена конкретна причина за възникване на пътнотранспортни произшествия, а демонстриране на възможностите, които предоставят интегрирането на пространствени данни и аналитичните методи за подпомагане на процесите за оценка на риска и вземане на информирани решения в областта на пътната безопасност.

1 Материали и методи

1.1 Източници на данни и подготовка на информационната база

Ефективното използване на пространствени данни при анализ на пътната безопасност изисква обединяване на информация от различни източници, които описват отделни характеристики на транспортната система. В настоящото изследване са използвани публично достъпни данни, свързани със състоянието на пътната инфраструктура, от Държавна агенция "Безопасност на движението по пътищата" (ДАБДП) [4] и регистрирани пътнотранспортни произшествия, от Министерство на вътрешните работи (МВР) [6].

Основната информационна база включва пространствени данни за републиканската пътна мрежа, съдържащи информация за отделни пътни участъци и актуалното състояние на тяхната настилката. Използваните данни представляват последната налична оценка на състоянието на пътната настилка, като за всеки участък са налични атрибути, описващи категорията на състоянието, дължината и други характеристики на пътния сегмент.

Втората група от данни включва информация за регистрирани пътнотранспортни произшествия за периода 01.01.2024–13.07.2026 г. За всяко събитие са използвани неговите пространствени координати, дата на настъпване, характеристики на произшествието, както и информация за броя на загиналите и пострадалите лица.

За целите на анализа е разглеждана само републиканската пътна мрежа, за която е налична информация, позволяваща съпоставяне между състоянието на настилката и регистрираните пътнотранспортни произшествия. От анализа са

изключени автомагистрали, както и участъци от уличната мрежа в населени места и местни пътища, тъй като в наличните данни за тях се срещат категории, описващи специфични характеристики на пътната инфраструктура, като наличие на разделителна ивица, мантинели (ограничителни системи за пътища) и други особености, които не представляват директна оценка на състоянието на настилката. Това ограничава възможността за коректно сравнение с категориите, използвани за оценка на състоянието на пътните участъци.

Всички пространствени данни са приведени към единна (официално възприета у нас) координатна система EPSG:7801 (БГС2005), което осигурява съвместимост между отделните информационни слоеве и позволява извършването на последващи пространствени операции.

1.2 Пространствено интегриране на данните

Основното предизвикателство, при този анализ на пътната безопасност е свързването на информацията за характеристиките на пътните участъци с конкретни събития. Докато данните за състоянието на пътната настилка са представени като линейни обекти, информацията за пътнотранспортните произшествия е представена като точкови обекти.

За осигуряване на пространствено съответствие между двата типа информация е приложен подход, основан на пространствено свързване, чрез обособяване на зона на влияние около пътните участъци. Създадена е буферна зона с ширина 25 m около линейните обекти, която отчита възможните неточности при позициониране на произшествията [2].

След създаване на буферните зони е извършено пространствено присъединяване на данните за ПТП към съответните пътни участъци. По този начин, към всеки анализиран сегмент са отнесени броят на регистрираните произшествия, броят на загиналите лица, датата на събитието и различна допълнителна информация. Така структурирана, информацията позволява едновременно разглеждане на двата вида данни.

1.3 Определяне на показатели за анализ

Поради различната обща дължина на пътните участъци, принадлежащи към отделните категории състояние на настилката, директното сравнение по абсолютен брой произшествия не би представило коректно различията между тях. Поради тази причина са изчислени показатели, нормализирани спрямо общата дължина на участъците във всяка категория.

За оценка на концентрацията на пътнотранспортните произшествия е използван показателят:

$$\text{ПТП}/_{km} = \frac{N_{\text{ПТП}}}{L^i}, \quad (1)$$

където:

ПТП/km- концентрация на пътнотранспортните произшествия (ПТП/km);

$N_{\text{ПТП}}$- брой регистрирани ПТП, в участък от разглежданата категория състояние на настилката;

L^i- обща дължина на всички участъци, принадлежащи към съответната категория (km).

За оценка на тежестта на настъпилите събития е използван показателят:

$$F/_{km} = \frac{F_{\text{ПТП}}}{L^i}, \quad (2)$$

където:

F/km- плътност на загиналите лица (брой загинали/km);

$F_{\text{ПТП}}$- брой регистрирани ПТП със смъртни случаи, в участък от разглежданата категория състояние на настилката;

L^i- обща дължина на всички участъци, принадлежащи към съответната категория (km).

Изчислените показатели се използват за анализ и графичното представяне на резултатите, което позволява сравнение между различните категории състояние на настилката независимо от тяхната пространствена представителност.

1.4 Статистически анализ

Графичното представяне на резултатите позволява да бъдат установени определени тенденции, но не дава основание да се приеме, че наблюдаваните различия са статистически значими [3]. Поради тази причина, е извършен допълнителен статистически анализ върху данните за всеки отделен пътен сегмент.

За всеки анализиран участък са изчислени индивидуални показатели за плътност на ПТП и ПТП със загинали лица, като броят на регистрираните събития е съпоставен към дължината на съответния пътен сегмент. Получените стойности формират извадката, върху която са приложени съответни статистическите подходи.

Поради наличието на значителен брой участъци, без регистрирани произшествия, е използван непараметричен метод – тест на Крускал–Уолис [10]. Чрез него е оценено дали съществуват статистически значими различия между отделните категории състояние на настилката, по отношение на плътността на пътнотранспортните произшествия и плътността на загиналите лица.

$$H = \frac{12}{N(N+1)} \sum_{i=1}^{k} \frac{R_i^2}{n_i} - 3(N+1), \quad (3)$$

където:

H – стойност на тестовата статистика;

N – общ брой анализирани пътни участъци (N=8545);

k – брой сравнявани категории на състоянието на настилката (k=4);

R_i – сума на ранговете в i-тата категория;

n_i – брой пътни участъци в i-тата категория.

След установяване на статистически значими различия е приложен последващият тест Дън Post-hoc с корекция по Холм, който позволява да бъдат определени конкретните двойки категории, между които се наблюдават статистически значими различия.

При теста на Дън, за всяка двойка категории, се изчислява статистиката Z, която се основава на разликата между средните рангове на сравняваните групи, нормализирана чрез стандартната грешка. С цел ограничаване на вероятността за допускане на грешка от първи род при извършването на множествени сравнения по двойки (общо шест), получените p-стойности са коригирани по метода на Холм. При тази процедура p-стойностите се подреждат във възходящ ред и последователно се сравняват с коригирани критични равнища на значимост. По този начин се осигурява надеждна оценка на статистически значимите различия, при предварително определено ниво на статистическа значимост [12].

Допълнително е използван и коефициентът на ранговата корелация на Спирман. Използването му е обусловено от специфичния характер на анализираните данни и води до няколко ключови методологически предимства за научното изследване. Използването на коефициента позволява да бъде отчетен поредният (ординален) характер на независимата променлива. Докато тестът на Крускал–Уолис разглежда четирите категории на настилката, като отделни (дискретни) групи, при него не се отчита тяхната естествена логическа последователност. Коефициентът на Спирман допълва анализа, като улавя и оценява наличието на общата монотонна тенденция – т.е. дали с влошаването на състоянието на настилката се наблюдава устойчива монотонна тенденция към увеличаване на риска от ПТП. Тъй като показателите за плътност на произшествията и особено на броя загинали лица съдържат голям брой нули (участъци без инциденти) и нямат нормално разпределение, стандартната линейна корелация на Пиърсън би дала възможност за ненадеждни оценки. Ранговата корелация на Спирман е по-слабо чувствителна към подобни особености на данните, тъй като борави с подредбата на стойностите, а не с техните абсолютни величини, което гарантира висока статистическа устойчивост при мащабни извадки [11].

$$\rho = 1 - \frac{6\sum d_i^2}{n(n^2-1)}, \quad (4)$$

където:

ρ – коефициент на ранговата корелация на Спирман.

n – общия брой на изследваните участъци

d_i – разликата между ранговете на двете сравнявани променливи на i-тия участък

Комбинирането на трите подхода осигурява комплексен поглед върху изследвания проблем. Чрез Крускал–Уолис се доказва общият ефект на пътната настилка, чрез Дън се идентифицират конкретните критични прагове (между кои конкретни категории настъпва скок в произшествията), а чрез Спирман се верифицира общата посока и сила на изследваната зависимост. Това елиминира риска от случайни грешки и повишава надеждността на направените заключения за целите на пътната безопасност. При всички статистически анализи е прието ниво на статистическа значимост α=0,05.

Комбинирането на пространствените анализи с непараметрични статистически методи, позволява резултатите да бъдат разглеждани не само като графично представяне на данните, а като количествено оценени зависимости, които могат да подпомогнат последващи анализи и процеса на вземане на решения в областта на пътната безопасност.

2 Резултати и анализ

2.1 Разпределение на пътната мрежа по категории състояние

Анализът обхваща 8545 пътни участъка от републиканската пътна мрежа с обща дължина 5595,17 km. След обработката и класифицирането на данните участъците са разпределени в четири категории, според състоянието на пътната настилка – „Добро", „Задоволително", „Незадоволително" и „Лошо" (Таблица 1).

Полученото разпределение създава необходимата основа за анализ на връзката между състоянието на настилката и регистрираните пътнотранспортни произшествия, като позволява оценката да бъде извършена чрез относителни показатели, отчитащи различния пространствен обхват на отделните категории.

Таблица 1. Основни характеристики на анализираната пътна мрежа по категории**:**

№	Състояние на пътя	Брой участъци	Обща дължина, [km]	ПТП за участък	ПТП с фатален край	ПТП/km	F/km
1	ДОБРО	304	236,40	223	9	0,943	0,038
2	ЗАДОВОЛИТЕЛНО	3594	2396,29	2639	137	1,101	0,057
3	НЕЗАДОВОЛИТЕЛНО	3185	1985,54	1817	68	0,915	0,034
4	ЛОШО	1462	976,94	1746	81	1,787	0,083

2.2 Анализ на плътността на пътнотранспортните произшествия и загиналите лица

За оценка на връзката между състоянието на пътната настилка и регистрираните ПТП са използвани нормализирани показатели, отчитащи броя на произшествията и тези със загиналите лица спрямо общата дължина на участъците в съответната категория (Таблица 1).

Графичното представяне на резултатите (Фиг. 1) показва различия между отделните категории както по отношение на броя на регистрираните пътнотранспортни произшествия, така и по отношение на тежките произшествия със загинали лица. Най-високи стойности на двата показателя се наблюдават при участъците с категория „Лошо", при които се отчита по-висока концентрация на произшествия спрямо останалите категории.

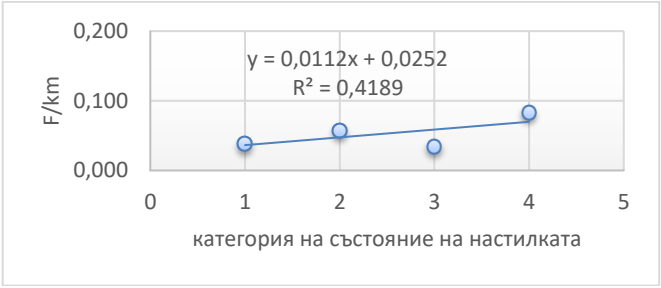


Фигура 1: Връзка между състоянието на пътната настилка, ПТП и загиналите на пътя

За допълнително изследване на наблюдаваната тенденция категориите на състоянието на настилката са кодирани с последователни стойности от 1 до 4, съответстващи на таблица №1. Получените зависимости са представени чрез точкови диаграми с апроксимирана линейна тренд линия (Фиг.2 и Фиг.3).



Фигура 2: Изменение на плътността на ПТП спрямо категорията на състояние на пътната настилка



Фигура 3: Изменение на плътността на ПТП с жертви спрямо категорията на състояние на пътната настилка

Получените резултати показват наличие на възходяща тенденция и при двата анализирани показателя. При показателя ПТП/km се наблюдава увеличаване на плътността на регистрираните пътнотранспортни произшествия, с влошаване на състоянието на настилката, като линейният тренд е описан с уравнение y=0,2346x+0,6004, при коефициент на детерминация R2 = 0,5492.

Аналогична зависимост се наблюдава и при показателя F/km, характеризиращ плътността на ПТП с жертви. Линейната тенденция показва нарастване на стойностите, при преминаване към по-ниски категории на състояние на настилката, като полученото уравнение е y=0,0112x+0,0252, при R2 = 0,4189.

Наблюдаваните зависимости показват, че участъците с по-неблагоприятно състояние на настилката се характеризират с по-високи стойности на показателите за пътна безопасност. Тези резултати представляват първоначална оценка на установената тенденция, като статистическата значимост на различията между отделните категории е допълнително изследвана чрез, прилагане на непараметрични статистически методи.

2.3 Статистическа оценка на различията между категориите състояние на настилката

За проверка на установените, чрез графичния анализ, зависимости е извършен статистически анализ, върху индивидуалните стойности на показателите ПТП/km и F/km за всеки пътен сегмент. Приложен е тест на Крускал–Уолис. За ПТП/km е получена стойност $H = 159.73$, $p < 0.001$, а за F/km H=20.31, p=0.00015,което показва, че разпределението на двата показателя е различно за между отделните категории настилка.

За определяне на конкретните различия между категориите е приложен тестът на Дън с корекция по метода на Холм. При показателя ПТП/km статистически значими различия се установяват основно между категория „Лошо“ и всички останали категории, както и между категориите „Задоволително“ и „Незадоволително“. Получените резултати потвърждават наблюдаваната тенденция при графичния анализ, за по-висока концентрация на произшествия при участъците с по-ниска оценка на състоянието на настилката.

При показателя F/km, значими различия се установяват между категориите „Задоволително“ и „Незадоволително“, както и между „Незадоволително“ и „Лошо“. Това показва, че разпределението на произшествията, със загинали лица, не следва същата последователна тенденция като общия брой ПТП.

Допълнително е оценена монотонната зависимост, чрез коефициента на ранговата корелация на Спирман. За показателя ПТП/km е получена слаба, но статистически значима положителна зависимост $\rho = 0.0557$, $p < 0.001$, която потвърждава общата тенденция за увеличаване на концентрацията на произшествия при влошаване на състоянието на настилката. За F/km не е установена статистически значима монотонна зависимост ρ=0.0017, p=0.874, което показва, че тежестта на произшествията не се изменя еднопосочно спрямо категорията на настилката. Полученият резултат подчертава комплексния характер на факторите, влияещи върху тежките пътнотранспортни произшествия.

3 Обсъждане

Получените резултати показват, че интегрирането на пространствени данни от различни източници създава предпоставки за извършване на значително по-задълбочени анализи в областта на пътната безопасност. Използването на ГИС позволява не само пространственото обединяване на информация за състоянието на пътната инфраструктура и настъпилите ПТП, но и извличането на количествени показатели, които могат да бъдат подложени на последваща статистическа оценка.

Използваният пространствен анализ е надеждно средство за идентифициране на участъци с повишена концентрация на произшествия и за оценка на връзката между състоянието на настилката и показателите за пътна безопасност. Получените резултати не следва да се разглеждат еднозначно, като доказателство за пряка зависимост, а като пример за възможностите на ГИС да подпомага откриването на значими пространствени закономерности и да насочва вниманието към участъци, които изискват по-задълбочено обследване.

Практическата стойност на подобен подход се състои във възможността различни пространствено свързани данни, да бъдат обединявани в единна информационна среда и използвани като основа за аргументирано планиране на последващи дейности, свързани с управлението и повишаването на пътната безопасност.

Заключение

Демонстрирани са възможностите на ГИС като инструмент за интегриране, анализ и визуализация на пространствено свързани данни в областта на пътната безопасност. Чрез комбиниране на информация за състоянието на пътната инфраструктура и регистрираните ПТП, е разработен и предложен подход, който позволява количествена оценка на пространствените зависимости на тези параметри и тяхната статистическа проверка.

Получените резултати показват, че подобен подход може да подпомогне идентифицирането на участъци с повишен риск, както и да предостави обективна информационна основа при планирането на дейности, свързани с поддържането и ефективното управление на пътната инфраструктура, ориентирано към повишаване на безопасността на движението. Същевременно, методиката позволява лесно разширяване, обхвата на анализа, чрез включване на допълнителни пространствени данни, което от своя страна създава предпоставки за разработване на по-комплексни модели, подпомагащи процеса на вземане на адекватни управленски решения.

Литература

1. Андреева П., (2023). „Геоинформационни технологии“ – монография, НВУ „В. Левски“ Шумен 2023 г., ISBN 978-954-753-368-4
2. Андреев, А., Андреева П., (2021). Геоинформатика,геоинформационн и системи, геоинформационни технологии“ – монография НВУ „В.Левски“ В. Търново, ISBN - 978-619-7531-24-4

3. Господинов, С., Ламбева, Т., (2024). Основни вероятностни и статистически аспекти с приложение в геодезията, ISBN 978-619-277-046-4, София
4. Държавна агенция „Безопасност на движението по пътищата" - Интерактивна карта на състоянието на безопасността на пътната инфраструктура в Република България, 13.07.2026г.
5. Илиева, Т., Иванова, Й., Славчева, К. (2024). Приложение на гис за идентифициране и оценка на риска за пътната инфраструктура от възникване на свлачищни процеси – проучване за територията на област Сливен, България, Годишник на Университета по архитектура, строителство и геодезия, софия, Том 57, Брой 2
6. Министерство на вътрешните работи - Актуални данни за ПТП в периода от 01.01.2024 до момента, 13.07.2026г., Държавна агенция "Електронно управление", Отдел "Данни"
7. Миланов, Р., (2017). Директива за управление безопасността на пътната инфраструктура. Одит и инспекция по пътна безопасност, Семинар на тема: „Към ВИЗИЯ 0 жертви от ПТП", гр. Правец
8. Щерева, К., Пеев, И., Марков, М., (2022). Анализ на времево обусловените премествания на дискретни точки от стената на яз. Златогад, Сборник с доклади от Осма национална научно-техническа конференция с международно участие, Девин, ISSN 1314-7056
9. Kunchev, I., Angelova, M., (2023). Development of a Conceptual Model of a Road Accident Geoinformation System, Kartografija i geoinformacije, Vol. 22, No. 39, pp. 4–19, https://doi.org/10.32909/kg.22.39.1
10. Nurulfajri, N., Arifin, S., (2025). A Review of Kruskal–Wallis Test Applications in Scientific Research, Journal of Actuarial, Finance and Risk Management (JAFRM) e-ISSN:28303938 Vol. 4(2), December, 2025
11. Smeeton, N., Spencer, N., Sprent, P., (2025). - Applied Nonparametric Statistical Methods, 5th Edition, ISBN 9780367344894
12. Susilowati, A, Rachmat, H., Anna, N., Elfiati, D., (2025). Stand composition and structure of Rubroshorea curtisii in a lowland Dipterocarp remnant forest of Bukit Tiban, Riau Islands, Indonesia, Biodiversitas Journal of Biological Diversity 26(9), DOI:10.13057/biodiv/d260948

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

INTEGRATION OF MACHINE LEARNING IN CLASSICAL GRAVIMETRY AND GNSS STUDIES

Marko Markov

Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levski"
markomarkov8@abv.bg

***Abstract**: An innovative framework for integrating machine learning into classical gravimetry is proposed, aiming to transition from interpolation to predictive multifactor modeling. By analyzing topographic parameters in high-relief terrains and applying suitable algorithms, the identification of local anomalies and the design of geodetic networks are optimized, by reduces fieldwork, without compromising accuracy.*

***Keywords:** Machine Learning, Gravimetry, GNSS, Predictive Modeling*

Въведение

Определянето на силата на тежестта и локалните гравитационни аномалии е фундаментална задача в съвременната физическа геодезия. Традиционно за локализиране на подземни структури, кухини или различни природни залежи се прилагат съвместни релативни гравиметрични измервания и такива реализирани с помощта на глобални навигационни спътникови системи (GNSS). Подобни класически подходи са доказали своята ефективност през годините – както при откриването на солни находища [7], така и при определянето на дълбочинните параметри на карстови форми и подземни кухини, чрез детайлен анализ на аномалиите на Буге (Bouguer) и локалните аномалии [8].

Въпреки тяхната надеждност, конвенционалните методи изискват създаването на геодезически мрежи, с голяма гъстота и провеждането на мащабни полеви измервания. При значими по площ терени с голяма денивелация и сложен релеф, класическата интерполация на гравиметричните данни може да се окаже недостатъчна, за прецизно локално моделиране, а самата теренна работа е изключително времеемка и изисква значителен ресурс. Това налага търсенето на нови аналитични подходи, които да оптимизират процеса.

През последните години внедряването на алгоритми за машинно обучение (Machine Learning – ML) предизвика фундаментална трансформация, в анализа на пространствени и гравиметрични данни. В практиката все по-често се преминава от стандартни математически модели, към прогнозно моделиране. Методите на машинното обучение вече намират успешно приложение при прогнозирането на гравитационни аномалии [11] и при решаването на версията на обратната гравиметрична задача, като например възстановяването на данни за подземни водни запаси, чрез комбиниране на гравиметрия и алтиметрия (барометрични измервания) [12]. Специфични подходи, като графовите невронни мрежи (GNNs), показват висок потенциал при анализа на гравиметрични данни и детекцията на кухини [10]. Графовите невронни мрежи са вид изкуствен интелект, създаден да

анализира данни, които имат сложна структура на мрежата. За разлика от обикновените невронни мрежи, които обработват таблици, текст или изображения, GNN работят с обекти и връзките между тях [14].

Потенциалът на алгоритмите за прецизно прогнозиране е доказан и в други интердисциплинарни изследвания, базирани на комбиниран сензорен мониторинг [10].

Предложена е иновативна методологична рамка, която интегрира машинно обучение в класическата гравиметрия, осигурявайки преход от конвенционална интерполация към прогнозно многофакторно моделиране. Основната цел е, чрез анализ на топографските параметри (при терени с голяма денивелация) и прилагане на подходящи алгоритми, да се оптимизира и прецизира идентифицирането на локални аномалии и проектирането на геодезически мрежи.

1 Концептуална методологична рамка

Надеждността на всеки локален, или регионален модел, на гравитационното поле, зависи пряко от качеството на първичните данни и математическите методи, използвани за тяхната обработка и пространствена интерполация [2][3]. Внедряването на съвременни алгоритми изисква преосмисляне на досегашните подходи към редукциите и калибрирането на измерванията.

1.1 Ограничения на конвенционалните подходи и влияние на редукциите

Класическата обработка на гравиметрични данни разчита на интерполационни методи (например популярния "Кригинг" метод) при визуализация на аномалиите, за дадена територия. Тези методи предполагат плавен преход на стойностите между отделните дискретни точки. При терени с рязка промяна в надморската височина обаче зависимостта между топографията и гравитационното поле е силно нелинейна [16].

Прилагането на математически редукции към измерените пространствени величини (например преминаването към проекционни равнини) може да доведе до съществено изкривяване на физическия модел [9]. Подобен проблем възниква и в гравиметрията – свеждането на 3D топографските маси, към опростени 2D модели на аномалиите на „Буге", или „Свободен въздух" където често се губи ценна пространствена информация, особено в зони с ниска плътност на измерванията [5].

1.2 Ролята на еталонните измервания като основа за AI модели

За да бъдат алгоритмите за машинно обучение ефективни, те се нуждаят от масиви с висококачествени данни. Това превръща прецизните измервания в изключително важен компонент, от новата концептуална рамка. Създаването и поддържането на еталонни гравиметрични полигони и калибрационни линии позволява събирането на надеждни абсолютни и релативни данни [1][4]. Интегрирането на високоточни измервания от надеждни локални мрежи гарантира, че референтните данни (Ground Truth), подавани към невронните мрежи, не са обременени от систематични инструментални грешки (например дрейф на нулата на гравиметъра) или неправилно калибриране на апаратурата.

1.3 Преход към прогнозно многофакторно моделиране

Вместо да разчита на линейна или пространствена зависимост между съседни точки, предложената рамка използва машинното обучение като многофакторен инструмент за прогнозиране. Схемата на решение включва:

- Входни параметри: Пространствени координати (X, Y), елипсоидна височина (H), получена в резултат от GNSS измервания и топографски характеристики (наклон, кривина на терена).
- Изходни параметри: Стойности на силата на тежестта (g) и съответните гравиметрични аномалии.
- Моделиране на нелинейността: Алгоритъмът изгражда математическа функция, която не просто интерполира данните на картата, а предвижда гравиметричната стойност въз основа на сложни взаимовръзки между терена и плътността на масите.

Този подход решава проблема с редукционните изкривявания, тъй като моделът се "обучава" директно чрез тримерните координати и не изисква предварително геометрично "сплескване" на данните в 2D пространството.

2 Формиране на входните параметри и избор на алгоритми

Успешното внедряване на машинно обучение в гравиметрията зависи от процеса на извличане и структуриране на признаците. За да е в състояние един алгоритъм да предвижда точно гравитационните аномалии или да локализира подземни структури, той трябва да бъде захранен с оптимален набор от пространствени и морфологични данни.

2.1 Дефиниране на обучаващия набор от данни

Основните входни параметри включват:

- Пространствени координати: Геодезически координати (X, Y) и елипсоидни височини (H), придобити чрез високоточни GNSS измервания.
- Топографски характеристики: Наклон на терена, кривина и др., извлечени от надежден цифров модел на релефа (DEM). Тези метрики са ключови за обучението на модела, да разпознава гравитационните ефекти на видимите топографски маси.
- Целеви променливи : Реално измерените и коригирани стойности на аномалиите "свободен въздух" и аномалиите "Буге".

2.2 Разпознаване на слаби сигнали и дълбочинни структури

Специфично предизвикателство в приложната гравиметрия е локализирането на дълбочинно разположени кухини. Съвременните гравиметрични методи имат потенциала да откриват подобни структури, но интерпретацията им е силно затруднена от "затихването" на гравитационния сигнал в дълбочина и маскиращия ефект на повърхностния релеф [6].

Машинното обучение предлага решение на този проблем. Обучен върху достатъчно голям масив от точки, алгоритъмът може да се научи да изолира "шума", генериран от сложния терен, както и да идентифицира специфичните микро-аномалии, характерни за липсващи маси в дълбочина. Това превръща ML модела във високочувствителен дигитален филтър.

2.3 Статистическа оценка на различията между категориите състояние на настилката

Изборът на архитектура зависи от обема на данните и спецификата на терена [13][15]:

- Комбинирани методи: Тези алгоритми изграждат множество „дървета на решенията“ и са изключително подходящи за ползване на таблични данни (координати и височини). Те се справят отлично с нелинейни зависимости и са устойчиви на екстремни стойности в сложен релеф.
- Изкуствени невронни мрежи и графови мрежи: За по-мащабни мрежи, невронните модели могат да "картират" сложните 3D пространствени връзки между точките, улавяйки фини вариации в плътността на земната кора, които стандартната статистическа интерполация пропуска.
- “Опорни вектори” (SVR): При локални мрежи с по-малък брой измервания (под 500 точки), SVR осигурява висока прецизност при прогнозирането на аномалиите, минимизирайки риска от преобучаване на модела.

3 Оценка на модела и оптимизация на полевите измервания

3.1 Валидиране и оценка на точността

За да бъде приложим в реални геодезически задачи, всеки ML модел преминава през строг процес на проверка и одобряване. Обичайно масивът от измервания (например 250–300 реални точки от даден терен) се разделя на тренировъчен (80%) и тестов набор (20%). Моделът се "обучава" с данните от първата част, след което "предсказва" стойностите на гравитационните аномалии за скритата тестова извадка. Точността на алгоритъма се оценява чрез Средна квадратна грешка (RMSE) и Средна абсолютна грешка (MAE). Когато прогнозираните стойности на Δg се отклоняват от реално измерените в рамките на допустимата инструментална грешка (например под 0.05 mGal), моделът се счита за успешен и готов за приложна експлоатация.

3.2 Валидиране и оценка на точността

При класическото планиране на гравиметрични рейсове в сложен релеф се залага на равномерна гъстота на точките, което често води до прекомерни разходи и излишни измервания в еднородни зони. Обученият ML алгоритъм позволява обратен подход – прогнозно планиране. Чрез анализ на топографските особености, моделът може предварително да маркира зоните с очаквано високо гравитационно "разсейване". Това дава възможност, на геодезическите екипи, да съсредоточат измерванията (GNSS и гравиметрични) единствено върху значимите участъци. Стойностите за останалите, по-предсказуеми зони

Заключение

Интегрирането на алгоритми за машинно обучение бележи една естествена “крачка“ при анализа на съвместни гравиметрични и GNSS измервания. Предложената, в настоящата статия, концептуална рамка демонстрира, че AI технологиите не заместват прецизните физически методи, а ги надграждат.

Преходът от стандартна интерполация, към прогнозно многофакторно моделиране, позволява заобикаляне на "изкривяванията", съпътстващи класическите редукции при силно пресечен релеф. Нещо повече, способността на алгоритмите да филтрират топографския шум отваря нови възможности за локализиране на дълбочинни кухини и слаби аномални зони. В крайна сметка, синергията между класическата геодезия и науката за данните (Data Science) води до оптимизиране на полевите гравиметрични рейсове, значително намаляване на разходите и повишаване на надеждността на локалните гравиметрични модели.

Литература

1. Андреев, А., Андреева, П., Димова, Г., Моделиране на геоида (квазигеоида) за област Търговище, Proceedings of International Scientific Conference "Defense Technologies – DefTech 2024", Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, pp. 529-544, ISSN 2367-7902
2. Андреев, А., Съвременни методи за локално моделиране на геоида, Шумен 2008г, ISBN - 978-954-9681-40-6
3. Господинов, С., Пенева – Златкова, Е., Андреев, А., Михайлов, Г., АНАЛИЗ НА ДЪРЖАВНАТА ГРАВИМЕТРИЧНАТА МРЕЖА НА РЕПУБЛИКА БЪЛГАРИЯ, Доклад на работна група по задача 3.3. Създаване на Програма за обновяване и усъвършенстване на Държавните геодезически мрежи (Държавна гравиметрична мрежа) към Съвета по геодезия, картография и кадастър, 2014
4. Господинов, С., Пенева, Е., Ламбева, Т., Радев, И., ИЗГРАЖДАНЕ НА НАЦИОНАЛЕН ЕТАЛОНЕН ГРАВИМЕТРИЧЕН ПОЛИГОН, ГОДИШНИК НА УНИВЕРСИТЕТА ПО АРХИТЕКТУРА, СТРОИТЕЛСТВО И ГЕОДЕЗИЯ, СОФИЯ 2018, ТОМ 51, Брой 12, ISSN 2534-9759
5. Господинов, С., Постоловски, А., Хаджиева, Б., Марков, М., Определяне и генериране на гравиметрични аномалии в района на гр. Златоград, Proceedings of the XI International Geomechanics Conference 16 – 20 September 2024, Golden Sands Resort, Bulgaria, стр. 104-111, ISSN: 1314-6467
6. Славова, Т., ЛОКАЛИЗИРАНЕ НА ДЪЛБОЧИННО РАЗПОЛОЖЕНИ КУХИНИ, ПОСРЕДСТВОМ ГРАВИМЕТРИЧНИ МЕТОДИ, ИК „Свети Иван Рилски", София, 2026 г., ISBN 978-954-353-504-0
7. Djorova, S., Localization of salt deposits by using of combined relative gravimetric and navigational GPS measurements, 6th International Scientific Conference on Modern Management of Mine Producing, Geology and Environmental protection, SGEM 2006
8. Djorova, S. & Nikolova, M., DETERMINATION OF DEPTH PARAMETERS OF SUBSURFACE VOIDS USING GRAVIMETRIC AND GLOBAL NAVIGATION SATELITTE SYSTEMS MEASUREMENTS, SGEM OnLine

Scientific Library from the 24th International Multidisciplinary Scientific GeoConference, 2024, 475-482. 10.5593/sgem2024/1.1/s05.60.

9. Gospodinov, S., Peneva, E., Lambeva, T., Investigation of Crustal Deformation by the Means of Directly Defined Spatial Chords – Possibility or Predeterminancy, World Multidisciplinary Earth Sciences Symposium (WMESS 2019), IOP Conf. Series: Earth and Environmental Science 362 (2019) 012155, doi:10.1088/1755-1315/362/1/012155
10. Panda, G., Singh, V., Kumar, A., Saharia M., Kumar, S., Graph Machine Learning Framework for Gravimetry Data Analysis and Cavity Detection," in IEEE Transactions on Artificial Intelligence, vol. 7, no. 7, pp. 3897-3912, July 2026, ISSN: 2691-4581, doi: 10.1109/TAI.2025.3648693.
11. Zhanakulova, K., Adebiyet, B., Orynbassarova, E., Yerzhankyzy, A., Kassymkanova, K, Abdykalykova, R., Zakariya, M., Application of Machine Learning Methods for Gravity Anomaly Prediction. Geosciences 2025, ISSN: 2076-3263, https://doi.org/10.3390/geosciences15050175
12. Irrgang C., Saynisch-Wagner, J., Dill, R., Boergens, E., Thomas, M., Self-Validating Deep Learning for Recovering Terrestrial Water Storage From Gravity and Altimetry Measurements, Geophysical Research Letters, 27 August 2020, ISSN:1944-8007, https://doi.org/10.1029/2020GL089258
13. Reiman, L., Random Forests, Machine Learning, 45, 5–32, 2001, ISSN 1573-0565, https://doi.org/10.1023/A:1010933404324
14. 14. Noble, J., What is a GNN (graph neural network), IBM, https://www.ibm.com/think/topics/graph-neural-network [viewed 2026-08-03].
15. Hastie, T., Tibshirani, R., Friedman, J., The Elements of Statistical Learning Data Mining, Inference, and Prediction, Second Edition, Stanford, California, August 2008, ISBN 978-0387848570
16. Xia, J., Correction of topographic distortions in potential-field data: A fast and accurate approach. GEOPHYSICS, VOL. 58, NO. 4 (APRIL 1993), P. 515-523

ANALYSIS OF METHODS FOR CREATING AN UNDERGROUND CADASTRE

Petina A. Andreeva, Hristiyan Georgiev

Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levski" petiand@abv.bg
Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levski"

***Abstract**: The underground cadastre is a necessary and strategically important tool for modern territorial management. Its implementation and development create conditions for the efficient, safe, and sustainable use of underground space, while simultaneously meeting the growing demands of modern society.*

***Keywords:** GIS, CADASTRE, vertically planning S*

АНАЛИЗ НА МЕТОДИТЕ ЗА СЪЗДАВАНЕ НА ПОДЗЕМЕН КАДАСТЪР

Петина Андреева, Християн Георгиев

Въведение

Подземният кадастър представлява съществено направление в развитието на съвременните кадастрални системи, породено от необходимостта за по-пълно и точно отразяване на пространството под земната повърхност. Неговото предназначение е свързано със събирането, поддържането и управлението на информация за подземни инженерни мрежи, транспортни съоръжения, подземни сгради и други обекти, които имат важно значение за функционирането на урбанизираните територии. За разлика от традиционния кадастър, който е насочен предимно към обектите на земната повърхност, подземният кадастър въвежда вертикалното измерение като неразделна част от пространственото описание и по този начин осигурява по-пълна представа за реалното устройство на територията.

Тясната връзка между подземния и тримерния кадастър показва необходимостта от прилагане на нови подходи за моделиране и управление на пространствената информация, които да отчитат сложните пространствени взаимоотношения между надземните и подземните обекти. Това е особено важно в условията на интензивна урбанизация, когато различни инженерни съоръжения и инфраструктурни елементи често се пресичат или разполагат на различни нива под земята. Наличието на точна и актуална информация за тяхното местоположение е от съществено значение за устройственото планиране, инвестиционната дейност, поддръжката на инженерната инфраструктура и предотвратяването на аварийни ситуации.

Освен техническите си функции, подземният кадастър има важно значение и от правна гледна точка, тъй като създава условия за ясно определяне на правата върху

подземното пространство и за намаляване на възможностите за възникване на спорове. Същевременно интегрирането на данни за геоложките и хидрогеоложките условия подпомага устойчивото управление на природните ресурси и опазването на околната среда. [2],[3].[4].[5],[6],[7],[9],[10].

Всичко това определя подземния кадастър като необходим и стратегически важен инструмент за съвременното управление на територията, който създава предпоставки за безопасно, ефективно и устойчиво използване на подземното пространство в условията на постоянно нарастващи обществени и инфраструктурни потребности

1. Обект за изследване

За изследването е избран обект: територията на Националния военен университет „Васил Левски", факултет А, ПВО и КИС, разположен в град Шумен.

Избраният обект представлява обособена урбанизирана територия със специално предназначение, в рамките на която са разположени редица подземни инженерни съоръжения, обслужващи учебния и административния процес на факултета.

Целта е да се изследват съществиващите подземни съоръжения, разположени под територията на факултета, включително водопроводни и канализационни мрежи, газопроводи, електроразпределителни линии, оптични и телекомуникационни кабели, както и да се анализират методите по планиране, проектиране и нанасянето им в актуален цифров вид с цел бъдещо използване.

За постигане на целта се премина през следните етапи от работния процес:

1. Извърши се проучване и анализиране на съществуващите планове на подземните съоражения.

2. Извършиха се реални геодезически измервания и обработка на данните за обекта.

3. Направи се анализ на методите за създаване на подземен кадастър.

2. Входни данни и използвана информация

Като основен пространствен ориентир е използвана действащата кадастрална карта за територията на Националния военен университет „Васил Левски", факултет А, ПВО и КИС, гр. Шумен. Кадастралната карта предоставя информация за границите и обхвата на имотите, но не съдържа детайлни данни за подземните съоръжения, което налага използването ѝ предимно като базов план за последващо наслагване и анализ на допълнителна информация. Заедно с това са използвани и наличните архивни хартиени планове и схеми, които отразяват отделните елементи на подземната инфраструктура. Поради разликите в годините им на изготвяне, се наблюдават големи разлики и несъответствия. Данните в тях са актуални до определена степен, но като цяло са непълни и не обхващат цялата територия на обекта. По отношение на отделните видове подземни мрежи е налична сравнително по-пълна информация за газопроводната мрежа, за която съществува схема, както и частична информация за водопроводната мрежа и оптичните кабели. Основните липси в изходните данни са свързани с отсъствието на надлъжни и

напречни профили, липсата на координатна информация, данни за дълбочината на полагане на съоръженията и отсъствието на единна система за отразяване на подземната инфраструктура. За компенсиране на част от липсващата информация са извършени теренни огледи и визуални наблюдения, които са използвани за ориентиране в разположението на видими елементи и за потвърждаване или коригиране на наличните данни.

В обобщение може да се каже, че използваните изходни данни са разнородни, непълни и с различна степен на надеждност, което отразява реалните условия при работа с подземна инфраструктура.

3. Приложени методи и технологии

Изборът на методи и технологии при изпълнението на конкретния обект беше съобразен както с поставените цели, така и с реалните теренни условия, наличната документация и техническите ограничения. Основната задача се заключава в отразяване на съществуващите и новоизградени подземни мрежи и съоръжения, контрол върху изпълнението на строителните дейности и актуализиране на кадастралната информация.[1], [12],[13].

За изследвания обект се избра да се използва тахиметрично заснемане с тотална станция (Hi-Target HTS-420R) и ГНСС измервания с RTK приемник. Обработката на данните премина през последователно използване на няколко софтуера TPLAN, MKAD и AutoCAD.

4. Геодезическа снимка

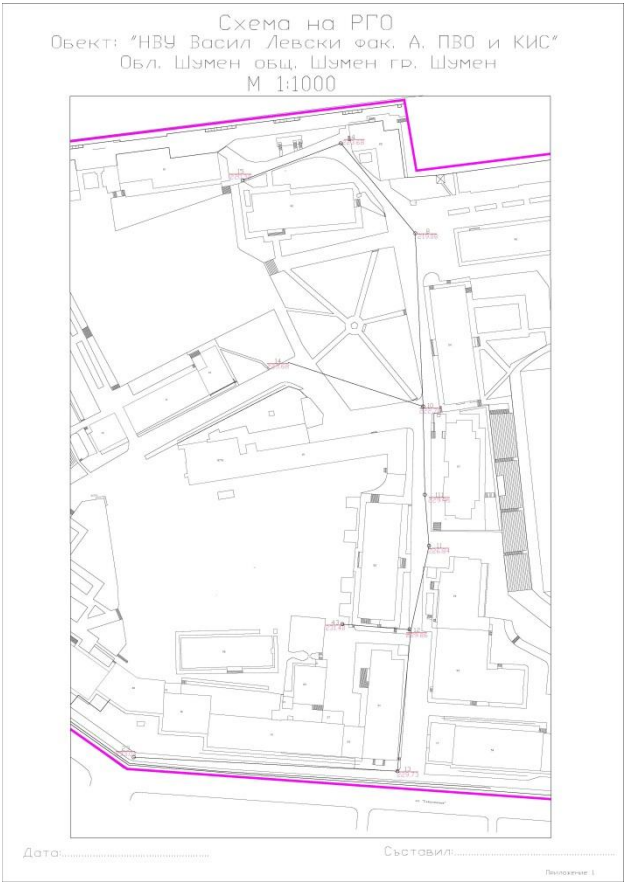
Геодезическите измервания бяха извършени чрез комбинирано използване на класически тахиметрични методи и спътникови технологии за позициониране. Прилагането на този подход позволява съчетаване на високата точност на тахиметричните измервания с бързината и ефективността на GNSS наблюденията, което е особено подходящо при работа в урбанизирана среда и при заснемане на инженерна инфраструктура.[11],[14],[15],[16]

За изпълнението на теренните измервания беше използвана тотална станция Hi-Target Total Station Model HTS-420R (2"), предназначена за инженерно-геодезически дейности и измервания с висока точност. Инструментът позволява извършването на прецизни ъглови и линейни измервания, което го прави подходящ за детайлно заснемане на инженерни съоръжения и характерни точки от инфраструктурата. Тоталната станция беше използвана основно за тахиметрично заснемане на характерни точки от подземните съоръжения, както и за извършване на измервания, свързани с определяне на дълбочината на отделните тръбопроводи. При наличието на разкрити участъци от инженерните мрежи беше възможно директно да се измерят както хоризонталното положение, така и вертикалното разположение на съответните елементи.

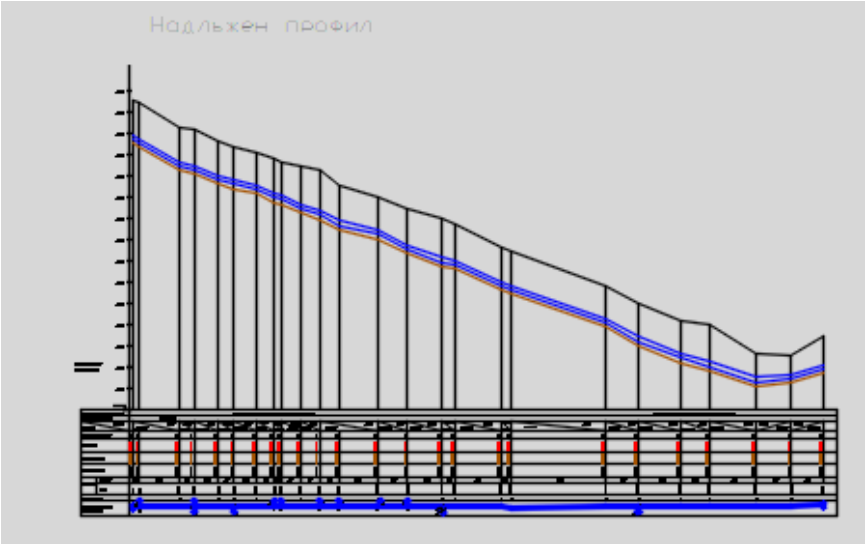
Паралелно с това беше използвана и спътникова измервателна техника – GNSS RTK система на Hi-Target, която позволява определяне на координатите на точки с висока точност в реално време. GNSS приемникът беше използван основно при заснемането на шахтовите съоръжения и други лесно достъпни точки от

инфраструктурата, които се намират на повърхността на терена. Чрез този подход беше възможно бързо да се събере значителен обем пространствена информация, като същевременно се запази необходимото ниво на точност за целите на настоящото изследване.

Комбинираното използване на тотална станция и GNSS приемник позволи да се постигне по-ефективна организация на измервателния процес. [17],[18].



Фиг. 1: РГО на обекта и геодезическа снимка



Фиг. 2: Схема на надлъжен профол на водопровода

Заключение

В резултат на извършеното заснемане и последващата обработка на данните бяха създадени няколко основни крайни продукта. На първо място беше изготвен актуализиран подземен план на част от разглежданата територия, който отразява установеното положение на новосъздадения водопровод. Този план представлява важен инструмент за визуализация и анализ на подземната инфраструктура.

Освен това беше създаден подробен CAD чертеж, в който всички събрани данни са организирани в отделни тематични слоеве. Тази организация позволява ясно разграничаване на различните видове инженерни мрежи и улеснява работата с чертежа при бъдещи анализи или допълнения. Всеки вид инфраструктура е представен в самостоятелен слой, което дава възможност за селективно визуализиране и редактиране на информацията.

Към CAD чертежа беше разработена и схема за обозначаване на различните инженерни мрежи, видими по време на ремонтните дейности, която осигурява ясна и еднозначна интерпретация на използваните символи и графични елементи. Това е важна част от документацията, тъй като гарантира, че създадената информация може да бъде използвана и от други специалисти.

Изследването потвърждава, че въвеждането на подземен кадастър е необходима стъпка за повишаване на безопасността, подобряване на координацията между институциите и по-ефективното управление на подземното пространство. Реализирането на единна цифрова информационна система би

улеснило актуализирането на данните, вземането на инженерни решения и дългосрочното планиране на развитието на техническата инфраструктура.

Литература

1. Андреев А. И..Инженерни, природонаучни и други направления на приложната геодезия част II. ШУ „Епископ Константин Преславски" Шумен 2020 г.
2. Господинов, С., Марков, М., Хаджиева, Б. /2024г./ Применение лазерного сканирования для обследования объектов, имеющие отношение к безопасности дорожного движения, Современные информационные технологии. Сборник научных статей по материалам 10-й Международной научно-технической конференции, стр. 337-346, Москва 2024г., УДК 004.65, ББК 32.973.26-018.2, eLIBRARY ID: 68606783, https://elibrary.ru/item.asp?id=68606783
3. Господинов, С., Постоловски, А., Хаджиева, Б., Марков, М., /2024г./ Определяне и генериране на гравиметрични аномалии в района на гр. Златоград, Proceedings of the XI International Geomechanics Conference 16 – 20 September 2024, Golden Sands Resort, Bulgaria, стр. 104-111, ISSN: 1314-6467
4. Димитров, М., Марков, М., Хаджиева, Б. /2021г./ Създаване на 3D модел на стена на хвостохранилище по резултати от наземно лазерно сканиране, Сборник с доклади от Национална научно-техническа конференция "Управление и безопасност на хвостохранилища", стр. 85-90, ISBN 978-619-90939-7-9
5. Димова Г. Общи принципи, прилагани при управлението на риска от природни бедствия. Proceedings of International Scientific Conference "Defense Technologies" DefTech 2025,Faculty of Artillery, Air Defense and Communication and Information Systems.Стр.1083-1092, ISSN2815-4282 – онлайн издание.
6. Димова Г. Управление на риска при наводнения. International Scientific Conference "Defense Technologies" DefTech 2025,Faculty of Artillery, Air Defense and Communication and Information Systems. Стр.1076-1084, ISSN2815-4282 –онлайн издание
7. Димова Г. Управление на риска при свлачища, срутища и земни пропадания. . International Scientific Conference "Defense Technologies" DefTech 2025,Faculty of Artillery, Air Defense and Communication and Information Systems. Стр.1066-1076, ISSN2815-4282 –онлайн издание
8. ИНСТРУКЦИЯ И УСЛОВНИ ЗНАЦИ ЗА ИЗРАБОТВАНЕ И ПОДДЪРЖАНЕ НА ПЛАНОВЕ НА ПОДЗЕМНИ ПРОВОДИ И СЪОРЪЖЕНИЯ, Министерството на строителството и селищното устройство - Главно управление по геодезия, картография и кадастър през 1984 г
9. Марков, М., Митев, И. /2024г./ Применение лазерного сканирования для картографирования картирования горных образований, Современные информационные технологии. Сборник научных статей по материалам

10-й Международной научно-технической конференции, стр. 453-464, Москва 2024г., УДК 004.65, ББК 32.973.26-018.2, eLIBRARY ID: 68606793, https://elibrary.ru/item.asp?id=68606793

10. Марков, М., /2024г./ Развитие гео роботов, Сборник научных статей по материалам 2-й Международной научно-практической конференции "Интеллектуальные и киберфизические системы: управление, логистика, безопасность", Страницы: 95-106, Номер: 3 (45), Год: 2024, УДК 004, ББК 22.18, eLIBRARY ID: 68620146, https://elibrary.ru/item.asp?id=68620146
11. Марков, М., /2025г./ Анализ дорожных рисков с применением лазерного сканирования, Сборник научных статей по материалам 7-й Международной научно-практической конференции "Методы и модели пространственного анализа", Страницы: 134-142, Номер: 1 (47), Год: 2025, УДК 004, ББК 22.18, eLIBRARY ID: 79510275, https://elibrary.ru/item.asp?id=79510275
12. НАРЕДБА № 8 ОТ 28 ЮЛИ 1999 Г. ЗА ПРАВИЛА И НОРМИ ЗА РАЗ-ПОЛАГАНЕ НА ТЕХНИЧЕСКИ ПРОВОДИ И СЪОРЪЖЕНИЯ В НАСЕ-ЛЕНИ МЕСТА
13. НАРЕДБА № РД-02-20-2 ОТ 20 ДЕКЕМВРИ 2017 Г. ЗА ПЛАНИРАНЕ И ПРОЕКТИРАНЕ НА КОМУНИКАЦИОННО-ТРАНСПОРТНАТА СИСТЕМА НА УРБАНИЗИРАНИТЕ ТЕРИТОРИИ TEPLAN, MKAD – Софтуерни продукти – България – 2024 г.
14. Постоловски, А., Димитров, М., Марков, М. /2021г./ Приложение на MTLS – технология при одит на тунелното строителство, XVI международна конференция по открит и подводен добив на полезни изкопаеми, стр. 279-285, Варна 2021г., ISSN 2535-0854
15. Хаджиева, Б., Господинов, С., Марков, М., /2025г./ Необходима ли е геодезическа мрежа с местно предназначение при създаване на кадастрална карта за урбанизирана територия, Списание "Минно дело и геология", Брой 1-2/2025, Година LXXIX, ISSN 0861 – 5713, ISSN 2603 – 4549 (Online)
16. Щерева К., Пеев И., Марков М. /2022г./ Анализ на времево обусловените премествания на дискретни точки от стената на яз. „Златоград“, Осма национална научнотехническа конференция с международно участие, стр. 81-87, Девин 2022г., ISSN 1314-7056
17. Andreev A., Andreeva G. Modeling of the river system of Goliama Kamchia. Journal "Scientific and applied research", vol.2, p.50-58, 2012 ISSN 1314-6289 София – 2016 г.
18. Markov, M., /2026/ Assessment and monitoring of road marking reflectivity using mobile laser scanning to improve road safety, Trakia Journal of Sciences, Vol. 24, No 2, pp 192-196, 2026, ISSN 1313-3551 (online), doi:10.15547/tjs.2026.02.014

FLOODING RISK ASSESSMENT IN THE KAMCHIA RIVER BASIN AFTER APPLICATION OF MULTI-CRITERION ANALYSIS

Gergana Dimova

Department Artillery, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levski"
geriandimova@gmail.com

Abstract: *Multi-criteria analysis (MCA) is a methodological approach used to prioritize different alternatives through the analysis of a number of structured criteria. It is a complex tool for evaluating and selecting options. When selecting options, a numerical value is assigned to individual criteria that allow for quantitative measurement (of the relevant options) and allow their comparison. The criteria are weighted, emphasizing their relative importance. The weighted sum of the different selected criteria is used to prioritize the evaluated options. As a methodology, MCA is a structured framework that allows for combining expert assessments when using it, and is suitable for decision-making when the options cannot be quantified.*

On this basis, the report assessed the flood risk along the Goliama Kamchia River. The results obtained show no significant differences from the MCA for the entire country.

Keywords: *MCA, risk, Goliama Kamchia River*

ОЦЕНКА НА РИСКА ОТ НАВОДНЕНИЯ ПО ПОРЕЧИЕТО НА РЕКА КАМЧИЯ СЛЕД ПРИЛАГАНЕ НА МНОГОКРИТЕРИАЛЕН АНАЛИЗ

Гергана Димова

Въведение

Оценката на риска от наводнения е от изключително значение за националната ни сигурност. Във тази връзка държавното ръководство на РБългария полага сериозни усилия в материално и методическо отношение. На базата на опита от нашия и чуждестранен опит бяха подготвени на национално и регионално ниво редица документи, като: Национална програма за намаляване на риска от бедствия 2021-2025 г., Национална стратегия за намаляване на риска от бедствия – 2018-2030г., План за управление на риска от бедствия в България 2022г. и др.



Фиг.1: Връзка между стратегическите и планиращи документи отнасящи се до защитата при бедствия (Национална стратегия за намаляване на риска от бедствия – 2018-2030г.)

В тези документи основната цел е осъществяването на мониторинг на риска от природни бедствия и техногенни катастрофи. Това се постига чрез осъществяване на наблюдения и оценка на мерките съдържащи се в предварително подготвените документи.

Този процес предполага събирането на данни (количествени и качествени), които да се съпоставят с изходното състояние и бъдещите резултати. Събирането и анализа на информацията се базира на подходящи критерии, които се залагат в годишните планове на национално и регионално ниво. Основните фактори са: Индикатори за ресурси, Индикатори за резултат, Индикатори за въздействие. Те включват в себе си: мярка, цел, източник на информация, честота на измерването.

В Плана за управление на риска от бедствия в България 2022 г. са дадени оценките за всяка опасност след проведен многокритериален анализ. Общата оценка за всяка мярка е с комбинирана тежест от горните критерии, като оценката е между 1 и 3 (1- най-нисък приоритет, 3 –с най-висок приоритет).

В таблица 1 са дадени индикаторите от многокритериалния анализ за риска от наводнения. (План за управление на риска от бедствия в България 2022г).

Таблица 1. Многокритериалния анализ за риска от наводнения в РБългария

Критерии и тежест	**Значение на риска**	**Ефикасност**	**Ефективност**	**Устойчивост**	**Капацитет**	**Спешност**	**Обща оценка**
Мерки	*25%*	*20%*	*20%*	*15%*	*10%*	*10%*	*100%*
1. Повишаване на готовността и подобряване на реагирането на населението	2	3	3	3	3	3	**2.8**
2. Прилагане на системи за ранно предупреждение (СРП), специално насочени към поройните наводнения, или на системи за ранно предупреждение за множество опасности с разработен модул за наводнения.	2	3	3	3	2	3	**2.7**
3. Поддържане на стабилна правна, административна и икономическа рамка за прилагане на политиката за защита от наводнения	2	3	3	3	2	3	**2.7**
4. Оценка на капацитета на канализационните мрежи в населените места	2	1	2	3	2	3	**2.1**
5. Укрепване на капацитета за мониторинг	2	2	3	3	2	3	**2.5**
6. Укрепване на капацитета за прогнозиране	2	2	3	3	2	3	**2.5**
7. Координация и сътрудничество между всички нива на управление (национално, басейново и местно) на единната спасителна система	2	3	3	3	3	3	**2.8**
8. Прилагане на стандартни оперативни процедури (СОП) за координация	2	2	3	3	3	3	**2.6**
9. Пълно прилагане на системи за ранно предупреждение	2	3	3	3	2	3	**2.7**
10. Подобряване на взаимовръзките с други опасности	2	3	3	3	2	2	**2.6**
11. Интеграция на изградени локални системи за ранно предупреждение за наводнения (СРПН) в национална платформа	2	3	3	3	2	3	**2.7**

12. Ревизия и актуализация на системите за ранно предупреждение за наводнения (СРПН)	2	3	3	3	2	2	**2.6**
13. Координация	2	2	3	3	3	3	**2.6**
14. Насърчаване на използването на имуществени застраховки в райони, застрашени от наводнения	2	2	3	3	3	3	**2.6**
15. Контрол на наводненията чрез съобразно с тях земеползване и залесяване за увеличаване на водозадържащия ефект	2	1	3	3	3	3	**2.4**
16. Развитие на зелена инфраструктура, зони за отдих и други услуги, насочени към човека, с цел естествено или изкуствено водозадържане	2	1	1	3	3	1	**1.8**
17. Изграждане, реконструкция и поддръжка на канализационни системи	2	1	1	3	3	2	**1.9**
18. Повишени изисквания към сгради и съществуваща инфраструктура в заливаемите зони	2	1	2	3	3	3	**2.2**
19. Премахване на незаконни сгради, огради, складови площи и други в рамките на речните легла или дерета	2	1	2	3	3	3	**2.2**
20. Изграждане (и поддържане) на корекции и поддръжка на речните легла	2	1	2	2	3	3	**2.0**
21. Мерки за защита от наводнения на крайбрежни зони	2	1	2	2	3	1	**1.8**
22. Поддържане и подобряване на състоянието на съществуващите язовири	2	1	1	3	3	3	**2.0**

Индекс на оценката	**Ниска - 1**	**Средна - 2**	**Висока - 3**

Значимостта на риска е количествен критерий със стойност, изведена от оценката на риска от бедствия, извършена при разработването на профила на риска.

Ефективността показва степента, в която инвестиционен приоритет (мярка) допринася за постигането на една или повече от оперативните цели на

Националната стратегия за намаляване на риска от бедствия (2018–2030 г.), и степента, до която целите могат да бъдат постигнати.

Ефикасността показва икономическата жизнеспособност на инвестиционните приоритети (мерки) т.е. степента, до която разходите и инвестициите допринасят за постигане на очакваните социално-икономически ползи.

Устойчивостта отразява степента, до която инвестиционните приоритети (мерки) са устойчиви и имат принос за устойчивостта към бедствия.

Капацитетът показва настоящата наличност на ресурсите (административни, финансови, човешки), необходими за прилагане на мерките за постигане на целите и за извършване на дейностите на НСНРБ (2018–2030 г.).

Спешността отразява необходимостта да се определи кои мерки трябва да бъдат приложени незабавно и в краткосрочен план предвид рисковете, които бедствията представляват за обществото и икономиката, и потенциалните ползи от инвестирането в управлението на рискове от бедствията.

1. Прилагане на многокритериалния анализ за оценка на риска от наводнения за река Камчия.

През периода 2012 г – 2022 г бяха извършени наблюдения на река Камчия от язовир Тича до устието на река Камчия с Черно море. Участъка е с дължина 134 км. Река Камчия преминава през територията на общините: В. Преслав, Шумен, Смядово, Дългопол и Старо Оряхово. [10]

В р. Голяма Камчия се вливат реките Врана, Поройна и Луда Камчия. Бреговете на реката в участъците преминаващи през общините В. Преслав и Шумен са слабо укрепени с диги и други инженерни съоръжения. Много добре се поддържат бреговете в общините Дългопол и Старо Оряхово там са изградени диги и е направена в някои участъци корекция на коритото и бетонни подпорни стени (Дългопол). На много места са построени мостове за превозни средства и пътници (около 28 бр.). [1],[2],[3],[4],[5]

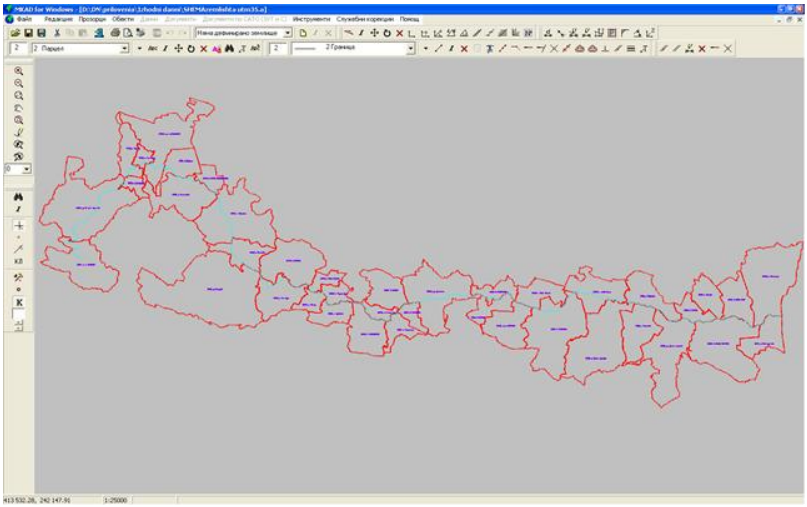
През 2012 г. по цялото поречие бяха извършени геодезически измервания с ГНСС и тотални станции, включващи прокарване на 28 напречни профила за да се установи състоянието на коритото и прилежащите площи. В някои участъци с извърши заснимане с дрон Fantom IV pro 2 за картографиране и 3D моделиране.[6],[7],[8],[9],[11].

Бяха анализирани годишните планове на общините – програми за намаляване на риска от бедствия за периода 2012 – 2025 г. Наблюденията включват всички дейности отнасящи се за изпълнението на критериите за анализ на риска от наводнения.

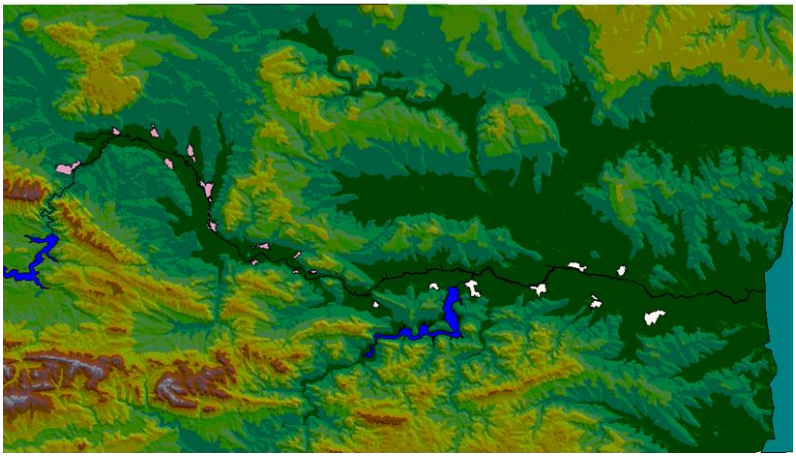
- За повишаване на готовността и подобряване на реагирането на населението във всички програми на общините се отчита, че са взети необходимите мерки за изпълнение на този критерий. Проведени са обучения със екипите на ПБ и ГО и щабовете към общините. Извършена е разяснителна дейност сред населението и са представени нагледни материали.K1=2.5
- Относно критерият за прилагане на системи за ранно предупреждение (СРП), специално насочени към поройните наводнения, или на системи за ранно

предупреждение за множество опасности с разработен модул за наводнения по поречието на р. Голяма Камчия няма изградени автоматизирани устройства, които да регистрират покачване на нивото на водите и предаване на информацията в оперативните центрове на общините. Единствено за целта се очаква да се задейства системата „ALERT". К2=2.0

- Поддържане на стабилна правна, административна и икономическа рамка за прилагане на политиката за защита от наводнения се описва и обяснява в ежегодните програми на общините. В застрашените участъци близо до реката се препоръчва да се предприемат мерки за застраховане, набелязват се мерки за подобряване на инфраструктурата и почистване на речният участък. К3=2.8
- Оценка на капацитета на канализационните мрежи в населените места – в повечето села от разгледаните общини липсва канализационна мрежа. Отичането на повърхностните води става гравитачно и е насочено към реката. Откриване на потенциални проблеми. Разработване на стратегия за бъдещо развитие на канализационната мрежа. К4=2.1
- Укрепване на капацитета за мониторинг – извършва се засилване ролята на платформите за намаляване на риска от бедствия на национално, областно и общинско ниво. Провеждане на обучения за повишаване на капацитета за управление на риска от бедствия на служителите от съответната администрация, служби, други оперативни структури за изпълнение на дейности по защита при бедствия. К5=2.2
- Укрепване на капацитета за прогнозиране - Интегриране на намаляването на риска от бедствия в публичния и частния сектор, с цел повишаване на устойчивостта и осигуряване на непрекъснатост на доставките на основни стоки/услуги. Анализиране на наличните системи за мониторинг и изготвяне на прогнози, с цел усъвършенстване на системата за ранно предупреждение. К6=2.5.
- Координация и сътрудничество между всички нива на управление (национално, басейново и местно) на единната спасителна система – в областите и общините по поречието на р. Камчия се извършва Подобряване на диалога и сътрудничеството между заинтересованите страни за осигуряване на информирано вземане на решения при управление на риска от бедствия, чрез прилагането на научните постижения.К7=2.8



Фиг. 2: Населени места с административните граници по поречието на р. Голяма Камчия



Фиг. 3: Цифров модел (3|D) на р. Камчия от язовир Тича до устието с Черно море

- Прилагане на стандартни оперативни процедури (СОП) за координация - Извършване на прегледи на нормативните актове свързани с управлението на риска от бедствия и инициране на промени, при необходимост. К8=2.2
- Пълно прилагане на системи за ранно предупреждение –общинските администрации са планирали използване на съвременните технологии и иновации за изграждане на ефективна система за ранно предупреждение на населението и органите на изпълнителната власт, но на практика те липсват. К9=2.00
- . Подобряване на взаимовръзките с други опасности – Въвеждане на механизъм и процедури за тестване на технологичната среда, предназначена за взаимодействие при бедствия. К10=2.0
- Интеграция на изградени локални системи за ранно предупреждение за наводнения (СРПН) в национална платформа –К11=2.0
- Ревизия и актуализация на системите за ранно предупреждение за наводнения (СРПН) – К12=2.0
- Координация – изградена е координация между национални, областни и общински структури К13=2.5
- Насърчаване на използването на имуществени застраховки в райони, застрашени от наводнения – в някои общини се извършва стимулиране на застраховането и други механизми за трансфериране на риска сред населението и частния сектор, с цел по-бързо възстановяване след бедствия.К14=2.2
- Контрол на наводненията чрез съобразно с тях земеползване и залесяване за увеличаване на водозадържащия ефект – в някои населени места дигите са разорани (унищожени) с цел увеличаване площта за засаждане с култури (Бял бряг). Не се извършва целенасочено залесяване с цел водозадържане и намаляване на ерозията и свлачища.К15=1.5
- Развитие на зелена инфраструктура, зони за отдих и други услуги, насочени към човека, с цел естествено или изкуствено водозадържане – няма изградени паркове около реката.К16=1.2
- Изграждане, реконструкция и поддръжка на канализационни системи – няма изградена канализационна система в повечето населени места. К17=2,1
- Повишени изисквания към сгради и съществуваща инфраструктура в заливаемите зони – в районите няма застрашени сгради но има шосета и ж.п. линии. К18=2.0.
- Премахване на незаконни сгради, огради, складови площи и други в рамките на речните легла или деретата –няма такива. К19=2.5.
- Изграждане (и поддържане) на корекции и поддръжка на речните легла – К20=2.0.
- Мерки за защита от наводнения на крайбрежни зони – устието на р.Камчия е регулирано и се следи за поддържане на дигите. К21=2.5.
- Поддържане и подобряване на състоянието на съществуващите язовири – язовирите Тича и Цонево се поддържат и се следи за деформации и нивото им. К22=2.8.

Таблица 2. Многокритериалния анализ за риска от наводнения по поречието на река Голяма Камчия

Критерии и тежест	**Значение на риска**	**Ефикасност**	**Ефективност**	**Устойчивост**	**Капацитет**	**Спешност**	**Обща оценка**
Мерки	*25%*	*20%*	*20%*	*15%*	*10%*	*10%*	*100%*
1. Повишаване на готовността и подобряване на реагирането на населението	3	2	2	3	2	3	**2.5** (2.8)
2. Прилагане на системи за ранно предупреждение (СРП), специално насочени към поройните наводнения, или на системи за ранно предупреждение за множество опасности с разработен модул за наводнения.	2	2	2	2	2	2	**2.0 (2.7)**
3. Поддържане на стабилна правна, административна и икономическа рамка за прилагане на политиката за защита от наводнения	2	3	3	3	3	3	**2.8 (2.7)**
4. Оценка на капацитета на канализационните мрежи в населените места	2	1	1	3	3	2	**2.1 (2.1)**
5. Укрепване на капацитета за мониторинг	2	2	3	3	3	3	**2.2 (2.5)**
6. Укрепване на капацитета за прогнозиране	3	2	2	3	2	3	**2.5 (2.5)**
7. Координация и сътрудничество между всички нива на управление (национално, басейново и местно) на единната спасителна система	2	3	3	3	3	3	**2.8 (2.8)**
8. Прилагане на стандартни оперативни процедури (СОП) за координация	2	2	3	3	3	3	**2.2 (2.6)**
9. Пълно прилагане на системи за ранно предупреждение	2	2	2	2	2	2	**2.0 (2.7)**
10. Подобряване на взаимовръзките с други опасности	2	2	2	2	2	2	**2.0 (2.6)**
11. Интеграция на изградени локални системи за ранно предупреждение за наводнения (СРПН) в национална платформа	2	2	2	2	2	2	**2.0 (2.7)**

12. Ревизия и актуализация на системите за ранно предупреждение за наводнения (СРПН)	2	2	2	2	2	2	**2.0 (2.6)**
13. Координация	3	2	2	3	2	3	**2.5 (2.6)**
14. Насърчаване на използването на имуществени застраховки в райони, застрашени от наводнения	2	2	3	3	3	3	**2.2 (2.6)**
15. Контрол на наводненията чрез съобразно с тях земеползване и залесяване за увеличаване на водозадържащия ефект	2	1	2	1	2	1	**1.5 (2.4)**
16. Развитие на зелена инфраструктура, зони за отдих и други услуги, насочени към човека, с цел естествено или изкуствено водозадържане	2	1	1	1	1	1	**1.2 (1.8)**
17. Изграждане, реконструкция и поддръжка на канализационни системи	2	1	1	3	3	2	**2.1 (1.9)**
18. Повишени изисквания към сгради и съществуваща инфраструктура в заливаемите зони	2	1	2	2	3	3	**2.0 (2.2)**
19. Премахване на незаконни сгради, огради, складови площи и други в рамките на речните легла или деретата	2	1	2	3	3	3	**2.5 (2.2)**
20. Изграждане (и поддържане) на корекции и поддръжка на речните легла	2	1	2	2	3	3	**2.0 (2.0)**
21. Мерки за защита от наводнения на крайбрежни зони	3	2	2	3	2	3	**2.5 (1.8)**
22. Поддържане и подобряване на състоянието на съществуващите язовири	2	3	3	3	3	3	**2.8 (2.0)**

Индекс на оценката	**Ниска - 1**	**Средна - 2**	**Висока - 3**

Заключение

Многокритериалният анализ (МКА) е методически подход, използван за приоритизация на различни алтернативи чрез анализ на редица структурирани критерии. Той е комплексен инструмент за оценка и избор на варианти. При избора на варианти се определя числова стойност за отделни критерии, които дават възможност за количествено измерване (на съответните варианти) и позволяват

тяхното сравнение. Критериите са претеглени, като се подчертава относителната им значимост. Претеглената сума на различните избрани критерии се използва за приоритизиране на оценените варианти. Като методика МКА е структурирана рамка, която позволява при използването ѝ да се съчетават експертни оценки, и е подходяща за вземане на решения, когато вариантите не могат да бъдат изчислени количествено.

На тази база в доклада беше направена оценка на риска от наводнения по поречието на р. Голяма Камчия. Получените резултати показват не съществени разлики от МКА за цялата страна.

Литература:

1. Господинов, С., Марков, М., Хаджиева, Б. /2024г./ Применение лазерного сканирования для обследования объектов, имеющие отношение к безопасности дорожного движения, Современные информационные технологии. Сборник научных статей по материалам 10-й Международной научно-технической конференции, стр. 337-346, Москва 2024г., УДК 004.65, ББК 32.973.26-018.2, eLIBRARY ID: 68606783, https://elibrary.ru/item.asp?id=68606783
2. Господинов, С., Постоловски, А., Хаджиева, Б., Марков, М., /2024г./ Определяне и генериране на гравиметрични аномалии в района на гр. Златоград, Proceedings of the XI International Geomechanics Conference 16 – 20 September 2024, Golden Sands Resort, Bulgaria, стр. 104-111, ISSN: 1314-6467
3. Димитров, М., Марков, М., Хаджиева, Б. /2021г./ Създаване на 3D модел на стена на хвостохранилище по резултати от наземно лазерно сканиране, Сборник с доклади от Национална научно-техническа конференция "Управление и безопасност на хвостохранилища", стр. 85-90, ISBN 978-619-90939-7-9
4. Марков, М., Митев, И. /2024г./ Применение лазерного сканирования для картографирования картирования горных образований, Современные информационные технологии. Сборник научных статей по материалам 10-й Международной научно-технической конференции, стр. 453-464, Москва 2024г., УДК 004.65, ББК 32.973.26-018.2, eLIBRARY ID: 68606793, https://elibrary.ru/item.asp?id=68606793
5. Марков, М., /2024г./ Развитие гео роботов, Сборник научных статей по материалам 2-й Международной научно-практической конференции "Интеллектуальные и киберфизические системы: управление, логистика, безопасность", Страницы: 95-106, Номер: 3 (45), Год: 2024, УДК 004, ББК 22.18, eLIBRARY ID: 68620146, https://elibrary.ru/item.asp?id=68620146
6. Марков, М., /2025г./ Анализ дорожных рисков с применением лазерного сканирования, Сборник научных статей по материалам 7-й Международной научно-практической конференции "Методы и модели пространственного анализа", Страницы: 134-142, Номер: 1 (47), Год: 2025,

УДК 004, ББК 22.18, eLIBRARY ID: 79510275, https://elibrary.ru/item.asp?id=79510275

7. Постоловски, А., Димитров, М., Марков, М. /2021г./ Приложение на MTLS – технология при одит на тунелното строителство, XVI международна конференция по открит и подводен добив на полезни изкопаеми, стр. 279-285, Варна 2021г., ISSN 2535-0854
8. Хаджиева, Б., Господинов, С., Марков, М., /2025г./ Необходима ли е геодезическа мрежа с местно предназначение при създаване на кадастрална карта за урбанизирана територия, Списание "Минно дело и геология", Брой 1-2/2025, Година LXXIX, ISSN 0861 – 5713, ISSN 2603 – 4549 (Online)
9. Щерева К., Пеев И., Марков М. /2022г./ Анализ на времево обусловените премествания на дискретни точки от стената на яз. „Златоград“, Осма национална научнотехническа конференция с международно участие, стр. 81-87, Девин 2022г., ISSN 1314-7056
10. Andreev A., Andreeva G. Modeling of the river system of Goliama Kamchia. Journal "Scientific and applied research", vol.2, p.50-58, 2012 ISSN 1314-6289 София – 2016 г.
11. Markov, M., /2026/ Assessment and monitoring of road marking reflectivity using mobile laser scanning to improve road safety, Trakia Journal of Sciences, Vol. 24, No 2, pp 192-196, 2026, ISSN 1313-3551 (online), doi:10.15547/tjs.2026.02.014

SURVEY AND RENOVATION OF THE GEODETIC NETWORK OF THE "V. LEVSKI" NATIONAL MILITARY UNIVERSITY – SHUMEN CAMPUS

Viktor Dragiev, Andrey Andreev

Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levski"
Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levski" andreev_an@abv.bg

Abstract: *The Global Navigation Satellite System (GNSS) is a radio-navigation system used to determine the spatial position of points on and near the Earth's surface with high accuracy in real time. GNSS measurements can be successfully applied to establish local geodetic networks and working geodetic control frameworks.*

This report presents a study aimed at surveying and updating the geodetic network of the "V. Levski" National Military University (Shumen campus) using modern geodetic methods and GNSS technology.

Keywords: *GNSS, GPS, NMU*

ОБСЛЕДВАНЕ И ОБНОВЯВАНЕ НА ГЕОДЕЗИЧЕСКАТА МРЕЖА НА НВУ „В. ЛЕВСКИ" – РАЙОН ШУМЕН

Виктор Драгиев, Андрей Андреев

Въведение

Геодезията е наука, която определя формата и размерите на Земята и външното и гравитационно поле, за изобразяване на земната повърхност или на част от нея във вид на карти и планове, за определяне на точки, линии и повърхнини върху терена по зададени размери чрез трасиране, за измерване и проектиране, свързани с други теоретични и практически задачи.

Тя има важно значение за изграждането на инженерни обекти, кадастъра, картографията и създаване на инфраструктурните проекти[1],[2],[3],[9],[10],[11]. Чрез геодезическите измервания се осигурява необходимата точност при проектиране, строителство и контрол на различни обекти и съоръжения [4],[5], [6].

Глобалната навигационна спътникова система (ГНСС) е радионавигационна система за определяне на пространственото положение на точки от и около земната повърхност с висока точност в реално време. ГНСС измервания може успешно да се прилагат за създаване на геодезически мрежи с местно предназначение и работна геодезическа основа[8],[12],[13],[15].

Докладът представя едно изследване което цели обследване и обновяване на геодезическата мрежа на НВУ „В. Левски" – район Шумен със съвременни геодезически методи и ГНСС.

1. Измервания с ГНСС за създаване на геодезически мрежи

Измерванията с ГНСС са съвременен метод в геодезията. Те позволяват определяне на координати на точки от физическата земна повърхност с висока точност.

Основното им предимство е, че не изискват изграждане на сложни геометрични фигури между точките. Измерванията се базират на спътникови сигнали и позволяват бързо събиране на голям обем данни.

Определянето на координатите от приемника става чрез измерване на псевдоразстояния до спътниците и изчисление на пространствена линейна засечка.

На съвременния етап на развитие ГНСС се използват главно в две направления – навигационно и геодезическо [16],[17],[18],[19].

За геодезически цели се използват специални геодезически приемници. Те могат да бъдат различни като възможности, начин на управление и предназначение.

При геодезическите измервания се извършват относителни определения, при които се определят компонентите на пространствения вектор между две точки, също в единна Декартова и геоцентрична координатна система. Относителните измервания се извършват като се наблюдават едни и същи спътници едновременно от два приемника, разположени на точките, между които се измерва пространствен вектор.

Спътниковите измервания могат да бъдат автоматизирани и управлявани в реално време. Приемниците могат да бъдат едночестотни, приемащи и обработващи сигнал на честота L1 и двучестотни, приемащи и обработващи сигнал на честоти L1 и L2.

Върху измерванията с ГНСС влияние оказват редица фактори. Един от най-съществените е рефракцията (закъснението на сигнала) породена от йоносферата и тропосферата. При прецизни измервания, рефракцията намалява точността на измерванията и следва да се вземе предвид. При едночестотните измервания не могат да бъдат директно определени корекциите заради йоносферната и тропосферна рефракция. Наблюденията от двучестотните станции се явяват като референтни (наблюденията на тях са непрекъснати през цялото време на измерване на мрежата).

Определянето на положението на точките с ГНСС може да се осъществи със следните методи :[14],

1. *Кинематични методи*
   - непрекъснат режим (continuous), постобработка;
   - „спри и върви“ (“Stop and go”), постобработка;
   - реално време (Real Time Kinematics. – RTK).
2. *Относителни методи*
   - статика (statics);
   - ускорена статика (fast, rapid statics);
   - псевдостатика (pseudo statics, reoccupation).

При прилагане на ГНСС, чрез използване на кинематични методи всяка точка от мрежата се определя двукратно съобразно изисквания предвидени в инструкциите:

1. Базови станции могат да бъдат:
   - Базови станции от наличната ГНСС инфраструктура;
   - Виртуални базови станции;
   - Потребителски базови станции, определени съгласно действащата нормативна уредба;
2. Максимално разстояние между определяемите точки и базовите станции, както следва:
   - За кинематични методи с потребителски базови станции - 10 km;
   - При прилагане на виртуални станции - 10 km;
   - При прилагане на ГНСС инфраструктура в реално време - в рамките на обхвата на обслужване на инфраструктурната мрежа – (30 km).
3. Минимална продължителност на измерванията на всяка определяема точка - 30 sec;
4. Интервал на измерванията – 1-2 sec;
5. Тип на решенията - фиксирани;
6. Средни квадратични грешки по положение - 1-2 cm, и във височина - до 5 cm;
7. Когато локалните координатни и височинни системи не са напълно дефинирани, т.е. не са определени по реда на Инструкцията за преобразуване на съществуващите геодезически и картографски материали и данни в "Българска геодезическа система 2005"[ ], се съставят локални трансформационни модели, параметрите, на които се определят въз основа на трансформационни точки;
8. Резултатите от работата се представят с обяснителна записка, към която се прилагат следните данни за определянето на всяка точка:
   - Начало и край на измерването;
   - Географски и проекционни координати в БГС 2005;
   - Средни квадратични грешки по положение и височина. (Инструкция № РД-02-20-25 от 20 септември 2011 г.)[7]

При прилагане на ГНСС, чрез използване на **статични методи** се изисква:

1. изходните точки трябва да бъдат:
   а) точки от Държавната GPS мрежа и/или станции от ГНСС инфраструктура;
   б) минимум три на брой;
2. точките от ИГМ се определят единично или групово, както следва:
   а) всяка единична точка се свързва с три или повече изходни точки;
   б) в случай на групово определяне всяка точка от ИГМ се свързва с две или повече базови станции;
3. векторите, свързващи точките в ИГМ, трябва да са:
   а) с максимална дължина 25 km, т. 1;
   б) независими или частично независими помежду си.

Номиналната продължителност на ГНСС измерванията се определя като се , изхождайки от:

1. вида на базовите станции;
2. средната дължина на векторите - за цялата ИГМ;
3. индивидуалните дължини на векторите - за свързване с отдалечени изходни точки.

При геодезическите измервания с ГНСС се използват различни режими на работа в зависимост от необходимата точност, начина на обработка и условията на измерване. Основните режими са статичен, кинематичен и RTK режим.

Статичният режим се използва при високоточни геодезически измервания и изграждане на геодезически мрежи. При него приемниците остават неподвижни върху определените точки за по-дълъг период от време. Това позволява натрупване на голям обем наблюдения и получаване на висока точност при обработката.

Кинематичният режим се използва при движение на приемника между различни точки. Методът позволява бързо определяне на координати, но изисква непрекъснато проследяване на спътниковите сигнали.

RTK режимът представлява измерване в реално време с използване на корекции от базова станция или мрежа от постоянни ГНСС станции. Този режим осигурява сантиметрова точност и се използва широко в инженерната геодезия и кадастъра.

При избора на режим на измерване се вземат предвид:

- необходимата точност;
- дължината на базовите линии;
- условията на терена;
- времето за работа;
- видът на използваната апаратура.

1. Обработка на измервания с ГНСС

Обработката на измервания с ГНСС е един от най-важните етапи от прилагането на този съвременен метод в геодезията.

Процесът започва с извличане на данните от приемника. След това се извършва проверка на качеството – дали има прекъсвания, шум или липсващи наблюдения.

Следват изчисления на базовите линии между точките. Това е основният етап, при който се определят векторите между приемниците.

При обработката се вземат предвид:

- орбитални данни;
- атмосферни модели;
- часовникови грешки;
- многолъчевост.

Накрая се извършва изравнение на мрежата и се получават окончателни координати.

Обработката извън реално време се осъществява след приключване на измерванията и едва тогава става възможно да се видят крайните резултатите. Извършва се със специализирани програмни продукти (софтуер), които най-общо могат да бъдат два вида: фирмени и институционални.

Фирменият софтуер се доставя от производителите на ГНСС апаратура. Доколкото е възможно, работата с него е опростена и са създадени редица удобства за потребителя – в статичен и кинематичен режим.

Обикновено не се предвиждат опции за въвеждане измервания с апаратура на други производители в оригиналния им вид, но е възможно преобразуването на собствените измервания в общоприетия формат за обмен на данни RINEX, както и въвеждането за последваща обработка на измервания в същия формат.

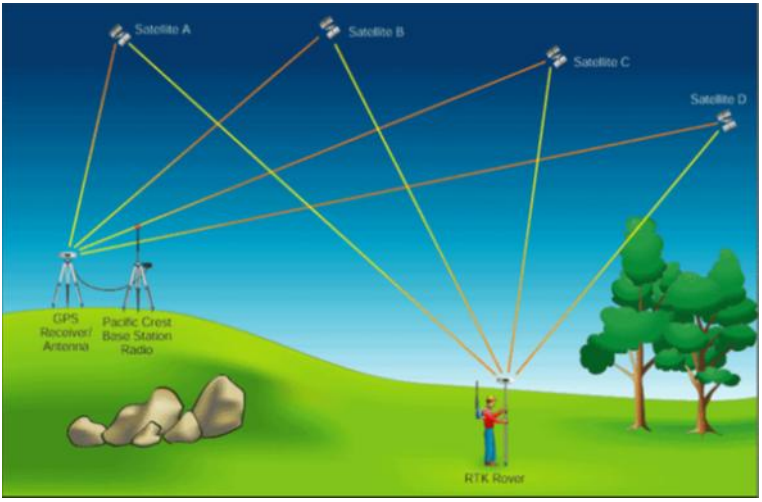
Работата в реално време има следните предимства:

- резултатите от измерванията и тяхната обработка се получават на място, което почти изключва възможността за допускане на некачествени резултати;
- спестява се голяма част от времето за последваща обработка на резултатите.

Приложима е в случаите на статични и кинематични определения, работата в реално време е с особено значение за ефективността на последните.

Например, чрез кинематичните методи в реално време ("Real Time Kinematic" – RTK) се реализират най-продуктивните възможности за приложение на ГНСС.

В режим RTK е възможно масовото координиране на снимачни и други подробни точки, заснемането на линейни и площни обекти, актуализирането на пространствени и атрибутни данни, трасирането на точки, прави линии и криви, и осъществяването на много други рутинни геодезически задачи.



Фиг. 1: Кинематични измервания в реално време

Методите в реално време са силно зависими от начина за предаване на данни от базовата станция. Най-често се използват микровълновият радиодиапазон или канали за данни на клетъчните телефонни мрежи. В класическия вариант – с една базова станция приложението на RTK е възможно в радиус до 10 km около нея, а

ако се създаде виртуална базова станция (VRS) този обхват може да се разшири 3 - 4 пъти.

В последния случай е необходимо да функционира референтна мрежа от минимум 3-4 станции на разстояние 50 - 70 km помежду им, а най-добре – да е създадена такава мрежа с национален обхват (Геовара, Геонет, Йокто1 и др.).

Измерванията с ГНСС може успешно да се прилагат за създаване на геодезически мрежи с местно предназначение и работна геодезическа основа.

Във всяка от тях се проектират поне две базови станции, от които се определят векторите към останалите точки – нови и изходни.

Всяка точка трябва да бъде свързана с минимум две други точки, с което се създават геометрични условия в мрежата. От друга страна, винаги е желателно дължината на векторите да е минимална. Така окончателният брой на референтните станции се определя в зависимост от местните условия, най-важни от които са:

- форма и размер на територията обхванатa от измерванията;
- физикогеографски условия;
- пътна мрежа и проходимост;
- степен на урбанизация;
- състояние на геодезическите мрежи.

Уместно е измерванията да се проектират в две групи:

1. Вектори свързващи базовите станции помежду им и с изходните точки в мрежата;

2. Вектори свързващи определяемите точки с базовите станции.

По този начин се гарантира независимостта на векторите в мрежата при използване на повече от два приемника едновременно и се дава възможност за оптимизиране на организацията на работата на терена.

Векторите в ГММП се определят чрез двучестотни ГНСС (GPS/Глонасс/Бейду/Галилео) измервания, а в РГО са допустими и едночестотни измервания. В последния случай продължителността на сеансите се удвоява.

Измервания във всеки сеанс се извършват при минимална височина на спътниците 15° над хоризонта и максимална стойност на геометричния фактор DOP 7. Интервалът между регистрациите е 5 или 10 sec.

В началото и края на сеанса на всяка точка се измерва височината на антената. Това е разстоянието от надземния център до марка посочена от производителя. Затова еднакво важни са както измерената височина, така и данните за типа на антената и начина по който е центрирана върху точката (на тринога, щок, стълб и пр.).

Резултатите от измерванията, натрупани в паметта на приемниците се прехвърлят на компютър и се архивират в два формата - в оригиналния им вид и във формат RINEX. В последните е необходимо да се уточнят всички данни за точките, ГНСС апаратурата и височините на антените.

Математическата обработка на GPS измерванията обхваща следните етапи:

1. Изчисление на вектори

2. Проверка на геометричните условия в мрежата

3. Изравнение на мрежата по МНМК

Изчислението на вектори се извършва чрез последваща обработка на измерванията, записани по време на работата на терена. Използват се радиоефемериди или прецизни орбити, а тропосферните корекции се определят със стандартни метеорологични данни. Допустими са само фиксирани решения.

За проверка на геометричните условия се сумират координатните разлики по осите X, Y и Z по затворените геометрични фигури в мрежата, образувани от независимо определените вектори. Предпочитат се триъгълникови условия, но е допустимо сключването и на други фигури.

Изравнението на ГММП се извършва като включена мрежа, в която изходни са точките от ДGPS-мрежа, а това на РГО – и точките от ГММП, определени с ГНСС.

Съвременната обработка на геодезически данни се извършва чрез специализиран софтуер. Той автоматизира голяма част от изчисленията.Софтуерът значително намалява времето за обработка и минимизира човешките грешки.

2. Експериментални изследвания

Обект на изследването са избрани геодезически точки в даден район, които са подходящи за ГНСС наблюдения. Точките са разположени така, че да осигуряват добра видимост към ГНСС и минимални препятствия за приемане на спътниковите сигнали.

Разработена е методика за измерване на точки от РГО, чрез използване на ГНСС технологията в режим RTK и статичен режим.

Изследването има за цел да установи ефективността на разработената методика за приложение на ГНСС в режим RTK и статичен режим при създаване на РГО, на базата на реални геодезични измервания, проведени по класически и ГНСС методи.

Изследването се заключава в анализ на геодезичните дейности и оценка на получените резултати.

Обект – „НВУ „В. Левски“ – район Шумен.

Измерванията са извършени с два броя двучестотни ГНСС приемника Hi Target iRTK5.

За изследването се разполага с представителна извадка от данни от проведени в съответния район класически и ГНСС измервания. На базата на тези данни – планови и височинни, са извършени съответните сравнения между координатите и височините на точките.

НВУ „В. Левски“ – район Шумен се намира в централната част на гр. Шумен. Площта на района по кадастралния план е 134000 кв. м.. Улиците са благоустроени. Застрояването е многоетажно с административни, учебни и битови сгради. Районът е разположено северно от Шуменското плато. Релефът е слабо пресечен. Надморската височина в района на урбанизираната територия е около 250 m. Като изходни точки са използвани съществуващите точки от ГММП и точки от РГО (42 бр.). Разположението на РГО осигурява пълно покритие на района. Координатната система на изходните точки е в БГС2005. Височинната система е Балтийска височинна система.

Методи на измерване, обработка и оценка на точността при класически измервания с тотална станция са предоставени от архива на катедра „Геодезия".



Фиг. 2: Схема на геодезическата мрежа на НВУ"В. Левски" – район Шумен

Геодезичните дейности, свързани при създаване на РГО с ГНСС в режим RTK са на база разработената методика.

Извършени са наблюдения в режим RTK с интервал на запис 2 sec., с потребителска базова станция (тт.6) и с перманентната ГНСС мрежа на ГЕОВАРА. В режим RTK с потребителска базова станция са извършени наблюдения на точките от РГО, като са направени измервания на всяка една точка, но с различна продължителност – 30 sec. Изследва се влиянието на продължителността на измерването върху точността на определяне на точките, тъй като съгласно „Инструкция РД-02-20-25 от 20 септември 2011 г [7]. за определяне на геодезични точки с помощта на глобални навигационни спътникови системи", чл. 31, т. 3 минималната продължителност за измерване при определяне на точка с цел трайно стабилизиране за многократна експлоатация е 30 секунди.

При измервания в режим статичен и използване на перманентна базова станция от изградената инфраструктурна мрежа на ГЕОВАРА е необходимо допълнителна обработка на височинните измервания, чрез въвеждане на локален модел на геоида (БГС Транс). В тази връзка се препоръчва да се използват измервания в режим статичен и използване на потребителска базова станция, поради това, че

височините се получават директно в зададената координатна система на базовата станция.

Направен е анализ и сравнение на получените координати и височини на точките от различните методи на измерване (класически и ГНСС). В таблица 2 са представени получените резултати от изследването в района с оценка на точността.

Таблица №1

№т	Координати ОГМ от 2002			Координати ОГМ от ГНСС RTK			Координати ОГМ от ГНСС Static		
	N	E	Hr.	N	E	Hr.	N	E	Hr.
5	4793529,253	616378,146	263,635	4793529,279	616378,249	263,156	4793529,282	616378,243	263,0813
6	4793551,721	616399,15	262,269	4793551,74	616399,224	261,882	4793551,746	616399,237	261,806
7	4793525,729	616324,855	264,487	4793525,716	616324,984	264,092	4793525,761	616324,986	264,009
19	4793602,328	616109,525	267,872	4793602,995	616109,363	267,534	4793602,981	616109,368	267,472
23	4793473,565	616123,71	272,629	4793473,567	616123,879	272,259	4793473,575	616123,883	272,176
36	4793663,495	616325,671	259,713	4793663,501	616325,76	259,327	4793663,519	616325,749	259,25
38	4793699,596	616322,782	257,468	4793699,573	616322,885	257,097	4793699,594	616322,866	257,001
81	4793589,105	616020,797	271,175	4793589,112	616020,978	270,761	4793589,108	616020,991	270,733
2001	4793737,319	616346,219	255,915	4793737,337	616346,309	255,544	4793737,351	616346,305	255,486
2003	4793710,369	616373,254	255,452	4793710,397	616373,334	255,082	4793710,381	616373,351	255,013

Таблица №2

Обект: НВУ		Сравнения	
		РГО класически метод (2002 г) - РГО ГНСС static	РГО RTK - РГО ГНСС static
Район	Бр. измервания.	ср.кв.гр.m (cm)	ср.кв.гр.m (cm)
Шумен	10	mx = 0.208	mx = 0.019
		my = 0.125	my = 0.011
		mh = 0.460	mh = 0.072

Заключение

Широкото приложение на ГНСС е безспорен факт и необходимостта от тях все повече нараства. За геодезични цели интерес представляват многоканалните приемници, които имат възможност да приемат едновременно сигнали от много спътници на две честоти. С модернизацията и въвеждането на допълнителни сигнали от ГНСС се подобрява точността и достъпността до потребителите. С въвеждането и развитието на перманентните геодезични мрежи, измерванията в

режим RTK стават много по-бързо и се изпълняват изискванията на Инструкциите за създаване на РГО.

Разработената методика за измерване на точки от РГО, чрез използване на технологията на ГНСС в статичен и RTK режим дава много добри резултати и може да се приложи и за други обекти, където е необходимо обновяване на геодезическата мрежа.

Литература:

1. Господинов, С., Марков, М., Хаджиева, Б. /2024г./ Применение лазерного сканирования для обследования объектов, имеющие отношение к безопасности дорожного движения, Современные информационные технологии. Сборник научных статей по материалам 10-й Международной научно-технической конференции, стр. 337-346, Москва 2024г., УДК 004.65, ББК 32.973.26-018.2, eLIBRARY ID: 68606783, https://elibrary.ru/item.asp?id=68606783
2. Господинов, С., Постоловски, А., Хаджиева, Б., Марков, М., /2024г./ Определяне и генериране на гравиметрични аномалии в района на гр. Златоград, Proceedings of the XI International Geomechanics Conference 16 – 20 September 2024, Golden Sands Resort, Bulgaria, стр. 104-111, ISSN: 1314-6467
3. Димитров, М., Марков, М., Хаджиева, Б. /2021г./ Създаване на 3D модел на стена на хвостохранилище по резултати от наземно лазерно сканиране, Сборник с доклади от Национална научно-техническа конференция "Управление и безопасност на хвостохранилища", стр. 85-90, ISBN 978-619-90939-7-9
4. Димова Г. Общи принципи, прилагани при управлението на риска от природни бедствия. Proceedings of International Scientific Conference "Defense Technologies" DefTech 2025,Faculty of Artillery, Air Defense and Communication and Information Systems.Стр.1083-1092, ISSN2815-4282 – онлайн издание.
5. Димова Г. Управление на риска при наводнения. International Scientific Conference "Defense Technologies" DefTech 2025,Faculty of Artillery, Air Defense and Communication and Information Systems. Стр.1076-1084, ISSN2815-4282 –онлайн издание
6. Димова Г. Управление на риска при свлачища, срутища и земни пропадания. . International Scientific Conference "Defense Technologies" DefTech 2025,Faculty of Artillery, Air Defense and Communication and Information Systems. Стр.1066-1076, ISSN2815-4282 –онлайн издание
7. Инструкция № РД-02-20-25 от 20 септември 2011 г. за определяне на геодезически точки с помощта на глобални навигационни спътникови системи. Министерството на регионалното развитие и благоустройството, Обн. ДВ. бр.79 от 11 Октомври 2011 г.
8. Йовев И. GPS технологиите и създаване на условия за тяхното ефективно приложение в България, сп."География`21", бр.5, 2007.

9. Марков, М., Митев, И. /2024г./ Применение лазерного сканирования для картографирования картирования горных образований, Современные информационные технологии. Сборник научных статей по материалам 10-й Международной научно-технической конференции, стр. 453-464, Москва 2024г., УДК 004.65, ББК 32.973.26-018.2, eLIBRARY ID: 68606793, https://elibrary.ru/item.asp?id=68606793
10. Марков, М., /2024г./ Развитие гео роботов, Сборник научных статей по материалам 2-й Международной научно-практической конференции "Интеллектуальные и киберфизические системы: управление, логистика, безопасность", Страницы: 95-106, Номер: 3 (45), Год: 2024, УДК 004, ББК 22.18, eLIBRARY ID: 68620146, https://elibrary.ru/item.asp?id=68620146
11. Марков, М., /2025г./ Анализ дорожных рисков с применением лазерного сканирования, Сборник научных статей по материалам 7-й Международной научно-практической конференции "Методы и модели пространственного анализа", Страницы: 134-142, Номер: 1 (47), Год: 2025, УДК 004, ББК 22.18, eLIBRARY ID: 79510275, https://elibrary.ru/item.asp?id=79510275
12. Постоловски, А., Димитров, М., Марков, М. /2021г./ Приложение на MTLS – технология при одит на тунелното строителство, XVI международна конференция по открит и подводен добив на полезни изкопаеми, стр. 279-285, Варна 2021г., ISSN 2535-0854
13. Хаджиева, Б., Господинов, С., Марков, М., /2025г./ Необходима ли е геодезическа мрежа с местно предназначение при създаване на кадастрална карта за урбанизирана територия, Списание "Минно дело и геология", Брой 1-2/2025, Година LXXIX, ISSN 0861 – 5713, ISSN 2603 – 4549 (Online)
14. Хофман-Веленхоф Б., Лихтенегер Х., Колинс Дж. Глобална система за определяне на местоположение: Теория и практика. Превод от английски, София, УАСГ, 2002
15. Щерева К., Пеев И., Марков М. /2022г./ Анализ на времево обусловените премествания на дискретни точки от стената на яз. „Златоград“, Осма национална научнотехническа конференция с международно участие, стр. 81-87, Девин 2022г., ISSN 1314-7056
16. Andreev A., Andreeva G. Modeling of the river system of Goliama Kamchia. Journal "Scientific and applied research", vol.2, p.50-58, 2012 ISSN 1314-6289 София – 2016 г.
17. Keller W. Observation Techniques in Satellite Geodesy , 2003.
18. Leick A, GPS satellite surveying. Third edition, Wiley, 2004.
19. Markov, M., /2026/ Assessment and monitoring of road marking reflectivity using mobile laser scanning to improve road safety, Trakia Journal of Sciences, Vol. 24, No 2, pp 192-196, 2026, ISSN 1313-3551 (online), doi:10.15547/tjs.2026.02.014

LINEAR MEASUREMENT WITH LIGHT RANGEMETERS ON A REFERENCE GEODESIC NETWORK

Maria Cendova, Andrey Andreev

Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levski"
Department Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levski" andreev_an@abv.bg

Abstract: *Geodesy is a science that determines the shape and dimensions of the Earth and the external and gravitational field, for depicting the Earth's surface or part of it in the form of maps and plans, for determining points, lines and surfaces on the terrain according to given dimensions by tracing, for measuring and designing, related to other theoretical and practical tasks.*

It is of great importance for the construction of engineering objects, cadastre, cartography and the creation of infrastructure projects. Geodetic measurements ensure the necessary accuracy in the design, construction and control of various objects and facilities.

The Global Navigation Satellite System (GNSS) is a radio navigation system for determining the spatial position of points on and around the Earth's surface with high accuracy in real time. GNSS measurements can be successfully applied to create geodetic networks with local purpose and a working geodetic basis.

The report presents a study that aims to survey and renew the geodetic network of the National University "V. Levski" - Shumen region with modern geodetic methods and GNSS.

Keywords: *GNSS, GPS, NMU*

ЛИНЕЙНИ ИЗМЕРВАНИЯ СЪС СВЕТЛОДАЛЕКОМЕРИ НА ЕТАЛОННА ГЕОДЕЗИЧЕСКА МРЕЖА

Мария Цендова, Андрей Андреев

Въведение

Геодезията е наука, която определя формата и размерите на Земята и външното и гравитационно поле, за изобразяване на земната повърхност или на част от нея във вид на карти и планове, за определяне на точки, линии и повърхнини върху терена по зададени размери чрез трасиране, за измерване и проектиране, свързани с други теоретични и практически задачи [13],[15],[16].

Тя има важно значение за изграждането на инженерни обекти, кадастъра, картографията, създаване на инфраструктурните проекти, контрол при техногенни катастрофи [4],[5],[6] . Чрез геодезическите измервания се осигурява необходимата точност при проектиране, строителство и контрол на различни обекти и съоръжения [.

Глобалната навигационна спътникова система (ГНСС) е радионавигационна система за определяне на пространственото положение на точки от и около земната повърхност с висока точност в реално време. ГНСС измервания може

успешно да се прилагат за създаване на геодезически мрежи с местно предназначение и работна геодезическа основа.

Докладът представя едно изследване което цели обследване и обновяване на геодезическата мрежа на НВУ „В. Левски" – район Шумен със съвременни геодезически методи и ГНСС.

1. Компариране на светлодалекомери

Светлодалекомерите представляват електрооптични геодезически инструменти за измерване на разстояния чрез електромагнитни вълни [1],[2]. В зависимост от точността на измерване и дължините, за които са предназначени, те се разделят на три основни групи: геодезически, топографски и прецизни далекомери. Тази класификация е възприета в редица учебници по геодезия и служи за по-ясно разграничаване на областите на приложение на отделните типове инструменти [3],[9],[10],[11].

Измерването на разстояния със светлодалекомери се основава на определяне на времето за разпространение на електромагнитния сигнал или на измерване на фазовата разлика между излъчения и приетия сигнал. Разстоянието се определя чрез зависимостта

(1) $$D=(c.t)/2$$

където D е измереното разстояние, с е скоростта на разпространение на електромагнитната вълна, а t е времето за двупосочното преминаване на сигнала. При фазовия метод разстоянието се изразява чрез

(2) $$D=(n.\lambda)/2+(\lambda.\varphi)/4\pi$$

където n е броят на целите дължини на вълната, λ е дължината на модулиращата вълна, а φ е измерената фазова разлика. Точността на измерването зависи от стабилността на честотния генератор, точността на фазовото измерване, характеристиките на отражателя и атмосферните условия. Поради влиянието на атмосферата скоростта на разпространение на електромагнитната вълна се определя от показателя на пречупване на въздуха, като

(3) $$c=c_0/n$$

където с0 е скоростта на светлината във вакуум, а n е показателят на пречупване на въздуха.

Съвременните геодезически далекомери са фазови и обикновено са съчетани с електронен теодолит. Тази комбинация се нарича електронен тахиметър (тотална станция) [12].

Фазовите светлодалекомери използват зависимостта между ъгловата скорост ω, фазовия ъгъл φ и времето τ:

(4) $$\varphi = \omega \tau.$$

Тогава търсеното разстояние S се определя по формулата:

(5) $$S = (v.\varphi) / (2\ \omega),$$

където v е скоростта на разпространение на електромагнитната вълна.

Най-често ъгловата скорост се изразява чрез модулиращата честота на информационния сигнал f ($\omega = 2\pi f$), откъдето:

(6) $$S = (v.\varphi) / (4\pi.f).$$

От друга страна съществува зависимост между модулиращата честота f, скоростта на вълната v и дължината на електромагнитните вълни λ ($v = f \lambda$), така че търсената дължина се получава и по формулата:

(7) $$S = (\varphi / (2\pi)) (\lambda / 2).$$

В зависимост от дължината на измереното разстояние, фазовият ъгъл може да надхвърля многократно стойността 2π, а вграденият в далекомера фазомер измерва ъглите само в този интервал. В най-общия случай фазовият ъгъл се представя като:

(8) $$\varphi = 2\pi. N + \varphi_0,$$

където N е цяло число (брой пълни периоди), а φ_0 е фазовата разлика, измерена директно от фазомера. Тогава формула (1.5) добива вида:

(9) $$S = (N + \Delta N) (\lambda / 2),$$

като $\Delta N = \varphi_0 / (2\pi)$ представлява дробната част от фазовия цикъл, определена пряко от измерването. За да се определи еднозначно броят N на пълните обороти на фазовия ъгъл, е необходимо измерванията да се извършват при различни модулиращи честоти [19].

2. Редукции към измереното разстояние

Преходът от измерената "пространствена крива" (D') към геодезически хоризонтално разстояние върху референтния елипсоид (D_0) е процес, включващ последователно прилагане на няколко типа редукции. Тези редукции се разделят условно на три групи: метеорологични, геометрични и проекционни.

Група I: Метеорологични редукции.

Това са първите и най-важните поправки, чиято цел е да преведат "пространствената крива" към геометрично наклонено разстояние (S) между центровете на пунктовете. Редукцията ΔDmet се изчислява въз основа на измерените по време на серията метеорологични елементи (t, P, e), използвайки емпирични формули за определяне на груповия коефициент на пречупване за светлина. Изразът има вида:

(10) $$\Delta Dmet = k * D',$$

където k е малък коефициент, но поради големината на измерваните разстояния абсолютната стойност на поправката може да бъде значителна (сантиметри до дециметри). Стойностите на метеопараметрите се осредняват по специална

методология от отчети в началната и крайната точка, направени преди и след всяка измервателна серия.

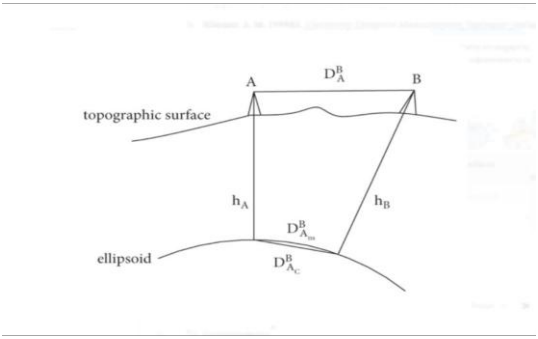
Група II: Геометрични редукции.

След като е получено наклоненото геометрично разстояние D', то се привежда към хоризонталното разстояние D_0 на нивото на измервателните инструменти чрез стандартна редукция за наклон, използваща измереното или тригонометрично определено превишение между пунктовете. След това, ако измерването е извършено ексцентрично (далекомерът или отражателят не са поставени точно над центровете на геодезическите пунктове), се прилага ексцентрична редукция. Тя, на базата на измерените ексцентрицитети (разстояния и посочни ъгли от центъра на пункта до инструмента), превежда разстоянието между инструментите в разстояние между центровете на пунктовете.

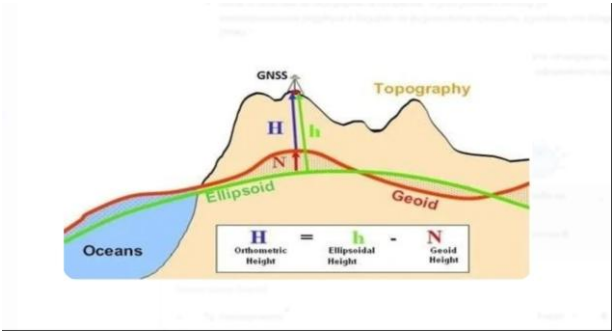
Група III: Редукции към референтната повърхност и проекционната равнина.

Това е финалният етап от математическата обработка.

1. Редукция към референтния елипсоид.



Фиг. 1: Редукция към референтния елипсоид



Фиг. 2: Системата височини в геодезията

Хоризонталното разстояние на земната повърхност (D_0) се проектира върху повърхността на приетия референтен елипсоид (например елипсоидът WGS84). Тази редукция (ΔDel) отчита разликата между височината на измервателната линия над елипсоида и кривината на земната повърхност. Поправката е пропорционална на средната височина на линията над елипсоида (Hm) и обратно пропорционална на радиуса на Земята (R):

(11) $$\Delta Del \approx - (Hm / R) * D_0.$$

Отрицателният знак показва, че разстоянието на елипсоида е по-късо от това на земната повърхност.

2. Редукция към проекционната равнина.

Разстоянието върху елипсоида (Del) не е праволинейно в използваната картографска проекция (напр. UTM). За да се получи разстоянието в равнината на координатната система (Dpr), се прилага проекционна редукция (ΔDpr). Тази поправка отчита изкривяването, въведено от проектирането на крива повърхност върху равнина и зависи от положението на линията спрямо осовия меридиан на зоната и нейната дължина. Крайният редуциран резултат е този, който се използва при изравняването на геодезическите мрежи и всички последващи изчисления.

(12) $$Dpr = Del + \Delta Dpr$$

Методика на измерване и обработка

Полевата работа

1. Центриране: Инструментът и отражателят се центрират върху геодезическите пунктове. Точността на центриране е 1-5 mm. При невъзможност се допуска ексцентрично поставяне с точно измерване на елементите на ексцентрицитетите.

2. Измервателни серии: Извършват се предписания брой серии (12 за ДГМ) през денонощието.

3. Метеорологични измервания: Преди и след всяка серия в двата пункта се отчитат t, P, e с прецизни уреди (аспирационен психрометър, барометър).

4. Запис на данни: Всички данни се записват в специален карнет за линейни измервания, включващ записи за сериите, метеоданните, ексцентричните елементи и резултатите от контролните проверки.

5. Обработка на място: Извършва се предварителна обработка за оценка на качеството - изчисляване на метеорологичните редукции, проверка на допустимите разлики между сериите, изчисляване на средното разстояние и оценка на неговата средноквадратична грешка по формулите: •

- Средна стойност:

(13) $$S = (\Sigma Si) / n \bullet$$

- Грешка на единично измерване:

(14) $$m_S=\sqrt{(\sum(Si-S)〗^2/(n-1))}$$

- Грешка на средната стойност:

(15) $$M_S=m_S/\sqrt{n}$$

2.2.2. Определяне на поправките към измереното разстояние

1. Редукция за наклон (привеждане към хоризонтално разстояние)

(16) $$S_0=\sqrt{((S'^2-h^2)}$$

Където S0 е хоризонтално разстояние; S' е наклонено разстояние; h е превишение между точките.

2. Редукция към референтния елипсоид.

По формула (11).

3. Редукция към проекционната равнина

По формула (12)

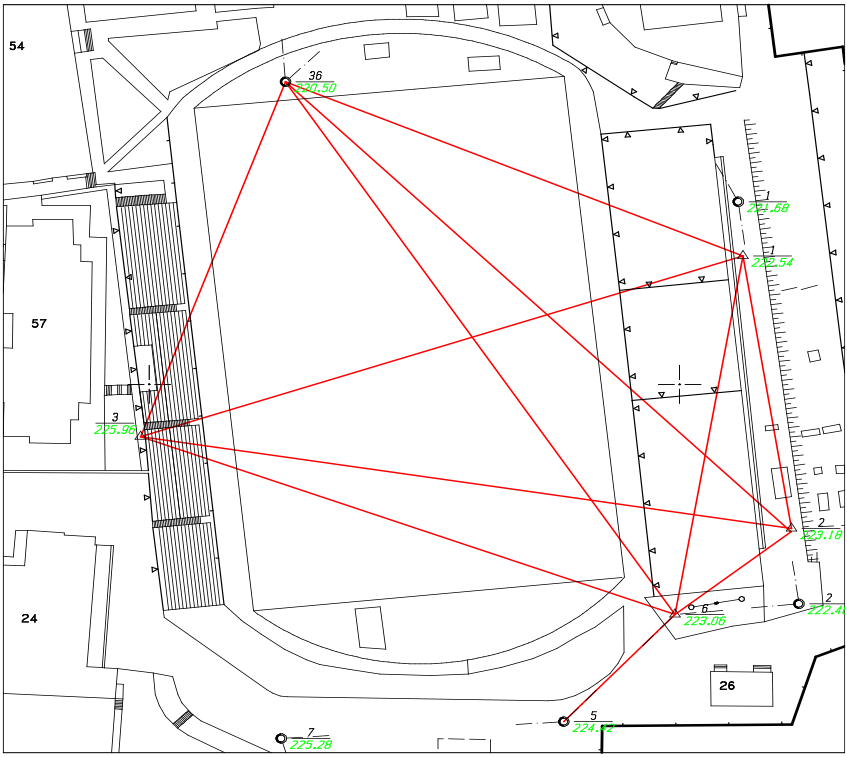
3. Експериментални изследвания

Създадената еталонна геодезическа мрежа в района на факултет „А, ПВО и КИС" осигурява условия за провеждане на учебни занятия и научни изследвания, като се използва информацията получена за точките от мрежата (3 бр. бетонни стълбове с устройства за принудително центриране) на базата на прилагане на съвременни геодезически методи и инструменти.

За изследването са използвани три точки от ЕГМ (т.1, т.2 и т.3) стабилизирани е бетонни стълбове и устройства за принудително центриране. Освен тях са използвани точки от РГО на НВУ – тт 6, рт. 5 и рт.36.

Измерванията по гирусния метод (в 3 гируса) се извършват последователно на точките от ЕГМ и на тт 6. Данните от измерванията са записани на електронен карнет.

Преди и след завършване на измерванията са измерени елементите на атмосферата – t, P и e. Данните са въведени в тоталната станция като корекции заради метеорологичните условия. Измерванията са проведени при благоприятни условия.



Фиг. 3: Схема на мрежата

1. Входни данни и условия:
   - Обект на измерване: ЕГМ на НВУ - Шумен •
   - Клас на мрежата: VII клас. •
   - Инструмент: Тотална станция HTS-420 R № , сертифициран
   - Метео условия: Неблагоприятен период е избягван;
2. Измерени и определени величини (фрагмент от обработката):
   2.1. Ексцентрични елементи - няма ексцентрични измервания
   2.2. Метеорологични данни

Таблица 1 Метеорологични измервания

Пункт/серия	**Температура t ^{0}C**	**Налягане P mmHg**
етт 1		
преди	**14.9**	**749.5**
след	**15.0**	**749.3**
етт 2		
преди	**15.2**	**749.1**
след	**15.1**	**749.0**
етт 3		
преди	**15.2**	**745.0**
след	**15.2**	**749.9**
тт 6		
преди	**15.1**	**749.0**
след	**15.1**	**749.8**
Ср. стойности	**18.175**	**748.65**

Таблица 2. Измерени наклонени разстояния от далекомера**:**

Разстояние между	**Наклонено разстояние D'$_{изм}$ (m)**
етт 1 – етт 2	**57.932**
етт 1 – етт 3	**119.808**
етт 1 – тт 6	**76.253**
етт 2 – етт 1	**57.931**
етт 2 – етт 3	**124.338**
етт 2 – тт 6	**28.333**
тт 6 – етт 1	**76.241**
тт 6 – етт 2	**28.329**
тт 6 – етт 3	**107.604**

2.3. Определяне на точността:

- Средноквадратна грешка на единично измерване (серия):

$m_S=\sqrt{([v^2]/(n-1))}=\pm 1mm$.

-Средноквадратна грешка на средноаритметичната стойност:

$M_S=m_S/\sqrt{n}= \pm 0.5mm$.

- Относителна грешка на измерената страна:

M_S/S 1:600000

2.4. Прилагане на геометрични и проекционни редукции:

***- Редукция за наклон (привеждане към хоризонтално разстояние)*:**

$$S_0 = \sqrt{(S'^2 - h^2)}$$

- Редукция към елипсоида WGS84:

- Средна височина на линията: $H_{_m}$ = m;

- Радиус на Земята: R ≈ 6371 km.

$$\Delta S_{el} = \frac{H_m}{R}.S_0$$

$$Sel = S_0 + \Delta S_{el}$$

- *Проекционна редукция (за UTM, зона 35):*

Средна координата $X_{_m}$ и отстояние от осовия меридиан $y_{_m}$ са изчислени. Поправката се изчислява по формулата:

Приема се y_m = km.

$$\Delta S_{pr} = \frac{y_m^2}{2R^2}.S_{el}$$

• *Крайно редуцирано разстояние в проекционната равнина:*

Spr = Sel + ΔSpr

Таблица №3. Определяне на редукциите

№	Sn	dH	S_0	Hm	dSel	Sel	Ym	dSpr	Spr
1,2	57,932	0,59	57,929	262,337	0,002385	57,927	616416,518	0,271132	58,198
1,3	119,808	3,402	119,760	263,743	0,004958	119,755	616355,118	0,560415	120,315
1,6	76,253	-0,172	76,253	261,956	0,003135	76,250	616405,579	0,356883	76,607
2,1	57,931	-0,59	57,928	262,337	0,002385	57,926	616416,518	0,271128	58,197
2,3	124,338	2,812	124,306	264,038	0,005152	124,301	616359,718	0,581699	124,883
2,6	28,333	-0,762	28,323	262,251	0,001166	28,322	308210,559	0,033141	28,355
3,1	119,807	-3,402	119,759	263,743	0,004958	119,754	616355,118	0,56041	120,314
3,2	124,337	-2,812	124,305	264,038	0,005152	124,300	616359,718	0,581694	124,882
3,6	107,602	-3,574	107,543	263,657	0,004451	107,538	616348,780	0,503235	108,041
6,1	76,241	0,172	76,241	261,956	0,003135	76,238	616405,579	0,356827	76,594
6,2	28,329	0,762	28,319	262,251	0,001166	28,318	616410,180	0,132541	28,450
6,3	107,604	3,574	107,545	263,657	0,004451	107,540	616348,780	0,503244	108,043

1	262,042	4793626,928	616411,917	262,0418
2	262,632	4793569,742	616421,118	262,6318
3	265,444	4793589,023	616298,318	265,4442
6	261,87	4793551,756	616399,241	261,8701

3.3. Експериментални измервания с ГНСС на ЕГМ [7],[8],[14],[17],[18].

За изследването са използвани три точки от ЕГМ (т.1, т.2 и т.3) стабилизирани е бетонни стълбове и устройства за принудително центриране. Освен тях са използвани точки от РГО на НВУ – тт 6 база.

3.4 Сравнение на резултатите от измервания с ТС и ГНСС

Табл. 4. Координати на точките получени от ТС и ГНСС

№ т.	**Координати с Тотална станция**			**Координати с ГНСС**		
	N (X)	**E (Y)**	**Нел.**	**N (X)**	**E (Y)**	**Нел.**
пт1	4793626.9280	616411.9170	262.0418	4793626.9118	616411.9175	262.0434
пт2	4793569.7420	616421.1180	262.6318	4793569.7448	616421.0954	262.6671
пт3	4793589.0230	616298.3180	265.4442	4793589.0110	616298.3358	265.4401
пт6	4793551.7560	616399.2410	261.8701	4793551.7423	616399.2373	261.8745
Ср.	4793584.3623	616382.6485	262.9970	4793584.3525	616382.6465	263.0063

Табл. 5. Разлики в координатите

Разлики		
ΔN	**ΔE**	**ΔH**
+0.0162	-0.0005	-0.0016
-0.0028	+0.0226	-0.0353
+0.0120	-0.0178	+0.0041
+0.0137	+0.0037	-0.0044
0.0098	0.0020	-0.0093

[d*.d*]	+0.0006	+0.0008	+0.0013
[d*.d*]/n	0.000150493	0.000210385	0.000321205
m=√[d*.d*]/n	0.012	0.015	0.018

Средните стойности на разликите в координатите и височините на точките са както следва:

за ΔN - 9.8 mm; за ΔE – 2.0 mm; за ΔH – 9.3 mm.

Със следните средни квадратни грешки:

За m ΔN=±1.2 cm; за mΔE =± 1.5 cm; за mΔH =± 1.8 cm.

Табл. 3. 7 Разлики в разстоянията и оценка на точността

Разстояния между точките	**ТС**	**ГНСС "статик"**	**Разлики [m] dS= Sts-Sgnss**	dS.dS		**mS[m]**
tt1 - tt6	76.234	76.2393	-0.0053	0.000028		
tt2 - tt6	28.321	28.328	-0.0070	0.000049		
tt3 - tt6	107.584	107.6093	-0.0253	0.000640		
tt1 -tt2	57.922	57.8990	0.0230	0.000527		
tt1 - tt3	119.756	119.7384	0.0176	0.000311		
tt2 - tt3	124.304	124.2622	0.0418	0.001743		
				0.003299	0.00055	0.0234

№ т.	Координати с Тотална станция			Координати с ГНСС		
	N (X)	E (Y)	Нел.	N (X)	E (Y)	Нел.
пт1	4793626.928	616411.917	262.0418	4793626.912	616411.9	262.0434
пт2	4793569.742	616421.118	262.6318	4793569.745	616421.1	262.6671
пт3	4793589.023	616298.318	265.4442	4793589.011	616298.3	265.4401

Средната квадратна грешка върху всичките разстояния е m_S=±23.4mm

Заключение

1. Проведените теренни измервания на еталонната геодезическа мрежа с тотална станция „HTS-420R" бяха изпълнени успешно, прилагайки всички стъпки от разработената методика. Измерванията са извършени в три гируса със спазване на реда и условията за точност.
2. Обработката на резултатите с TPLAN показа минимални отклонения от допустимите стойности и добра геометрична обусловеност на мрежата.
3. Проведеното паралелно наблюдение с ГНСС приемници (Hi-Target RTK-5) даде възможност за сравнителен анализ между резултатите от двата метода, който показа, че разликите са в рамките на допустимите стойности. Това потвърди надеждността на измерванията с тоталната станция.

4. Практическото изпълнение доказа не само приложимостта на методиката в реални условия, но и важността от добра организация, подходящи методи и методика, контрол и анализ. Постигнатата точност е напълно съвместима с изискванията за локални еталонни мрежи и показва потенциал за приложение в учебни, метрологични и инженерни задачи.

Литература:

1. Господинов, С., Марков, М., Хаджиева, Б. /2024г./ Применение лазерного сканирования для обследования объектов, имеющие отношение к безопасности дорожного движения, Современные информационные технологии. Сборник научных статей по материалам 10-й Международной научно-технической конференции, стр. 337-346, Москва 2024г., УДК 004.65, ББК 32.973.26-018.2, eLIBRARY ID: 68606783, https://elibrary.ru/item.asp?id=68606783
2. Господинов, С., Постоловски, А., Хаджиева, Б., Марков, М., /2024г./ Определяне и генериране на гравиметрични аномалии в района на гр. Златоград, Proceedings of the XI International Geomechanics Conference 16 – 20 September 2024, Golden Sands Resort, Bulgaria, стр. 104-111, ISSN: 1314-6467
3. Димитров, М., Марков, М., Хаджиева, Б. /2021г./ Създаване на 3D модел на стена на хвостохранилище по резултати от наземно лазерно сканиране, Сборник с доклади от Национална научно-техническа конференция "Управление и безопасност на хвостохранилища", стр. 85-90, ISBN 978-619-90939-7-9
4. Димова Г. Общи принципи, прилагани при управлението на риска от природни бедствия. Proceedings of International Scientific Conference "Defense Technologies" DefTech 2025,Faculty of Artillery, Air Defense and Communication and Information Systems.Стр.1083-1092, ISSN2815-4282 – онлайн издание.
5. Димова Г. Управление на риска при наводнения. International Scientific Conference "Defense Technologies" DefTech 2025,Faculty of Artillery, Air Defense and Communication and Information Systems. Стр.1076-1084, ISSN2815-4282 –онлайн издание
6. Димова Г. Управление на риска при свлачища, срутища и земни пропадания. . International Scientific Conference "Defense Technologies" DefTech 2025,Faculty of Artillery, Air Defense and Communication and Information Systems. Стр.1066-1076, ISSN2815-4282 –онлайн издание
7. Инструкция № РД-02-20-25 от 20 септември 2011 г. за определяне на геодезически точки с помощта на глобални навигационни спътникови системи. Министерството на регионалното развитие и благоустройството, Обн. ДВ. бр.79 от 11 Октомври 2011 г.
8. Йовев И. GPS технологиите и създаване на условия за тяхното ефективно приложение в България, сп."География`21", бр.5, 2007.

9. Марков, М., Митев, И. /2024г./ Применение лазерного сканирования для картографирования картирования горных образований, Современные информационные технологии. Сборник научных статей по материалам 10-й Международной научно-технической конференции, стр. 453-464, Москва 2024г., УДК 004.65, ББК 32.973.26-018.2, eLIBRARY ID: 68606793, https://elibrary.ru/item.asp?id=68606793
10. Марков, М., /2024г./ Развитие гео роботов, Сборник научных статей по материалам 2-й Международной научно-практической конференции "Интеллектуальные и киберфизические системы: управление, логистика, безопасность", Страницы: 95-106, Номер: 3 (45), Год: 2024, УДК 004, ББК 22.18, eLIBRARY ID: 68620146, https://elibrary.ru/item.asp?id=68620146
11. Марков, М., /2025г./ Анализ дорожных рисков с применением лазерного сканирования, Сборник научных статей по материалам 7-й Международной научно-практической конференции "Методы и модели пространственного анализа", Страницы: 134-142, Номер: 1 (47), Год: 2025, УДК 004, ББК 22.18, eLIBRARY ID: 79510275, https://elibrary.ru/item.asp?id=79510275
12. Постоловски, А., Димитров, М., Марков, М. /2021г./ Приложение на MTLS – технология при одит на тунелното строителство, XVI международна конференция по открит и подводен добив на полезни изкопаеми, стр. 279-285, Варна 2021г., ISSN 2535-0854
13. Хаджиева, Б., Господинов, С., Марков, М., /2025г./ Необходима ли е геодезическа мрежа с местно предназначение при създаване на кадастрална карта за урбанизирана територия, Списание "Минно дело и геология", Брой 1-2/2025, Година LXXIX, ISSN 0861 – 5713, ISSN 2603 – 4549 (Online)
14. Хофман-Веленхоф Б., Лихтенегер Х., Колинс Дж. Глобална система за определяне на местоположение: Теория и практика. Превод от английски, София, УАСГ, 2002
15. Щерева К., Пеев И., Марков М. /2022г./ Анализ на времево обусловените премествания на дискретни точки от стената на яз. „Златоград“, Осма национална научнотехническа конференция с международно участие, стр. 81-87, Девин 2022г., ISSN 1314-7056
16. Andreev A., Andreeva G. Modeling of the river system of Goliama Kamchia. Journal "Scientific and applied research", vol.2, p.50-58, 2012 ISSN 1314-6289 София – 2016 г.
17. Keller W. Observation Techniques in Satellite Geodesy , 2003.
18. Leick A, GPS satellite surveying. Third edition, Wiley, 2004.
19. Markov, M., /2026/ Assessment and monitoring of road marking reflectivity using mobile laser scanning to improve road safety, Trakia Journal of Sciences, Vol. 24, No 2, pp 192-196, 2026, ISSN 1313-3551 (online), doi:10.15547/tjs.2026.02.014

Proceedings of International Scientific Conference -" Defense Technologies" **DefTech 2026**,
Faculty of Artillery, Air Defense and Communication and Information Systems

ANALYSIS OF EXISTING SPECIAL GEODETIC NETWORKS IN BULGARIA

Georgi Tanev

Department Geodesy, Air Defense and Communication and Information Systems Faculty – Shumen, "Vasil Levsky" National Military University, georgi91@gmail.com

Abstract: *This comprehensive report delivers an in-depth technical, mathematical, and regulatory analysis of the operational status, structural design, classification, and technological evolution of Special Geodetic Networks (SGN) in the Republic of Bulgaria. SGNs serve as critical spatial foundations providing sub-millimeter to millimeter local accuracy for major infrastructure assets (nuclear power plants, hydroelectric dams, long-span bridges, and mountain tunnels), structural deformation monitoring, specialized cadastral domains (Work Geodetic Foundation – WGF / РГО), and geodynamic research. The paper details the paradigm shift from classical optical-mechanical observation techniques to automated hybrid systems combining Robotic Total Stations (RTS), Static Multi-GNSS relative positioning, Terrestrial Laser Scanning (TLS), Synthetic Aperture Radar Interferometry (InSAR), and automated Real-Time Monitoring (RTM) within the Bulgarian Geodetic System 2005 (BGS 2005). Furthermore, the mathematical foundations of Least Squares Adjustment (LSA) for both free and constrained networks are analyzed alongside localized 7-parameter 3D Helmert coordinate transformations from the legacy Coordinate System 1970 (CS-1970) to BGS 2005 (UTM projections). Systemic operational challenges—such as physical monument destruction, scale-factor distortions, data fragmentation across ministerial bodies, and maintenance capital deficits—are evaluated. Strategic imperatives for future development emphasize complete digitalization, centralized registry integration, and automated telemetry. [1], [2], [7], [10], [11]*

Keywords: *special geodetic networks; BGS 2005; deformation monitoring; free network adjustment; WGF.*

Introduction

The geodetic infrastructure of any nation represents the essential, albeit invisible, spatial backbone for national security, territorial planning, urban development, the construction and operation of complex engineering structures, and the monitoring of hazardous geodynamic processes. In the Republic of Bulgaria, the Unified Geodetic Foundation (UGF) establishes the general horizontal and vertical reference frame at the national level. However, solving complex engineering-geodetic, industrial, deformation, and specialized cadastral tasks demands levels of local accuracy, spatial point density, and geometric stiffness that fundamental state networks cannot provide independently. [1], [2], [8]

This specific, high-responsibility niche is filled by Special Geodetic Networks (SGN). SGNs are purpose-built engineering-geodetic control structures established, stabilized, and observed for a specific facility, territory, or monitoring type. The primary characteristics distinguishing SGNs from the state network include: [5], [6]

Superior Local Precision: Internal relative point positioning tolerances ranging from ± 0.1 mm to ± 2.0 mm depending on project technical specifications.

Optimized Geometric Configuration: Tailored network geometry designed to maximize structural stiffness and error propagation isotropy. [10]

High Physical Stability: Specialized monumentation engineered to eliminate thermal expansion, soil creep, and micro-movements. [5], [8]

1. Regulatory and Normative Framework in Bulgaria

The establishment, approval, mathematical adjustment, and maintenance of SGNs in Bulgaria are governed by a complex hierarchy of legislative acts, technical ordinances, and institutional standards: [1], [2], [3], [4], [7]

Law on Geodesy and Cartography (LGC): Establishes the legal status and structure of the Unified Geodetic Foundation (Article 13) and defines the institutional and technical principles for establishing local-purpose and special-purpose geodetic networks. [1]

Ordinance No. 2 of July 30, 2010 (MRDPW & MoD): Regulates the definition, implementation, and maintenance of the Bulgarian Geodetic System 2005 (BGS 2005). BGS 2005 defines: [2]

- **Horizontal Reference Frame:** BGS 2005 (aligned with ETRS89, epoch 2005.0) associated with the Ellipsoid GRS80 and UTM projection (Zones 34N and 35N). [2]
- **Vertical Reference Frame: European Vertical Reference Frame 2007 (EVRF2007), realized locally via the State Leveling Network. [2], [4]**

Ordinance No. RD-02-20-9 of May 21, 2012 (MRDPW): Outlines technical procedures for designing, executing, adjusting, and accepting local geodetic control networks (GMMR). [3]

Ordinance No. RD-02-20-1 of January 15, 2021 (AGCC): Specifies standards for establishing and maintaining the State Leveling Network, defining tolerances for Class I and Class II precise leveling. [4]

Specialized Instructions for Deformation Measurements (GUGK / AGCC / NEK): Normative instructions for high-precision geodetic measurements applied to monitoring dams, nuclear power plants, tunnels, and active landslide zones. [4], [6], [7]

2. Comprehensive Typology and Technical Classification of SGNs

SGNs in Bulgaria are categorized into four core domains based on their functional application, required precision, and operational lifecycle:

2.1. Engineering and Construction Control Networks

These networks are established on major industrial, energy, and infrastructure construction sites prior to building operations to govern spatial setting-out, assembly alignment, and structural positioning: [5]

Bridges, Viaducts, and Tunnels: Designed with extreme horizontal relative precision (± 0.5 mm to ± 2 mm) to guarantee breakthrough accuracy in tunneling and precise alignment of pre-cast bridge decks.

Industrial Complexes and Nuclear Power Plants (e.g., Kozloduy NPP): Micro-geodetic networks established on concrete foundation pads using forced-centering pillars. Vertical control utilizes deep-seated fundamental benchmarks anchored directly into

unweathered bedrock to monitor differential settlement of reactor containment buildings and turbine pedestals.

2.2. Structural Deformation Monitoring Networks

Deformation networks are designed for periodic or continuous tracking of subtle spatial movements in structures or natural landforms: [6], [9]

Hydrotechnical and Dam Deformation Networks: Installed on large concrete and embankment dams (e.g., Tsankov Kamak, Kardzhali, Iskar). They consist of stable reference points located outside the reservoir's active load zone, paired with deformation targets placed on the dam crest, downstream face, and internal inspection galleries. Methods combine invar wires, high-precision robotic total stations, and Class I geometric leveling. [9]

Landslide and Coastal Slope Networks: Deployed along active geohazard zones along the Northern Black Sea coast, the Danube riverbank, and mountainous highway corridors (e.g., Struma Highway, Kresna Gorge). [9]

2.3. Specialized Cadastral Networks (Work Geodetic Foundation - WGF / РГО)

WGF points are established as dense local control networks to support specialized cadastral mapping (underground utility networks, railway corridors, seaport basins, airport runways, and international state boundaries). WGF ensures boundary restoration tolerances under ± 0.05 m in urban zones. [7], [8]

2.4. Geodynamic and Scientific Research Networks

National GNSS Geodynamic Network: Comprises fundamental geodetic stations tied to continuously operating reference stations (CORS) across Bulgaria. It tracks active tectonic faulting, crustal deformation rates, and seismic hazard dynamics in the Balkan and Black Sea regions. [6]

3. Optimization and Geometric Network Design

The establishment of an SGN requires rigorous mathematical optimization prior to field data acquisition. Network design is classified into four sequential phases (Grafarend Design Framework): [10]

1. Zero-Order Design (ZOD) – Datum Definition: Selection of the mathematical reference system and strategy for fixing network origin, orientation, and scale. In SGNs, free network adjustments are preferred to avoid introducing external constraints.

2. First-Order Design (FOD) – Network Configuration: Optimizing point location and ray geometry to maximize structural stiffness and homogenize error propagation across all nodes.

3. Second-Order Design (SOD) – Weight Allocation: Selecting optimal measurement types (angles, distances, height differences, GNSS baselines) and instrument precision classes.

4. Third-Order Design (TOD) – Network Densification: Integrating new observation points into existing control schemes without weakening overall network geometry. [5], [8]

Precision Evaluation via Error Ellipses

Horizontal precision at any network node i is evaluated using the co-factor matrix $Q_{xx} = (A^T PA)^{-1}$. The semi-major axis a_i and semi-minor axis b_i of the mean error ellipse are derived as: (formulas 1 and 2)

$$a_i = \sigma_0 \sqrt{\frac{1}{2}\left(q_{xx} + q_{yy} + \sqrt{\left(q_{xx} - q_{yy}\right)^2 + 4q_{xy}^2}\right)} \quad (1)$$

$$b_i = \sigma_0 \sqrt{\frac{1}{2}\left(q_{xx} + q_{yy} - \sqrt{\left(q_{xx} - q_{yy}\right)^2 + 4q_{xy}^2}\right)} \quad (2)$$

Where q_{xx}, q_{yy}, q_{xy} are elements of the co-factor matrix Q_{xx} corresponding to point i, and σ_0 is the a posteriori reference standard deviation. The orientation angle θ_i of the semi-major axis is given by:

$$\tan(2\theta_i) = \frac{2q_{xy}}{q_{xx} - q_{yy}} \quad (3)$$

4. Monumentation and Physical Stabilization Techniques

Because SGNs demand long-term millimeter stability, conventional surface boundary markers are inadequate. SGN monumentation utilizes advanced geotechnical designs:

Forced-Centering Observation Pillars: Used extensively in industrial sites, dam monitoring, and high-precision triangulation schemes. Reinforced concrete pillars are sunk below the seasonal frost line (1.5 m to 2.5 m). The top surface features a precision-machined stainless steel or brass plate with a standard 5/8-inch thread or Leica spigot, eliminating centering errors ($\sigma_{center} \leq \pm 0.1$ mm). [8]

Deep-Seated Bedrock Benchmarks: For precise leveling and vertical deformation control, benchmarks consist of heavy-gauge steel pipes inserted into boreholes anchored into unweathered bedrock at depths between 3 m and 20 m. An outer sleeve pipe filled with bitumen isolates the internal rod from seasonal soil swelling and frost heave. [8]

Climate-Controlled Pillars for GNSS and RTS: Permanent monitoring installations feature thermally insulated pillars equipped with internal heating elements to minimize structural bending caused by asymmetrical solar radiation.

5. Technological Evolution and Observation Methods

5.1. High-Precision Terrestrial Methods

Modern terrestrial SGN observations utilize Robotic Total Stations (RTS) capable of $0.5''$ angular precision and distance measurement accuracy of $0.5\ \text{mm} + 1\ \text{ppm}$. Direction observations are executed in multiple sets (gyres) using automatic target recognition (ATR) to eliminate pointing error, while environmental parameters are monitored continuously. Precise geometric leveling using digital levels with invar barcode staffs yields standard deviations under ± 0.3 mm/km double-run leveling. [4], [5]

5.2. Satellite-Based Multi-GNSS Positioning

GNSS positioning in SGNs is conducted strictly via Static Relative Positioning with observation sessions ranging from 4 to 24 hours using multi-frequency Multi-GNSS receivers paired with Choke-Ring antennas and precise satellite orbit ephemerides (IGS). [6], [9]

5.3. Advanced Remote Sensing Techniques (TLS & InSAR)

Terrestrial Laser Scanning (TLS) and Interferometric Synthetic Aperture Radar (InSAR) complement terrestrial SGNs by offering continuous surface deformation modeling across structures and landforms.

6. Comparative Technological Assessment

Feature / Parameter	**Traditional SGN (Pre-2000)**	**Modern Advanced SGN (Current State)**
Primary Instrumentation	Optical theodolites ($1''$), invar tapes, optical levels	Robotic Total Stations ($0.5''$), Multi-GNSS, TLS, InSAR
Coordinate Reference Frame	Local independent grids, CS-1970 (zone-based)	BGS 2005 / ETRS89 (UTM 34N/35N), EVRF2007 height frame
Data Processing Paradigm	Manual / semi-automated least-squares adjustment	Automated 3D rigorous matrix adjustments (TBC, Leica Infinity)
Automation Level	Manual periodic campaign measurements	Continuous automated real-time telemetry (RTM)
Vertical Accuracy Standard	± 1.0 mm/km $\div \pm 2.0$ mm/km	$\leq \pm 0.3$ mm/km (Digital Leveling + Invar Staffs)

7. Rigorous Mathematical Processing and Network Adjustment

The mathematical processing of SGNs is governed by the Gauss-Markoff Model of Least Squares Adjustment (LSA) using parametric observations: [10], [11]

$$v = A \cdot dx - L \tag{4}$$

For constrained networks with fixed control points, the solution is $dx = N^{-1}A^{T}PL$. In free network adjustments, N is singular ($\det(N) = 0$) and the solution utilizes the Moore-Penrose pseudo-inverse N^{+} derived via Singular Value Decomposition (SVD): $dx = N^{+}A^{T}PL$. This isolates pure structural deformation from overall translation or rotation of the reference frame. (Fig.3.)

8. Spatial Transformations: CS-1970 to BGS 2005

Converting historical SGN observations from legacy Coordinate System 1970 to BGS 2005 (ETRS89 / UTM) requires a rigorous 3D 7- parameter Helmert Transformation:

At strategic engineering facilities, conventional periodic surveying has been augmented by Automated Real-Time Monitoring Systems (RTM) with continuous automated observation cycles and telemetry.

9. Systemic Challenges Facing SGNs in Bulgaria

1. Widespread Physical Monument Destruction: Intense construction, road repairs, and agricultural operations cause significant annual loss of control monuments.
2. Transformation Errors from CS-1970: Converting legacy cadastral and deformation networks to BGS 2005 frequently encounters non-linear local distortions.
3. Data Fragmentation and Administrative Silos: SGN data remains fragmented across separate public and private entities (AGCC, RIA, NEK, MRDPW, Municipalities).
4. Capital Maintenance Deficits: Periodic re-measurement of deformation networks requires continuous capital expenditure, which is frequently subject to budget cuts.

Conclusion

Special Geodetic Networks are a critical element of Bulgaria's engineering, civil safety, and scientific infrastructure. Their physical stability, geometric integrity, and processing rigor directly underpin the operational safety of major nuclear, hydrotechnical, and transportation assets. Key imperatives for future evolution include full digitalization with a centralized repository under the AGCC, complete systemwide alignment with BGS 2005, and expanding automated multi-sensor RTM networks. [2], [7], [9]

References:

1. Law on Geodesy and Cartography (Prom. SG No. 29 of April 7, 2006, as amended).
2. Ordinance No. 2 of July 30, 2010 on the definition, implementation, and maintenance of the Bulgarian Geodetic System 2005 (MRDPW & MoD, Prom. SG No. 62 of 2010).
3. Ordinance No. RD-02-20-9 of May 21, 2012 on the design, execution, and acceptance of local-purpose geodetic networks (MRDPW, Prom. SG No. 43 of 2012).
4. Instruction No. RD-02-20-1 of January 15, 2021 on the creation and maintenance of the State Leveling Network (AGCC).
5. Penev, E., & Madzharov, S. (2015). Applied Geodesy and Higher Geodesy in Construction. UACEG, Sofia.
6. Milev, G. (2012). Engineering Geodesy and Geodetic Networks for Deformation Studies. Technika Publishing, Sofia.

7. Agency for Geodesy, Cartography and Cadastre (AGCC). Technical Requirements and Instructions for Establishing the Work Geodetic Foundation. Sofia.
8. Tanev, T. (2024). Inspection and Construction of Points from the State Geodetic Network in Southern Bulgaria. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2024", Faculty of Artillery, Air Defense and CIS, NMU, Shumen, pp. 575–580, ISSN 2815-4282.
9. Tanev, T. (2025). Higrigraphyc measurements in the Bulgarian section of the Danube River. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2025", Faculty of Artillery, Air Defense and CIS, NMU, Shumen, pp. 1030–1037, ISSN 2815-4282.
10. Kuang, S. (1996). Geodetic Network Analysis and Optimal Design: Concepts and Applications. Ann Arbor Press, Michigan.
11. Niemeier, W. (2008). Ausgleichungsrechnung: Statistische Auswertemethoden für Geodäten und Geowissenschaftler. Walter de Gruyter, Berlin.

METHODS FOR ESTABLISHING SPECIAL GEODETIC NETWORK

Georgi Tanev

Department Geodesy, Air Defense and Communication and Information Systems Faculty – Shumen, "Vasil Levsky" National Military University, georgi91@gmail.com

Abstract: *This article provides an extended applied-scientific analysis of the methodology, mathematical modeling, and technological implementation in the design, monumentation, measurement, and mathematical processing of Special Geodetic Networks (SGN). The specific characteristics of SGNs as a critical component of engineering infrastructure—providing sub-millimeter and millimeter accuracy for deformation monitoring, construction of unique engineering structures (nuclear power plants, dams, tunnels), and specialized cadastral activities (Work Geodetic Foundation - WGF / РГО)—are discussed. A detailed review is conducted of classical terrestrial methods (triangulation, trilateration, linear-angular networks, precise leveling), satellite GNSS measurements (relative static positioning), and hybrid sensor systems. Algorithms for rigorous mathematical processing using the Least Squares Adjustment (LSA) method via free and constrained networks, systematic error corrections, atmospheric refraction effects, and transformation to the Bulgarian Geodetic System (BGS 2005) are analyzed. Special attention is given to the criteria for optimizing geometric configurations through accuracy analysis (error covariance matrix K_x) and reliability metrics. [5], [8]*

Keywords: *Special Geodetic Networks (SGN), LSA, BGS 2005, GNSS measurements, deformation analysis, error ellipses, WGF.*

Introduction

1.Theoretical Foundations of SGN

The Unified Geodetic Foundation (UGF) of the country establishes the general horizontal and vertical reference frame at the national level. However, for high-precision engineering-geodetic tasks, the point density, geometric configuration, and accuracy of state geodetic networks are often insufficient. [11]

Special Geodetic Networks (SGN) are local or regional engineering-geodetic control structures designed and implemented with specific precision, high reliability, and stable point monumentation. [11]

1.1. Classification and Purpose

SGNs are classified according to the following primary criteria:

- **Engineering and Construction Control Networks:** For positioning technological equipment (e.g., particle accelerators, nuclear reactors) with a relative precision of $1{:}\,100{,}000 \div 1{:}\,1{,}000{,}000$ (errors below 0.5 mm). [5]
- **Deformation Monitoring Networks**: For tracking spatial displacements of hydrotechnical structures (dams), bridges, tunnels, landslide areas, and geodynamic test sites. [7]
- **Work Geodetic Foundation (WGF / РГО):** For providing control for specialized cadastral maps, underground utilities, and urban planning projects. [10]

1.2. Normative Regulation in Bulgaria

The creation of SGNs in Bulgaria is governed by:

- Law on Geodesy and Cartography (LGC);
- Ordinance No. 2 of July 30, 2010, on the definition, implementation, and maintenance of the Bulgarian Geodetic System 2005 (BGS 2005);
- Ordinance No. RD-02-20-9 of May 21, 2012, on the design, execution, and acceptance of local-purpose geodetic networks;
- Instruction for surveying deformations of large engineering structures and landslides using geodetic methods.

2. Design and Optimization of Geometric Structure

The design of an SGN is a multi-criteria process in which network geometry is optimized prior to performing field measurements (Fig. 1). [8]

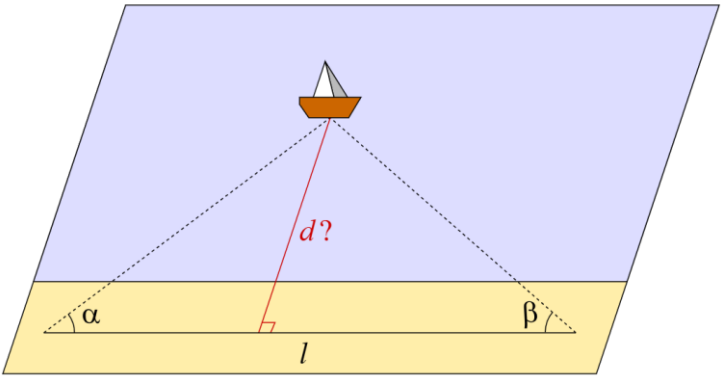


Fig. 1: Fundamentals of geometric triangulation

2.1. Optimization Criteria (Optimal Design)

The design process is divided into four ordering levels (Zero, First, Second, and Third Order Design):

- Zero Order Design (ZOD) – Datum Definition Problem: Selection of the covariance matrix definition and establishment of coordinate origin, orientation, and scale (particularly critical for free networks).
- First Order Design (FOD) – Configuration Problem: Selection of the optimal layout of geodetic points relative to the object under study to achieve maximum stiffness and homogeneous precision.
- Second Order Design (SOD) – Weight Allocation Problem: Optimal distribution of measuring instrument precision (choosing between angular, linear, or GNSS observations).

- Third Order Design (TOD) – Densification Problem: Inclusion of new points into existing networks without degrading overall stability. [11]

2.2. Mathematical Criteria for Accuracy and Reliability

The quality of the designed network is evaluated using the weight coefficient matrix through formula 1:

$$Q_{xx} = (A^T P A)^{-1} \tag{1}$$

Accuracy evaluation is performed by analyzing 3D error ellipsoids or 2D error ellipses in the plane. The semi-axes a and b of the mean error ellipse for a given point are calculated using the formulas 2 and 3:

$$a = \sigma_0 \sqrt{\frac{1}{2}\left(q_{xx} + q_{yy} + \sqrt{\left(q_{xx} - q_{yy}\right)^2 + 4q_{xy}^2}\right)} \tag{2}$$

$$b = \sigma_0 \sqrt{\frac{1}{2}\left(q_{xx} + q_{yy} - \sqrt{\left(q_{xx} - q_{yy}\right)^2 + 4q_{xy}^2}\right)} \tag{3}$$

Where q_{xx}, q_{yy}, q_{xy} are elements of the covariance matrix K_x, and σ_0 is the a posteriori standard deviation of unit weight. [8]. [9]

3. Monumentation and Reconnaissance Methods

The physical stability of SGN point monuments determines the long-term reliability of the entire system. Unlike general networks, eliminating micro-movements of the monument itself is required here. [5]

3.1. Types of Centers and Fundamental Benchmarks

- **Deep-seated Benchmarks (pipe or concrete):** Placed below the frost penetration line ($1.5 \div 3.0$ m), and for deformation networks, anchored into solid bedrock (piles down to $10 \div 20$ m).
- **Wall Bracket Benchmarks with Forced Centering:** Used for forced centering where instrument setups attach directly to a fixed metal plate with standard threading, eliminating optical/laser centering errors (≤ 0.1 mm).
- **Thermally Stabilized Pillars:** Designed for permanent GNSS stations or continuous automated robotic total stations (RTS).

4. Measurement Methods and Technologies

4.1. High-Precision Terrestrial Geodetic Surveying

- **Precise Angular Triangulation / Linear-Angular Networks:**
  - Executed using Robotic Total Stations (RTS) with angular accuracy of $0.5'' \div 1''$;
  - Gyro/set observation methods are applied for horizontal angles with complete compensation for inclination and collimation errors;
- **Precise Electronic Trilateration:**

- Distance measurements using laser distance meters with an accuracy of 0.5 mm $+ 1$ ppm;
- Mandatory application of meteorological corrections (temperature, atmospheric pressure, humidity) using the Barrell & Sears formula to derive the group refractive index n.

- **Precise Geometric Leveling (Class I and II):**
  - Performed using digital levels with accuracy ≤ 0.3 mm/km double-run leveling and invar barcode staffs;
  - Strict sightline symmetry (equal backsight and foresight distances within ≤ 0.5 m) is maintained to eliminate Earth curvature and atmospheric refraction effects.

4.2. Satellite (GNSS) Methods

- Relative Static GNSS positioning is applied exclusively for SGNs, with session durations ranging from 2 to 24 hours depending on baseline lengths;
- Multi-frequency GNSS receivers equipped with Choke-Ring antennas are used to mitigate multipath interference;
- Baseline vectors are processed with fixed phase ambiguity resolution using precise orbital ephemerides (IGS). [12]

5. Mathematical Processing and Adjustment of SGNs

Mathematical processing is based on the rigorous application of the Least Squares Adjustment (LSA) method using parametric observations. [6], [9]

5.1. Linearization of Parametric Equations

For each measured quantity S (distance) or α (azimuth/direction), a parametric observation equation for residuals is formulated through formula 4:

$$v = A \cdot \delta x - L \tag{4}$$

Where:

- A is the matrix of first partial derivatives (design matrix);
- δx is the vector of unknown coordinate corrections;
- $L = L_{\text{obs}} - L_{\text{calc}}$ is the vector of misclosures;
- v is the vector of residuals.

The LSA condition is: (formula 5)

$$v^T P v = \min \tag{5}$$

Where $P = K_l^{-1}$ is the weight matrix of observations.

5.2. System of Normal Equations and Solution

The normal equation system is expressed as: (formula 6)

$$(A^T PA) \cdot \delta x = A^T PL \tag{6}$$

Setting $N = A^T PA$ (normal equation matrix) yields: (formula 7)

$$\delta x = N^{-1} A^T PL \tag{7}$$

5.3. Free vs. Constrained Geodetic Networks

- **Constrained Networks:** Involves fixing k control points from the state network. The internal accuracy of the SGN can be degraded by errors in the external control data.
- **Free Networks (Free Network Adjustment):** The normal matrix N is singular ($\det N = 0$). The solution is derived using pseudo-inversion (Moore-Penrose inverse N^+) or via inner constraint conditions ($\delta x^T \delta x = \min$). This allows evaluation of the pure internal precision and stiffness of the SGN without deformation from external frames.

6. Transformation and Integration into BGS 2005

When integrating SGNs into the national BGS 2005 reference frame, a 7-parameter 3D Helmert transformation procedure is applied. For planar networks in UTM projections (Zones 34N / 35N) or legacy CS-1970, 2D conformal affine or Helmert transformations are implemented, strictly accounting for projection scale factors. [2], [10]

7. Practical Applications and Modern Challenges

7.1. Automated Real-Time Monitoring Systems (RTM)

Modern SGNs at critical infrastructure assets (e.g., Tsankov Kamak Dam, Kozloduy NPP) evolve into Real-Time Monitoring systems. Robotic total stations integrated with temperature and tilt sensors execute continuous measurements, automatically issuing alarm notifications when critical deformation thresholds are exceeded. [7]

7.2. Major Operational Challenges in Bulgaria

- **Monument Destruction:** Lack of strict enforcement mechanisms to preserve local network control points during infrastructure construction.
- **Data Fragmentation:** Absence of a centralized digital registry for SGNs under the Agency for Geodesy, Cartography and Cadastre (AGCC).
- **Transition from CS-1970 to BGS 2005:** The necessity of converting historical local deformation networks to the new reference frame without losing metric accuracy.

Conclusion

Special Geodetic Networks form the foundation of high-precision engineering geodesy. Their optimal design based on mathematical principles, the application of modern hybrid sensor methods (RTS + GNSS + digital leveling), and rigorous processing via free network adjustments ensure the reliability required for strategic infrastructure safety. The future of SGNs relies on full digitalization, integration with BIM/GIS platforms, and automated real-time telemetry. [12]

References

1. Закон за геодезията и картографията (Обн. ДВ. бр. 29 от 7 Април 2006 г., посл. изм. и доп.).
2. Наредба № 2 от 30 юли 2010 г. за дефиниране, реализация и поддържане на Българската геодезическа система 2005 (Издадена от МРРБ, Обн. ДВ. бр. 62 от 10 Август 2010 г.).
3. Наредба № РД-02-20-9 от 21 май 2012 г. за проектиране, изпълнение и приемане на геодезически мрежи с местно предназначение (Издадена от МРРБ, Обн. ДВ. бр. 43 от 8 Юни 2012 г.).
4. Инструкция за изследване деформациите на големи инженерни съоръжения и свлачища с геодезически методи (ГУГК, София).
5. Минчев, С., & Василев, Х. (2015). Високопрецизни геодезически измервания в инженерната геодезия. Издателство „УАСГ", София.
6. Пенев, Е. (2018). Математическа обработка на геодезически измервания и МНМК. Издателство „Академична геодезия", София.
7. Milev, I., & Tzontchev, R. (2018). Deformation Monitoring Concepts and Applied Geodesy in Infrastructure Projects. Journal of Geodesy and Cartography, Vol. 44(2), pp. 112–125.
8. Kuang, S. (1996). Geodetic Network Analysis and Optimal Design: Concepts and Applications. Ann Arbor Press, Michigan.
9. Niemeier, W. (2008). Ausgleichungsrechnung: Statistische Auswertemethoden für Geodäten und Geowissenschaftler. Walter de Gruyter, Berlin.
10. Агенция по геодезия, картография и кадастър (АГКК). Технически спецификации за прилагане на БГС 2005 при инженерни мрежи. (cadastre.bg).
11. Tanev, T. (2024). Inspection and Construction of Points from the State Geodetic Network in Southern Bulgaria. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2024", Faculty of Artillery, Air Defense and CIS, NMU, Shumen, pp. 575–580, ISSN 2815-4282.
12. Tanev, T. (2025). Hydrographic measurements in the Bulgarian section of the Danube River. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2025", Faculty of Artillery, Air Defense and CIS, NMU, Shumen, pp. 1030–1037, ISSN 2815-4282.

METHODS FOR INVESTIGATING VERTICAL DEFORMATIONS

Tsvetelina T. Mateeva, Vladimir M. Petrov

Faculty of Artillery, Air Defense and Communication and Information Systems, National Military University, Shumen, Bulgaria, cveti.mateeeva@abv.bg, vladimir8850@mail.bg.

Abstract: *This report will examine various methods for investigating vertical deformations. The classical methods include geometric, trigonometric, and hydrostatic levelling, based on precise angular and linear observations. Concurrently, global navigation satellite systems (GNSS) are increasingly being applied, providing high-precision real-time data. The results obtained confirm that combining the two methods ensures greater reliability and accuracy in monitoring deformations. It will also explore how these deformations directly affect dam walls.*

Keywords: *Vertical deformationl; levelling; GNSS.*

Introduction

Control over the stability and deformations of dam walls is a fundamental aspect of hydraulic engineering, maintenance, and operation of water management facilities. These structures play a critical role in water supply, irrigation, energy production, water level regulation, and flood protection. Deformations represent displacements of the structure or its individual parts caused by changes in the foundation, stresses, or external loads associated with operation and the environment. They become particularly dangerous when manifesting in specific directions or reaching significant proportions, with consequences ranging from operational difficulties and equipment damage to structural failure, severe material losses, and risks to human life.

Any deviation from the design state, particularly in the form of deformations, can threaten the technical integrity of dam walls, the environment, and public safety. Therefore, the monitoring of horizontal and other types of deformations constitutes an essential part of structural health monitoring, as geometric changes are often indicative of instability, displacements, or external impacts. Timely detection allows for accident prevention and the planning of repair and restoration activities.

Due to the diversity of engineering structures in terms of construction, purpose, and scale, the factors influencing deformations also vary. Consequently, classifying the types of deformations (Fig. 1), determining criteria and parameters, and utilizing appropriate methods (Fig. 2) for presenting results are crucial for accurate analysis and timely decision-making regarding safety and maintenance.

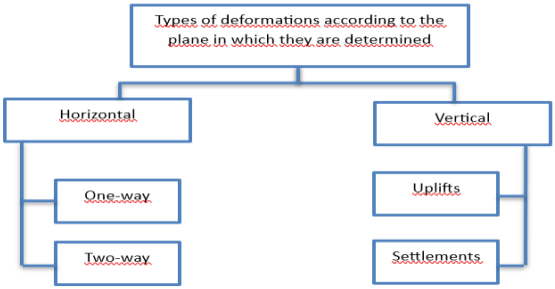


Fig. 1: Types of deformations according to the plane in which they are determined

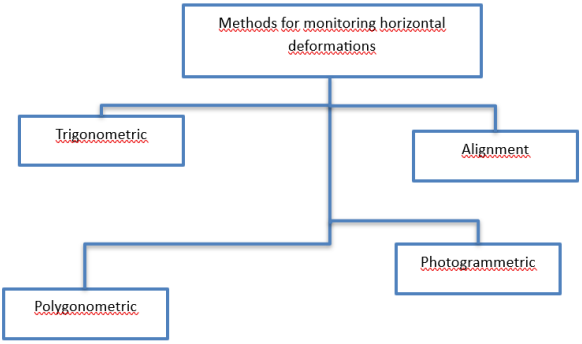


Fig. 2: Methods for Monitoring Horizontal Deformations

1.1. Trigonometric Method

This method utilizes a reference network of stable points from which angular and linear measurements are performed to determine the displacements of control points. It is suitable for precision observations over limited distances (up to ~300 m). It is characterized by high accuracy but requires a stable reference system and repeated measurements (Fig. 3)

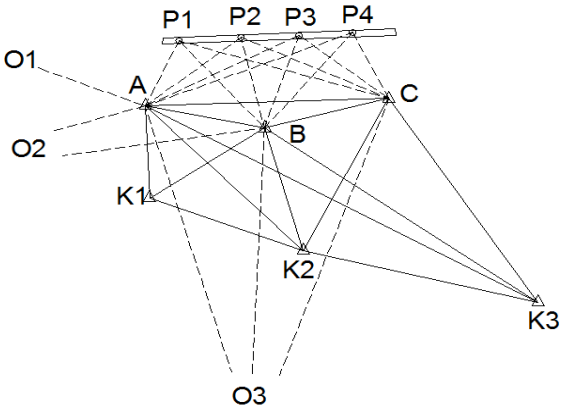


Fig. 3: Scheme of application of the trigonometric method

1.2 Traverse Method

Applied to linear structures by establishing traverse lines between reference points. Angles and distances are measured using total stations, and displacements are determined by comparing coordinates across different epochs. The method is convenient for larger structures.

1.3 Alignment Method

A classical approach used for linear structures. It determines the deviations of control points from a straight line (alignment) defined by stable terminal points. The method is relatively simple and reliable, but its accuracy is limited over long distances (Fig. 4).

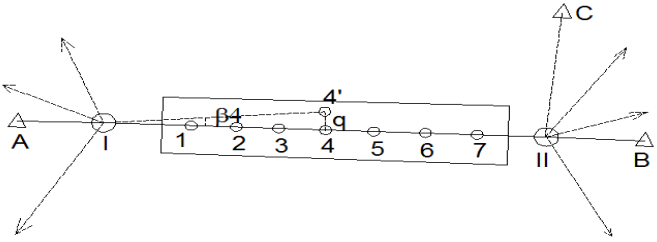


Fig. 4: Alignment method setup

1.4 GNSS Methods

The use of global navigation satellite systems enables high-precision, real-time displacement monitoring. It is applicable for large structures and in conditions where

direct line-of-sight between points is lacking. It requires at least three reference stations outside the deformation zone. [5], [6], [9]

1.5 Laser Scanning

Laser scanners can provide accurate three-dimensional models of structures and detect minor deformations that cannot be captured using traditional methods.[8]

1.6 Photogrammetric Method

Photogrammetry is a modern method for investigating dam wall deformations, utilizing aerial or terrestrial photographs to generate precise three-dimensional models of the object. By comparing images captured at different epochs, changes in geometry and horizontal displacements of the dam can be established. The technology allows for covering large areas without direct physical intervention on the structure while ensuring high precision and detail. Using specialized software, results are rapidly processed and visualized in the form of digital models and deformation maps. This makes photogrammetry a valuable tool for efficient and safe monitoring. [7]

2. Methodology of Observations

Geodetic surveys are conducted cyclically at predefined time intervals. The main stages include:

1. Designing a reference network and deploying control points on the structure.
2. Performing instrumental measurements (angles, distances, coordinates).
3. Data processing and adjustment.
4. Analysis through the comparison of results from different epochs.
5. Interpretation of results to identify trends, forecast future deformations, and undertake mitigating measures.

Discussion / Findings

The relationship between traditional and modern methods for investigating horizontal deformations is characterized by continuity and advancement. Classical methods—trigonometric, traverse, and alignment—lay the foundation of observations, having proven their reliability and accuracy. They establish the baseline upon which modern technologies are built. New methods such as GNSS, laser scanning, and photogrammetry do not entirely replace traditional ones; rather, they complement them by ensuring faster data acquisition, broader coverage, and continuous monitoring capabilities. In practice, a combined approach is frequently applied, where classical techniques guarantee stability and control, while modern ones ensure automation and detail. Thus, the highest reliability in analyzing and managing dam wall deformations is achieved.

Conclusion

The investigation Conclusion of horizontal deformations in dam walls is a key process for maintaining their safety and long-term operation. By combining classical and modern geodetic methods, engineers can provide reliable data on the state of structures and mitigate potential risks.

References:

1. Андреев А. Инженерни,природонаучни и други направления на приложната геодезия. УИ „Еп. К. Преславски'' 2020 Част I
2. Андреев А. Инженерни,природонаучни и други направления на приложната геодезия. УИ „Еп. К. Преславски'' 2020 Част II
3. Геодезически методи за мониторинг на деформации. Университет по архитектура, строителство и геодезия, София.
4. Георгиев М. (2012). Проектиране и наблюдение на язовирни стени. Технически университет – София.
5. Tanev, G. (2024). Maintenance of the Magnetic Station Network and Determination of Geomagnetic Field Elements in Northern Bulgaria. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2024", Faculty of Artillery, Air Defense and CIS, NMU, Shumen, pp. 562–574, ISSN 2815-4282.
6. Tanev, T. (2024). Inspection and Construction of Points from the State Geodetic Network in Southern Bulgaria. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2024", Faculty of Artillery, Air Defense and CIS, NMU, Shumen, pp. 575–580, ISSN 2815-4282.
7. Tanev, T., & Tanev, G. (2023). Establishment of Ground Control Points for Photogrammetric Surveying for Mapping the Northern Slopes of the Balkan Mountains. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2023", NMU, Shumen, pp. 679–684, ISSN 2367-7902.
8. Tanev, T. (2025). Higrigraphyc measurements in the Bulgarian section of the Danube River. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2025", Faculty of Artillery, Air Defense and CIS, NMU, Shumen, pp. 1030–1037, ISSN 2815-4282.
9. Tanev, G. (2025). Surveying and maintenance of the primary-class points of the state GPS network of the Republic of Bulgaria. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2025", Faculty of Artillery, Air Defense and CIS, NMU, Shumen, pp. 1038–1042, ISSN 2815-4282.

BASICS OF REMOTE SENSING AND SATELLITE SYSTEMS

Desislava A. Delkova, Momchil G. Georgiev, Veselin H. Gepov

Department of Geodesy, "Vasil Levski" NMU, Shumen, Bulgaria, desislavadelkova@abv.bg

***Abstract**: Remote sensing is a method of obtaining information about the Earth from a distance using sensors on satellites and aircraft, without physical contact. It measures reflected or emitted electromagnetic energy and goes through six stages – from the energy source (the Sun) to data analysis by the user. Its advantages include wide coverage, repeatability, speed, access to remote areas, and cost-effectiveness. Its applications cover environmental monitoring, agriculture, urban planning, cartography, defence, and telecommunications. There are two main types of sensors – passive (working only during the day in clear weather) and active (working day and night in all weather conditions), which complement each other. The future of remote sensing is connected with hyperspectral sensors, microsatellites, and artificial intelligence, which will make observation even more accurate and accessible.*

***Keywords:** Remote sensing; sensors; satellites*

Introduction

Remote sensing is the science of getting information about objects, areas, or natural events without having direct physical contact with them. Instead, we use special devices called sensors, which are placed on aircraft, drones, or satellites. These sensors measure the energy that is reflected or emitted from the Earth's surface.

In other words, remote sensing is like taking pictures of the Earth from a great height, but these pictures contain much more information than ordinary photographs. They can show temperature, humidity, plant health, water pollution, and even movements of the Earth's crust.

The term covers both the collection of data (through sensors) and its processing and interpretation (through computers and human analysis). Today, remote sensing is an essential tool in hundreds of professions – from farmers and geographers to military personnel and environmentalists.

1 How does remote sensing work?

First we need a source of energy. Everything starts with energy. In passive systems (the most common type), the source is the Sun. It sends light and heat towards the Earth.

Then the solar energy travels through the Earth's atmosphere. Some of the energy is scattered or absorbed by gases, water vapour, and dust particles. This affects the quality of the data, so scientists carefully consider atmospheric conditions.

Next the energy reaches the Earth's surface and interacts with different objects – trees, water, buildings, roads, soil, ice, etc. Each object reflects, absorbs, or emits energy in a different way. This is the basis of remote sensing – different materials have different "spectral fingerprints" [6].

In order to gain data the energy must be stored in some way. This is done by the sensor. It can be a camera, radiometer, spectrometer, or radar. Modern sensors are extremely sensitive and can capture energy in dozens of different bands [3].

The collected data is sent as radio signals to ground receiving stations. There, it is recorded, calibrated, and stored in digital format. Without these stations, remote sensing data would be useless.

The most important stage is human or computer analysis. Specialists look at the images, apply algorithms, search for patterns, and draw conclusions. This turns data into information. Final decisions depend on this stage – for example, whether to evacuate an area during a flood, or where to plant a specific crop.

The way images are taken in remote sensing is shown in fig. 1.

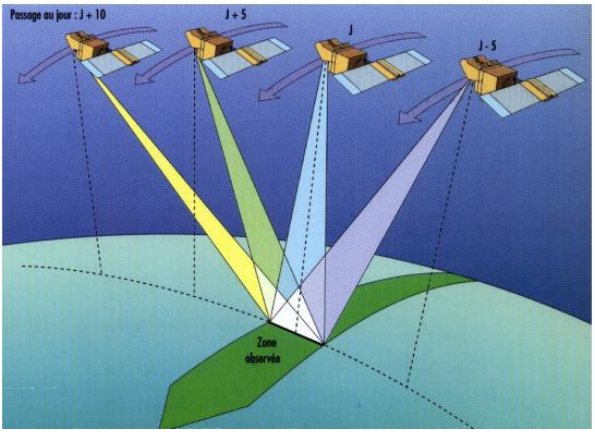


Figure 1: Taking pictures of the Earth

2 Advantages of Remote Sensing

Remote sensing offers many advantages that make it a preferred choice in many situations:

- **Wide coverage (synoptic view)** – One satellite image can cover an area of hundreds or thousands of square kilometers. This is impossible with ground surveys.
- **Repeatability and regularity** – Satellites orbit the Earth in predictable paths and can photograph the same place every few days or even hours. This allows us to track changes over time – for example, urban growth or glacier retreat.
- **Access to remote and dangerous areas** – With remote sensing, we can study deserts, jungles, oceans, polar regions, or war zones without risking human lives [2], [5].
- **Objectivity and accuracy** – Data is collected by machines, not people, which reduces subjective errors and bias.

- **Speed and efficiency** – Information can be obtained in minutes or hours, which is critical during disasters like earthquakes, floods, or oil spills.
- **Digital format** – Data is easy to archive, process with computer programs, and share between scientists and institutions around the world.
- **Cost-effectiveness** – In many cases, remote sensing is cheaper than organising large expeditions or ground measurements [7].

Having this in mind remote sensing can be used in almost all areas of human activity. We can group its use into three main categories:

- **Inventory and mapping** – Creating maps of land use, forests, water bodies, urban areas, and transport infrastructure [4], [8].
- **Monitoring and change detection** – Tracking changes over time – deforestation, urbanization, erosion, coastline changes, snow cover, etc.
- **Modelling and forecasting** – Using digital terrain models (DTM) for flood simulations, pollutant dispersion, or crop yield predictions.

3 Passive Sensors vs. Active Sensors – A Comparison

There are two main types of sensors used in space missions. Each has its own strengths and weaknesses, table 1.

Table 1: Comparison between passive and active sensors

Feature	Passive	Active
Energy source	Rely on the Sun	Have their own radar transmitter
Working time	Only during daylight	Work day and night
Weather effects	Clouds and rain block them	Not affected by clouds, fog, or rain
What they measure	Spectral characteristics – color, chemical composition	Physical characteristics – roughness, shape, moisture, dielectric properties
Update frequency	Depends on orbit and weather conditions	Constant, regardless of weather
Main applications	Cartography, agriculture, ecology, urban planning	Tectonics, ice monitoring, interferometry (InSAR), detecting flood traces

These two types of sensors do not compete – they complement each other. For example, a passive sensor can provide a detailed color map of an area, while an active sensor can show changes in the terrain after an earthquake, even if the sky is cloudy.

An example of passive sensor is an optical camera and an example of active sensor is a radar, fig. 2

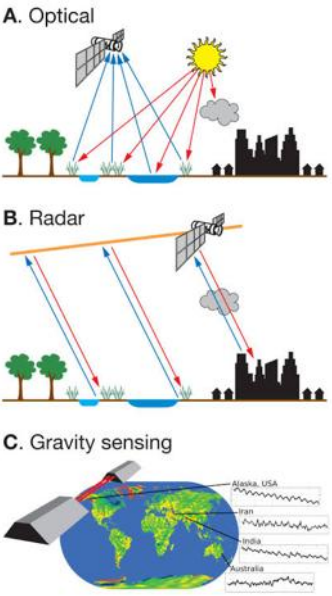


Figure 2: Optical sensor and a radar

Conclusion

Technology is advancing at a huge speed. Today we already have:

- **Hyperspectral sensors** that record hundreds of spectral channels, allowing us to identify minerals, pollutants, and even underground archaeological sites.
- **Microsatellites (CubeSats)** that are small, cheap, and can work in groups (constellations), providing daily coverage of the entire planet.
- **Artificial intelligence and machine learning** that automatically recognise objects, classify terrains, and predict events like droughts or floods [1].

In the future, remote sensing will become even more accessible, accurate, and fast. It will play a key role in fighting climate change, managing natural resources, and ensuring global security.

References

1. Borisova, A., L. Nikolov, "Systems with artificial intelligence for defense and security", Proceedings of the conference "Scientific research and education in the air force – AFASES 2023", pp. 53-58 https://doi.org/10.19062/2247-3173.2023.24.7
2. Bozov, I. "Remotely piloted aircraft systems (RPAS) in service to artillery formations", Proceedings of International Scientific Conference "Defense Technologies – DefTech 2022", Shumen, ISSN 2367-7902, pp.118-121

3. Lillesand M. et al. "Remote Sensing and Image Interpretation", Wiley, 7th edition
4. Niyazi-Yusuf, M. "Application of remote methods with unmanned aerial systems for the production of cadastral maps and cadastral registers on the territory of the Republic of Bulgaria", Mersin Photogrammetry Journal, Vol. 7, No. 1, pp. 1-8, Mersin, Turkiye, 2025, doi: 10.53093/mephoj.1666110
5. Parvanov, S. "Study on the use of hierarchical groups of unmanned aerial vehicles for area search and the detection of or strikes against specific targets", Proceedings of International Scientific Conference "Defense Technologies – DefTech 2023", Shumen, ISSN 2815-4282, pp.416-424
6. Salieva, N. "Spectral reflectance characteristics of the main classes of natural objects in remote sensing of the earth's surface", Scientific Conference with International Participation "MATTECH 2024", Shumen, 2024, ISSN 1314-3921, pp. 281-288
7. Stoyanova, S., I. Kalchev "Application of low-cost unmanned aerial systems for professional aerial photogrammetry", Geodesy, Cartography, Land Management Journal, No. 1-2, pp. 23-30, 2020
8. Tanev, T., G. Tanev "Establishment of Ground Control Points for Photogrammetric Surveying for Mapping the Northern Slopes of the Balkan Mountains", Proceedings of International Scientific Conference "Defense Technologies – DefTech 2023", Shumen, ISSN 2367-7902, pp. 679–684

METHODS FOR MAPPING THE BOTTOM OF A WATER BASIN

Tanislav Tanev

Department Geodesy, Air Defense and Communication and Information Systems Faculty – Shumen, "Vasil Levsky" National Military University, tanislav91@gmail.com

Abstract: *There is an analysis of the main methods used for mapping of the relief and characteristics of the bottom of water basins. The evolution of methods from classical direct measurements to modern remote sensing methods for collecting geospatial data is described. Acoustic mapping methods using single-beam and multi-beam echo sounders, as well as remote sensing methods (satellite bathymetry, LiDAR) are described. The methods for presenting cartographic data on nautical and pilot charts are described.*

Keywords: *mapping, single-beam and multi-beam echo sounders, remote sensing methods*

Introduction

Mapping the bottom of water basins is crucial for marine geodesy, oceanography, coastal zone protection, and the safety of river and maritime navigation. Unlike land, where direct topographic and aerophotogrammetric surveys are standard, the bottom of a water basin remains covered by water. This necessitates the development of specialized methods for measuring and subsequently mapping the bottom of the water basin.

The process of mapping the bottom of a water basin consists of two main stages:

1. Methods for collecting primary bathymetric and geophysical data (hydroacoustic, laser, satellite).
2. Cartographic methods for representing and modeling the relief (isobaths, bottom relief features, seabed type/ground, navigational hazards, underwater infrastructure).

1. Hydroacoustic Mapping Methods

Acoustic methods are the primary method for surveying the bottom of water basins of medium and great depths.

1.1. Method of Discrete Bathymetric Profiles (Single-Beam Acoustics with Survey Lines)

This was the first automated mapping method, based on single pulses emitted toward the bottom perpendicular to the water surface. [3], [4]

Principle: The travel time of the acoustic signal to the bottom and back is measured:

$$(d = \frac{v \cdot t}{2}) \quad (1)$$

where d is the measured depth, v is the propagation speed of the electromagnetic wave, and t is the two-way travel time of the wave to the bottom and back.

Cartographic specifics: The depth data consists of continuous series of points along the survey line (track) where the measurement was performed. This is clearly seen in Fig.

1. The areas between survey lines remain unsurveyed, requiring depth interpolation and side-scan sonar sweeps to search for objects and navigational hazards within those gaps (Fig. 2). [2]

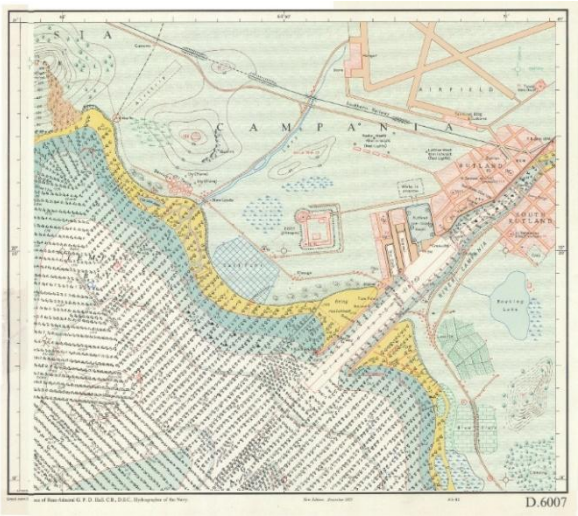


Fig. 1: Depths measured with a single-beam echo sounder

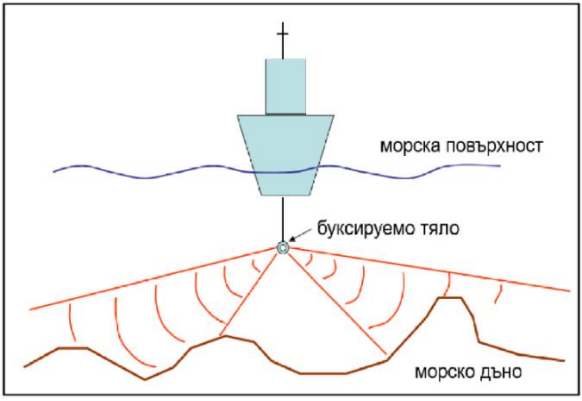


Fig. 2: Side-scan sonar

1.2. Area-based Mapping with Multi-Beam Echo Sounders

Multi-beam echo sounders transformed bottom mapping by transitioning from linear profiles to full areal coverage. [3], [4]

Principle: A wide, fan-shaped beam of pulses is emitted up to a 150° propagation angle, forming a swath on the bottom with a width 2 to 5 times the measured depth (Fig. 3).

Cartographic product: An extremely dense 3D point cloud is generated, serving as the basis for constructing digital bottom models.

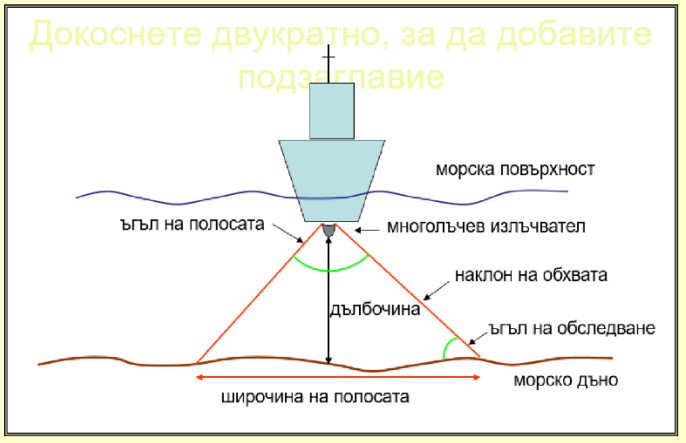


Fig. 3: Emission geometry of a multi-beam echo sounder

1.3. Acoustic Imaging Method

Side-scan sonar draws an acoustic image of the bottom comparable to a monochrome aerial photograph. By measuring backscatter strength, the texture and seabed composition (rocks, sand, mud) are determined, enabling the creation of geomorphological and lithological bottom maps.

2. Optical and Satellite Remote Sensing Methods

2.1. Airborne Laser Mapping (LiDAR Bathymetric Surveys)

Applied in shallow coastal zones (0 to 30–40 m depth) where vessel navigation is hazardous. Scanning lasers mounted on aircraft or UAVs are used. [7]

Result: A continuous model connecting terrestrial topography with underwater bathymetry within a shared coordinate and height system is generated.

2.2. Satellite Derived Bathymetry (SDB)

SDB relies on two fundamentally different methods:

Optical Satellite Bathymetry (for shallow waters): Uses multispectral satellite imagery (from Sentinel-2, Landsat, WorldView) based on the selective absorption of light by the water mass across different spectral bands (blue, green, red).

Satellite Altimetry (for deep water basins): Measures bulges and depressions on the sea surface (geoid) caused by the gravitational attraction of massive underwater topographic features (seamounts, ridges, trenches) (Fig. 4).

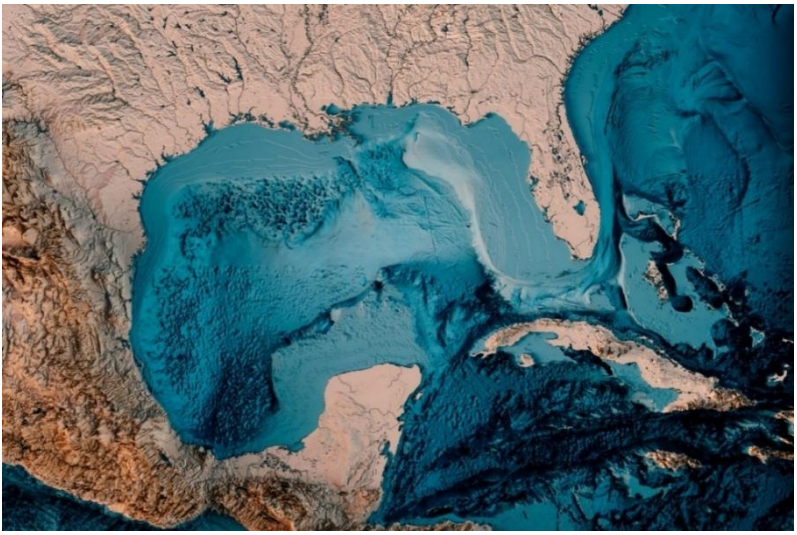


Fig. 4: Satellite altimetry of the Gulf of Mexico

3. Methods for Cartographic Representation of Bottom Relief

Classical and digital methods for visualizing underwater relief use specific standardized symbols and techniques established by the International Hydrographic Organization (IHO). [7], [8], [9], [10], [11]

3.1. Depth Sounding Spot Method

This is the oldest method, preserved to this day on nautical and navigational charts. Depths are written as numerical values at specific geographic points.

Point selection for mapping: During generalization, priority is given to plotting the shallowest depths (critical for navigation) and key relief features (peaks, deepest points in trenches).

3.2. Isobath Method

Isobaths are lines connecting points of equal depth, analogous to contours on topographic maps. They connect points of equal depth relative to the selected chart datum. Isobaths are typically drawn for depths of 2 m, 5 m, 10 m, 20 m, 50 m, 100 m, 200 m, 500 m, 1000 m, etc. [7]

Cartographic requirements: Conservative interpolation is applied to ensure navigation safety. In areas with large tidal fluctuations, Low Water (at ebb tide) and High

Water (at flood tide) are observed. In these cases, the Low Water point is adopted as the chart datum.

3.3. Bathymetric (Hypsometric) Tints Method

Used primarily in general geographic and educational maps to create a clear 3D/relief effect.

Color scale: Traditionally, a blue scale is used (lighter shades for shallow waters and progressively darker blue/violet tones for extreme oceanic depths). Modern 3D visualizations often utilize full spectral scales as well.

3.4. Hillshading and 3D Digital Models

In digital cartography, a hypothetical angular light source is calculated (typically from the northwest at a 45° angle). Dark shadows and light highlights provide a three-dimensional perception of slopes, canyons, and underwater ridges. For electronic navigational charts, compliance with standards established by the International Hydrographic Organization (IHO) and the Naval Hydrographic Service (such as S-57 and S-100) is mandatory. In recent years, a large-scale transition from the older generation of standards (S-57) to the modern Universal Hydrographic Data Model (S-100) has been underway. [10]

Table 4. Comparative Analysis of Surveying and Mapping Methods [5], [6]

Method	**Equipment**	**Accuracy & Resolution**	**Application**
Single-Beam Echo Sounder (SBES)	Acoustic transducer, GNSS	High along profile, low between profiles	River beds, traditional navigational tracks
Multi-Beam Echo Sounder (MBES)	Multi-beam array, INS/GNSS	Extremely high (centimetric)	Engineering hydrography, detailed bathymetric maps
Airborne LiDAR (ALB)	Dual-frequency laser on UAV/aircraft	High (up to 10–15 cm)	Coastal areas, shallow bathymetry
Satellite Altimetry	Radar altimeters (CryoSat, SWOT)	Low resolution (kilometers)	Global ocean maps (GEBCO), tectonics
Optical Satellite Bathymetry	Multispectral satellites	Medium (depends on water clarity)	Inaccessible regions, shallow tropical waters

Conclusion

Methods for mapping the seabed have evolved from point and profile measurements to continuous areal and 3D modeling. The integration of high-resolution hydroacoustic systems, remote satellite measurements, and modern GIS software enables the creation of precise marine navigational and thematic maps, as well as pilot charts for navigable rivers. The future of marine cartography is directly tied to the automation of data processing and the creation of dynamic digital products.

References

1. Белчев Б., Няголова З., Английски международни и адмиралтейски карти, изд. "Стено", Варна, 1997.
2. Дачев Ю., Хидрографски системи, използвани за заснемане на релефа на дъното на българското черноморско крайбрежие, Списание „Геодезия, картография, земеустройство", бр. 3-4, стр. 9-13, София, 2017, ISSN 0324-1610.
3. Стойков Е., Технически средства и системи при извършване на хидрографски измервания, ШУ, Шумен, 2019.
4. Коломийчук Н. Д., Гидрография, изд. МО, Москва, 1975.
5. Tanev, G. (2025). Surveying and maintenance of the primary-class points of the state GPS network of the Republic of Bulgaria. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2025", Faculty of Artillery, Air Defense and CIS, NMU, Shumen, pp. 1038–1042, ISSN 2815-4282.
6. Tanev, G. (2024). Maintenance of the Magnetic Station Network and Determination of Geomagnetic Field Elements in Northern Bulgaria. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2024", Faculty of Artillery, Air Defense and CIS, NMU, Shumen, pp. 562–574, ISSN 2815-4282.
7. IHO, Manual on Hydrography, Publication C-13, Monaco, 2011.
8. IHO Special Publication S-44, "IHO Standards for Hydrographic Surveys", Monaco, 2020
9. IHO Special Publication S-52, "Spécifications for Chart Content and Display Aspects of ECDIS", Monaco.
10. IHO Special Publication S-57, "IHO Transfer Standards for Digital Hydrographic Data", Monaco, 2005.
11. IHO Special Publication S-61, "Product Specification for Raster Navigational Charts", Monaco, 2011,
12. Symbols and abbreviations used on admiralty charts-NP 5011 (INT), Hydrographic office, London, United Kingdom, 2025.

MODERN MEANS FOR HYDROGRAPHIC SURVEYS

Tanislav Tanev

Department Geodesy, Air Defense and Communication and Information Systems Faculty – Shumen, "Vasil Levsky" National Military University, tanislav91@gmail.com

Abstract: *There is an overview of modern technical means for conducting hydrographic surveys in water areas of different types (shelf, coastal and inland water basins). The main technological directions are analyzed - multibeam echo sounders, side-scan sonar, airborne laser bathymetric imaging, as well as the integration of autonomous surface and underwater vehicles. Attention is paid to high-precision satellite positioning systems and inertial navigation systems that provide the spatial link of data with global geodetic reference systems. The processes of automated processing of data sets for seabed classification and the application of hydrographic data in marine cartography, engineering construction and inland waterways are examined.*

Keywords: *multibeam echo sounder, bathymetry, digital bottom models*

Introduction

Hydrography is an applied science dealing with mapping the relief of the bottom of water bodies. Over the last two decades, the science has undergone a fundamental transformation, moving from isolated single-point depth measurements (single-beam echo sounders) to high-resolution three-dimensional (3D) modeling of underwater relief. The main driver of this progress is the growing requirements for the safety of maritime and river navigation according to the standards of the International Hydrographic Organization (IHO), the Danube Commission, and the Rhine Commission. Modern hydrographic surveys represent a complex process combining acoustics, remote sensing methods, inertial navigation, and specialized data processing software.

1. Hydroacoustic Systems and Sensors

Acoustic waves remain the main tool for investigating the underwater environment due to the low level of sound absorption and attenuation in water compared to electromagnetic waves. Water, especially saline seawater, absorbs electromagnetic waves extremely quickly, which has necessitated the use of acoustic waves. [2], [3], [5]

1.1 Multibeam Echo Sounders (MBES)

Unlike traditional single-beam echo sounders, which measure depth only directly beneath the vessel, multibeam echo sounders form a fan-shaped beam of tens to hundreds of acoustic beams. [3]

Figure 1 shows the principle of fan-shaped bottom coverage with multibeam echo sounders. The emitted acoustic beam propagates in a fan shape, providing measurement of a wide swath of the bottom beneath the vessel.



Fig. 1: Principle of operation of a multibeam echo sounder

Operating Principle: A configuration of transmitting and receiving antennas is used (often in the form of a hydrophone array based on the Mills Cross geometry). The receiver uses phase and pulse detection methods to identify the bottom.

Characteristics: Operating frequencies range from 12 kHz (for deep-water oceanic surveys down to 11,000 m) to 200–700 kHz (for high-detail shallow-water surveys).

Advantages: Provides bottom coverage across a specific swath width as well as detection of underwater hazards (shipwrecks, rocks, shoals), generating dense point clouds (Fig. 2).

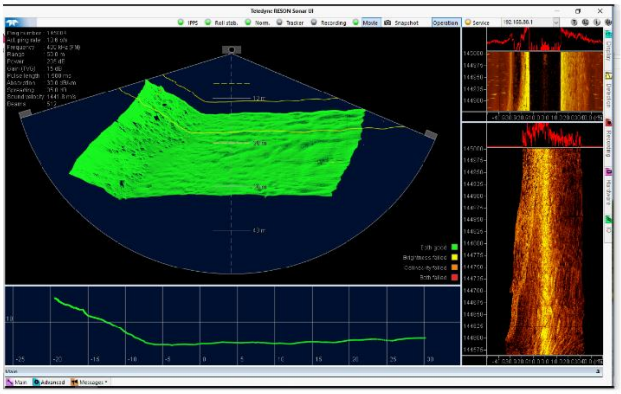


Fig. 2: Real-time bottom relief in the scanned swath beneath the vessel

1.2 Side Scan Sonar (SSS)

SSS systems are used to obtain high-resolution acoustic images of the relief and objects on the seabed (Fig. 3). [3], [7]

Operating Principle: Acoustic pulses that are narrow in the horizontal plane and wide in the vertical plane are emitted from both sides of the scanning body (towed sonar body or hull-mounted sensor).

Application: Detecting the position of infrastructure objects (cables, pipelines) and navigational hazards (shipwrecks, shoals, boulders), as well as determining bottom sediment types (sand, mud, rock) based on backscatter intensity. Modern systems operate on multiple frequencies simultaneously (e.g., 300/600/900 kHz).

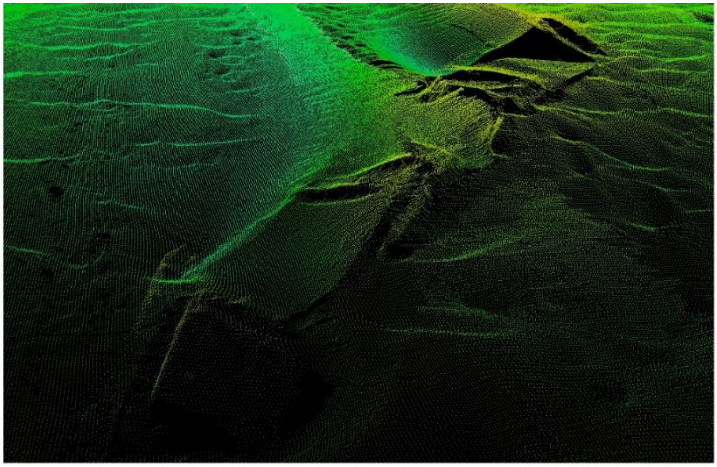


Fig. 3: Three-dimensional image of a navigational hazard – a sand-covered shipwreck

1.3 Sub-Bottom Profilers (SBP)

These systems use low-frequency sound (0.5 – 12 kHz) that penetrates beneath the seabed surface to determine the type and thickness of geological sediment layers. This information is crucial for engineering activities (construction of ports and offshore platforms) as well as for emergency vessel anchoring. [1], [4], [6]

2. Airborne Laser Bathymetry System (ALB)

For shallow waters, rocky coasts, and areas that are difficult for vessels to access, acoustic systems lose effectiveness. Under these conditions, Airborne Laser Bathymetry (ALB / Bathymetric LiDAR) has become the standard. [3], [7]

2.1 Dual-Frequency Emission Principle

The system uses two types of laser beams:

Infrared Laser (1064 nm): Reflected directly from the water surface to determine the water boundary (where the water starts).

Green Laser (532 nm): Penetrates the water surface, reaches the seabed, and is reflected back to the receiver.

The travel time difference between the two pulses, recalculated based on the refractive index of light in water, yields the exact depth (Fig. 4).

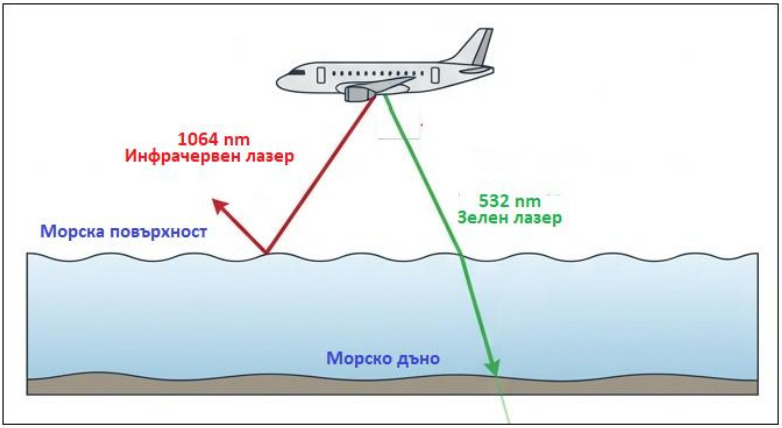


Fig. 4: Principle of airborne laser surveying

2.2 Limitations

The penetration depth of the green laser beam depends on water clarity and typically reaches up to 50 meters in clear waters. New technologies utilize topo-bathymetric LiDAR systems with low pulse energy and high repetition rates mounted on Unmanned Aerial Vehicles (UAVs).

3. Navigational Support and Positioning

Every bathymetric depth measurement is useless without precise positioning. A modern hydrographic system relies on integrated positioning and orientation systems.

3.1 Global Navigation Satellite Systems (GNSS)

GNSS receivers operating in real-time kinematic phase measurement modes (RTK) or post-processing modes (PPK / PPP - Precise Point Positioning) are used. They provide horizontal (x, y) and vertical (h) positioning accuracy within 1–3 cm.

3.2 Inertial Navigation Systems

A marine vessel is subject to continuous wave action and motion. To compensate for these movements, echo sounders are integrated with Inertial Measurement Units (IMUs) containing gyroscopes and accelerometers. They measure oscillations in Roll, Pitch, and Heading at high frequencies (100–500 Hz).

The integration of GNSS + INS via Extended Kalman Filters ensures precise spatial orientation of the acoustic beam with angular errors below 0.01°. [8], [9], [10], [11]

4. Autonomous Systems

Classic hydrographic ships are expensive to operate and have limited maneuverability in shallow or navigationally hazardous waters. This leads to the deployment of autonomous systems. [3], [6]

4.1 Unmanned Surface Vehicles (USV)

USVs are remotely controlled or fully autonomous boats/catamarans equipped with miniaturized MBES, GNSS/INS systems, and communication modules (Fig. 5).



Fig. 5: Unmanned Surface Vehicle (USV)

Advantages: Extremely low operating costs, ability to work in shallow waters (down to 0.5 m), environmentally friendly (frequently electrically powered).

Application: Mapping reservoirs, riverbeds, and port basins.

4.2 Autonomous Underwater Vehicles (AUV)

AUVs are self-propelled underwater robots carrying out pre-programmed missions at great depths.

Advantages: They descend close to the seabed (10–20 m above it), eliminating acoustic scattering in the water column.

Application: Deep-water surveys down to depths of 6,000 m, object detection, and underwater infrastructure inspection.

5. Software Processing, Modeling, and Quality Control

The hydrographic survey process does not end with seabed data acquisition. Processing raw data requires specialized software. The ultimate goal of hydrographic data processing is the generation of precise 3D Digital Terrain Models (DTM) used for cartography, geology, and engineering projects. [12]

The data processing phases are as follows:

Geometric and Physical Correction: Adjustments for water level fluctuations due to tides, refraction corrections, and compensation for vessel movement.

Noise Filtering: Removal of false reflections caused by interference, fish shoals, or water aeration/bubbles. The CUBE algorithm (Combined Uncertainty and Bathymetry Estimator) is widely applied for this purpose.

Data Classification and AI: Implementation of machine learning algorithms for automatic detection of underwater objects and automated segmentation of seabed sediment types based on acoustic backscatter.

Output Products: Digital Terrain Models (DTM / DEM) featuring high-resolution grids with cell sizes ranging from 0.1 m to several meters; Electronic Navigational Charts (ENC) created in compliance with IHO S-57 and S-100 standards; 3D point clouds and isobaths for engineering design and dredging operations.

6. Comparative Analysis of Hydrographic Systems and Technologies

The table summarizes the main technical and operational characteristics of the reviewed technologies:

Technology	Applicable Depth Range	Horizontal / Vertical Accuracy	Main Advantages	Limitations
Multibeam Echo Sounder (MBES)	0.5 m – 11,000 m	High (up to 1–5 cm in shallow water)	100% coverage, high data density	High costs for vessel and equipment
Side Scan Sonar (SSS)	1 m – 2,000 m	High for details (acoustic image)	Exceptional seabed relief detail	Does not yield direct bathymetric depth (relief only)
Bathymetric LiDAR (ALB)	0 m – 40 m (depends on clarity)	Medium to high (~15 cm)	Rapidly covers shallow areas	Limited by water clarity
Unmanned Surface Vehicles (USV)	0.2 m – 200 m	Depends on mounted sensor (MBES/SBES)	Access to shallow waters, low operating costs	Limited battery/fuel range
Autonomous Underwater Vehicles (AUV)	10 m – 6,000 m	Extremely high on deep-water targets	Independent of depth	High cost, complex underwater navigation

Conclusion

Modern hydrographic surveys have entered an era of digitalization and full automation. The integration of multibeam acoustic systems, airborne laser bathymetric scanners, high-precision satellite navigation, and inertial sensors allows for seabed mapping at a level of detail that was impossible two decades ago. The future of hydrography is bound to:

Widespread deployment of swarms of autonomous platforms (USVs/AUVs) for parallel surveying over large water areas.

Implementation of new data standards (IHO S-100) allowing dynamic, real-time integration of bathymetry, tides, and navigation.

Artificial Intelligence and cloud processing for immediate processing of collected datasets directly on board the vehicle.

These innovations not only improve navigation safety but also represent a key factor in the sustainable development and management of the World Ocean and inland waterways.

References

1. Белчев Б., Няголова З., Английски международни и адмиралтейски карти, изд. "Стено", Варна, 1997.
2. Дачев Ю., Хидрографски системи, използвани за заснемане н релефа на дъното на българското черноморско крайбрежие, Списание „Геодезия, картография, земеустройство", бр. 3-4, стр. 9-13, София, 2017, ISSN 0324-1610.
3. Стойков Е., Технически средства и системи при извършване на хидрографски измервания, ШУ, Шумен, 2019.
4. Коломийчук Н. Д., Гидрография, изд. МО, Москва, 1975.
5. Tanev, G. (2025). Surveying and maintenance of the primary-class points of the state GPS network of the Republic of Bulgaria. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2025", Faculty of Artillery, Air Defense and CIS, NMU, Shumen, pp. 1038–1042, ISSN 2815-4282.
6. Tanev, G. (2024). Maintenance of the Magnetic Station Network and Determination of Geomagnetic Field Elements in Northern Bulgaria. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2024", Faculty of Artillery, Air Defense and CIS, NMU, Shumen, pp. 562–574, ISSN 2815-4282.
7. IHO, Manual on Hydrography, Publication C-13, Monaco, 2011.
8. IHO Special Publication S-44, "IHO Standards for Hydrographic Surveys", Monaco, 2020
9. IHO Special Publication S-52, "Spécifications for Chart Content and Display Aspects of ECDIS", Monaco.
10. IHO Special Publication S-57, "IHO Transfer Standards for Digital Hydrographic Data", Monaco, 2005.
11. IHO Special Publication S-61, "Product Specification for Raster Navigational Charts", Monaco, 2011,
12. Symbols and abbreviations used on admiralty charts-NP 5011 (INT), Hydrographic office, London, United Kingdom, 2025.

THE LIGHTHOUSES AND AIDS TO NAVIGATION SYSTEM ALONG THE BULGARIAN BLACK SEA COAST: HISTORY, CURRENT STATUS, CHALLENGES, AND FUTURE DEVELOPMENT

Aleksandra P. Zidarova, Aylin N. Dzhom

Faculty „Artillery, Air Defense u CIS", National Military University "Vasil Levski", Shumen City, BulgariaE-mail: ali.zidarova@gmail.com, djomaylin@gmail.com

Abstract: This report presents a comprehensive analysis of the aids to navigation (AtoN) system along the Bulgarian Black Sea coast, focusing on lighthouses as critical elements of maritime safety infrastructure. It traces the historical evolution of coastal lighting facilities—from ancient beacon fires and Ottoman-era structures built by the French Lighthouse Company (Compagnie des Phares) to the state-managed modern network maintained by the Bulgarian Navy's Hydrographic Service and the Bulgarian Ports Infrastructure Company. The report classifies the coastal, island, and harbor lighthouses, detailing their technical characteristics, including light rhythms, focal height, range in nautical miles, and optical systems. Furthermore, it examines current maintenance procedures in aggressive marine environments, alongside physical risks such as coastal erosion and landslides (e.g., Cape Galata). The study highlights the strategic importance of traditional lighthouses as indispensable visual backups to modern satellite navigation (GPS/GNSS) and ECDIS systems. Finally, key recommendations for modernization are proposed, emphasizing full transition to LED matrices, autonomous solar-hybrid power systems, IoT remote monitoring, integration with AIS-AtoN digital broadcasting, and the potential for preserving these facilities as cultural maritime heritage.

Keywords: *Lighthouses, Aids to Navigation (AtoN), Bulgarian Black Sea Coast, Maritime Safety, Hydrography, Modernization, AIS.*

Introduction:

Navigation lighting systems along the Black Sea coast have been vital for maritime safety for centuries. Despite the advent of modern technologies such as satellite navigation (GPS) and electronic charts, lighthouses remain an indispensable visual aid for vessels, particularly during adverse weather conditions, maneuvering near the coast, and entering harbors.

The Bulgarian Black Sea coastline is characterized by a specific topography, shallows, reefs, and dynamic weather patterns, making a reliable lighthouse system critical for maritime transport and trade.

The primary objective of this report is to conduct a comprehensive analysis of the aids to navigation system along the Bulgarian Black Sea coast, examining its historical development, current technical status, maintenance procedures, and opportunities for future modernization.

To achieve this goal, the report sets the following tasks:

- To clarify the main functions and types of lighthouses according to their purpose and location.
- To trace the chronological development and construction of lighthouse facilities along the Bulgarian coast from Antiquity to the present day.

- To analyze the technical characteristics, power sources, and specific maintenance requirements in an aggressive marine environment.
- To identify key challenges facing the facilities (wear and tear, erosion, landslide processes).
- To propose concrete measures for technological enhancement through the implementation of innovations (LED modules, solar power, digital lighthouses, and IoT monitoring).

1. What is a Lighthouse and Its Purpose (Function and Application)

1.1 Definition and Essence

A lighthouse is a specially constructed navigational facility (most commonly a tower or tall structure) equipped with a powerful light source and an optical system. It is positioned at key geographical points—capes, islands, hazardous reefs, or at the entrances of ports and breakwaters.

The main purpose of a lighthouse is to provide visual orientation for vessels at night, during restricted visibility (fog, rain, storms), or under challenging weather conditions.

1.2 Main Functions of Lighthouses

In modern hydrography and navigation, lighthouses perform several critical tasks:

- **Warning against Hazards (Warning Function):** They signal the presence of shallows, submerged rocks, reefs, or dangerous coastal sections, preventing ships from running aground or shipwrecking.
- **Coastal Orientation and Positioning (Orientation Function):** Coastal lighthouses assist mariners in identifying the coastline and confirming their exact position by providing a physical, verifiable landmark.
- **Guidance along Safe Fairways (Harbor and Leading Function):**
  - **Port (Entrance) Lighthouses:** Mark the entrance to the harbor and protective structures (breakwaters, moles).
  - **Sector and Leading (Range) Lights:** Use colored light sectors (red, green, white) to indicate to captains whether they are within the safe axis of the channel (fairway) or deviating from it.
- **Redundancy and Backup Function:** In the era of satellite navigation (GPS/GNSS) and electronic charts (ECDIS), lighthouses serve as an absolutely necessary independent backup in the event of a cyberattack, signal jamming, or technical failure of onboard electronics.

1.3 Radio and Acoustic Signaling

To remain effective even when optical visibility is reduced to zero (e.g., in dense fog), modern lighthouse complexes are often equipped with additional systems:

- **Acoustic Systems (Fognorns/Nautophones):** Emit powerful sound signals at specific frequencies and rhythms to transmit warning signals over short distances.

- **Radiobeacons and Radar Beacons (RACON):** Broadcast a radio signal that appears directly on ship radar displays as a specific Morse code letter, confirming the position of the lighthouse.

2. A Brief History of Lighthouses along the Bulgarian Black Sea Coast

The historical evolution of navigational support along the Bulgarian Black Sea coast reflects the region's rich commercial and military history, progressing through several key stages:

2.1 Antiquity and the Middle Ages: The First Light Signals

The Black Sea has been an active maritime hub since the times of the ancient Greeks and Romans. The precursors of lighthouses on today's Bulgarian coast were open bonfires lit on high capes and rocks near ancient colonies such as Apollonia (Sozopol), Mesembria (Nessebar), Odessos (Varna), and Dionysopolis (Balchik). During the medieval period, signal fires were maintained primarily by local populations or merchant guilds to facilitate trading vessels.

2.2 Ottoman Period and the French Lighthouse Company (19th Century)

The organized construction of modern lighthouses began in the second half of the 19th century. Following the Crimean War (1853–1856) and increasing maritime traffic, the Ottoman Empire signed a contract with the French firm *Compagnie des Phares des Empires Ottomans* (French Lighthouse Company).

The company constructed and maintained the first classical lighthouses along the western Black Sea coast:

- **Shabla Lighthouse (1856):** The oldest and tallest preserved lighthouse on the Bulgarian coast, put into operation in its current form during this period.
- **Kaliakra, Emine, and Galata Lighthouses:** The initial structures on these key capes were also erected by French engineers using petroleum lamps and lenses advanced for their time.

2.3 Establishment of the Bulgarian Lighthouse Network (1878 – mid-20th Century)

Following the Liberation of Bulgaria (1878), a gradual process of buyout and transfer of lighthouse management to the Bulgarian state began, fully finalized in the early 20th century.

- **Nationalization and Modernization:** Under the leadership of Bulgarian military and civilian engineers, the old Ottoman and French equipment began to be replaced.
- **New Towers and Facilities:** The lighthouses at Cape Emine, Cape Galata, and Cape Kaliakra were rebuilt or underwent major reconstruction, alongside the island lighthouses on Saint Ivan Island (near Sozopol) and Saint Anastasia Island (in the Gulf of Burgas).
- **Harbor Lighthouses:** With the construction and expansion of modern ports in Varna and Burgas in the early 20th century, the first entrance harbor lights and breakwater lights were installed.

2.4 Socialist Period: Electrification and Automation

During the second half of the 20th century, the management of navigational equipment transitioned entirely to the Hydrographic Service of the Bulgarian Navy. Major achievements during this phase included:

- **Full Electrification:** Transition from gas and petroleum mechanisms to grid electric power and backup diesel generators.
- **Implementation of Radiobeacons and Foghorns:** Addition of acoustic and radar signaling equipment for navigation in fog.
- **Automation:** Reduction of the need for permanent lighthouse personnel on smaller structures.

3. Classification and Technical Characteristics of Lighthouses on the Bulgarian Black Sea Coast

Navigational light structures along the Bulgarian coast are categorized based on their location, functional purpose, and the technologies used.

3.1 Classification of Lighthouses

By Location and Function:

- **Coastal Lighthouses for Long-Range Navigation (Landfalls):** Situated on key, elevated capes along the coast. Their purpose is to provide orientation for ships passing in open waters at a considerable distance from the shore.
  - *Examples:* Shabla Lighthouse, Kaliakra Lighthouse, Emine Lighthouse, Galata Lighthouse, Maslen Nos Lighthouse.
- **Island Lighthouses:** Constructed on islands near the coast. They warn of landmasses, shallows, and submerged rocks around the island.
  - Examples: Lighthouse on Saint Ivan Island (near Sozopol), Lighthouse on Saint Anastasia Island (in the Gulf of Burgas).
- **Harbor (Port) and Breakwater Lighthouses:** Located at port entrances, breakwater heads, or moles. They serve for safe orientation and maneuvering during entry into and exit from port waters.
  - Examples: Lighthouses on the breakwaters in Varna, Burgas, Balchik, Sozopol, Tsarevo, and Ahtopol.
- **Leading (Range) Lights:** A pair of lighthouses positioned one behind the other at different heights, forming an imaginary line (channel axis). When a mariner aligns both lights vertically, it indicates the vessel is on the correct and safe course in a narrow channel.

3.2 Key Technical Characteristics

To fulfill its role, each lighthouse possesses a unique technical passport, including the following parameters:

- **Light Characteristic (Rhythm and Color):** Each lighthouse emits light in a precise pattern so it can be easily identified at night without confusion with adjacent lights or shore lighting.

- **Color:** White, red, and green lights are primarily used. White light is used mainly for long-range navigation due to its high atmospheric penetration, while red and green indicate port and starboard sides of a fairway entrance.
- **Rhythm (Character):** Expressed through alternating flashes and eclipses with precisely measured durations in seconds (e.g., "flashing white light every 5 seconds").

➢ Height **of Tower and Focal Plane:**

- **Structure Height:** Physical height of the object from base to top.
- **Focal Plane Height:** Height of the light source relative to mean sea level, critical for calculating geographical range.

➢ **Geographical and Optical Range (Visibility):** Measured in **nautical miles (NM)**. Depends on the focal plane height (due to Earth's curvature) and the intensity of the light source.

- Note: Shabla Lighthouse has a geographical range of 17 nautical miles, while Kaliakra Lighthouse reaches approximately 19 nautical miles.

➢ **Optical Systems:**

- **Fresnel Lenses:** Historically significant and highly efficient glass lenses that concentrate scattered light into a tight, powerful horizontal beam.
- **Modern LED Modules:** Compact, high-efficiency light-emitting diodes that are gradually replacing traditional lamps.

3.3. Power Sources and Electricity Supply

Technological advancements have transformed how lighthouses are powered:

➢ **Primary Supply:** Most coastal and port lighthouses are connected to the national electrical grid.

➢ **Emergency Supply (Backup Systems):** In the event of a power outage, diesel generators or storage batteries are automatically activated.

➢ **Autonomous Renewable Systems:** Isolated lighthouses (island or breakwater structures) are increasingly equipped with photovoltaic (solar) panels and lithium battery banks, making them fully self-sufficient and eco-friendly.

➢

4. Maintenance and Current Management of Lighthouses on the Bulgarian Black Sea Coast

Maintaining lighthouse facilities in full operational order is a critical process requiring continuous monitoring, technical service, and coordination between state institutions.

4.1 Institutional Framework and Responsibility

The management of the aids to navigation system along the Bulgarian coast is divided between two main entities:

➢ **Hydrographic Service of the Bulgarian Navy:** Responsible for coastal and island lighthouses of military and strategic national importance (e.g., Shabla,

Kaliakra, Emine, Saint Ivan Island). The service also maintains and publishes official nautical charts and Notices to Mariners.

- **Bulgarian Ports Infrastructure Company (BPI Co.):** Manages and maintains entrance and harbor lights located on breakwaters and within public port waters (Varna, Burgas, etc.).

4.2 Routine Technical Maintenance Activities

Maintenance is categorized into scheduled (preventive) and unscheduled (emergency):

- **Optical and Light Systems:** Regular inspection of LED modules or traditional halogen lamps, focal alignment, rotation mechanisms on revolving lights, and cleaning of optical lenses.
- **Power Systems:** Servicing of emergency diesel generators, battery banks, charge controllers, and solar panels on autonomous installations.
- **Structural and Civil Maintenance:** Due to exposure to aggressive marine conditions, towers require periodic rust removal, application of protective anti-corrosion coatings, repainting of daymarks for daytime visibility, and waterproofing.

4.3 Key Maintenance Challenges

Management of Bulgarian Black Sea lighthouses faces specific difficulties:

- **Aggressive Marine Environment:** Salt air, high humidity, strong winds, and winter icing rapidly degrade metal structures and electrical connections.
- **Geological Risks and Landslides:** Several coastal lighthouses are built on cliffs prone to abrasion and landslides. A prominent example is the **Cape Galata** area, where historical landslides threatened lighthouse infrastructure, requiring relocation. [11]
- **Coastal Erosion:** Continuous wave action undermines the base of rocky capes (e.g., Kaliakra and Emine), necessitating coastal defense engineering to preserve the towers. [12]
- **Logistical Access:** Certain lighthouses (island structures on St. Ivan and St. Anastasia, or remote capes) are difficult to access during heavy seas, hindering rapid emergency response. [10], [14]

5. Improvement of Lighthouses on the Bulgarian Black Sea Coast (Recommendations and Modernization)

To ensure maximum navigation safety while simultaneously optimizing long-term operational and maintenance costs, the aids to navigation (AtoN) system along the Bulgarian Black Sea coast requires a phased, comprehensive modernization. While the historical and physical infrastructure of lighthouses remains fundamental, relying solely on traditional visual techniques is no longer sufficient for modern maritime demands.

The strategy for improvement must focus on structural modernization through digital integration, smart telemetry, and energy-efficient technologies. Transitioning from

reactive maintenance to automated, sensor-driven oversight will significantly reduce human intervention in remote locations, minimize power consumption, and eliminate single points of failure. Furthermore, synchronizing physical lighthouses with digital broadcasting standards directly bridges the gap between classic visual seamanship and modern electronic navigation (e-Navigation) networks.

5.1 Technological Upgrades and Energy Efficiency

- **Full Transition to LED Arrays:** Conventional halogen and incandescent lamps should be replaced with modern LED modules, offering lower energy consumption, extended operational lifespans (exceeding 50,000 hours), and high vibration resistance.
- **Autonomous Hybrid Energy Systems:** Equipping all coastal and port lighthouses with standalone photovoltaic systems and high-grade lithium-iron-phosphate ($LiFePO_4$) batteries to ensure 100% autonomy during grid power failures.

5.2 Digitalization and System Integration

- **Implementation of Digital / Virtual Lighthouses (AIS-AtoN):** Integrating lighthouse structures with the Automatic Identification System (AIS). Installing AIS AtoN transmitters allows real-time position, operational status, and navigational data to be broadcast directly onto ship ECDIS displays and radar screens. [14]
- **IoT (Internet of Things) Remote Monitoring:** Installing smart sensors to enable remote telemetry tracking:
    - Light source operational status.
    - Battery state of charge.
    - Detection of unauthorized entry or physical damage.
    - Ambient temperature and humidity within equipment housing.

5.3 Infrastructure Resilience and Coastal Protection

- **Landslide and Erosion Monitoring:** Establishing permanent geodetic and sensor monitoring networks to track rock mass movement around threatened lighthouses (e.g., Cape Galata and Cape Emine). [11], [12], [13]
- **Coastal Defense Engineering:** Timely reinforcement of cliff foundations and construction of protective breakwaters/groynes to mitigate wave abrasion. [13]

5.4 Socialization, Cultural Preservation, and Tourism

- **Transformation into Cultural Heritage Sites:** Facilities with high historical value (such as Shabla and Kaliakra lighthouses) can be socialized by:
    - Establishing maritime heritage museums or visitor centers.
    - Organizing scheduled "Open Days" (in coordination with the Navy).
    - Integrating facilities into official regional cultural and tourism routes without compromising their operational navigational duties.

Conclusions:

Lighthouses along the Bulgarian Black Sea coast are not merely historical landmarks and symbols of maritime heritage, but vital components of national critical infrastructure for navigation safety. From ancient coastal bonfires to modern optical installations, their core objective remains unchanged: safeguarding human life at sea and ensuring the unhindered passage of vessels.

Despite rapid advancements in satellite technology, GPS navigation, and electronic charts, lighthouse complexes remain an indispensable, independent visual backup. They represent the final line of defense during technical system failures, cyber incidents, signal jamming, or severe weather conditions.

This analysis indicates that a sustainable future for the lighthouse network depends on a balanced approach. On one hand, digitalization and technological modernization—such as LED adoption, solar autonomy, IoT telemetry, and AIS-AtoN systems—are required. On the other hand, addressing natural threats like landslides and coastal erosion is crucial to preserving the physical structures.

Combining modernized functionality with the preservation of unique architectural and historical value will ensure that the lights along the Bulgarian coast continue to serve mariners reliably throughout the 21st century.

References:

1. Архив на Военноморския музей – Варна. (1944). Документи за изграждането и модернизацията на брегoвите фарове (Фонд на Хидрографското отделение 1879–1944 г.). Варна: Военноморски музей.
2. Дачев Ю., Димитракиев Д., Медникаров Б., & Димитракиева С. (2022). Българско черноморско крайбрежие: Морски пространства, населени места, морски планове, фарове и светещи знаци, несветещи знаци, заливи и бухти, носове, створове, ориентири, плажове, реки (2-ро изд.). Варна: ВВМУ „Н. Й. Вапцаров".
3. Димитров Б. (2012). Морската история на България и корабоплаването по западното Черноморие. София: Захарий Стоянов.
4. Държавно предприятие „Пристанищна инфраструктура". (2021). Годишен доклад за състоянието на навигационното оборудване и AtoN системите в публичните пристанища. София: ДППИ.
5. Панайотов И., & Колев В. (2008). Хидрографско осигуряване на корабоплаването в българските акватории. Варна: ВВМУ „Н. Й. Вапцаров".
6. Станев А. (2015). История на навигационните съоръжения по Българското Черноморие (1856–2010). Варна: Морски преглед.
7. Хидрографска служба на ВМС. (2022). Официален списък на светлините и навигационните знаци по Българското Черноморско крайбрежие. Варна: Военноморски сили на Република България.
8. Compagnie des Phares des Empires Ottomans. (1892). State of lighthouses and marine lights along the Black Sea coast. Paris: Imprimerie Nationale.

9. IALA. (2018). Navguide: Aids to navigation manual (8th ed.). Saint-Germain-en-Laye: International Association of Marine Aids to Navigation and Lighthouse Authorities.
10. Tanev, G. (2024). Maintenance of the Magnetic Station Network and Determination of Geomagnetic Field Elements in Northern Bulgaria. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2024", Faculty of Artillery, Air Defense and CIS, NMU, Shumen, pp. 562–574, ISSN 2815-4282.
11. Tanev, T. (2024). Inspection and Construction of Points from the State Geodetic Network in Southern Bulgaria. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2024", Faculty of Artillery, Air Defense and CIS, NMU, Shumen, pp. 575–580, ISSN 2815-4282.
12. Tanev, T., & Tanev, G. (2023). Establishment of Ground Control Points for Photogrammetric Surveying for Mapping the Northern Slopes of the Balkan Mountains. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2023", NMU, Shumen, pp. 679–684, ISSN 2367-7902.
13. Tanev, T. (2025). Higrigraphyc measurements in the Bulgarian section of the Danube River. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2025", Faculty of Artillery, Air Defense and CIS, NMU, Shumen, pp. 1030–1037, ISSN 2815-4282.
14. Tanev, G. (2025). Surveying and maintenance of the primary-class points of the state GPS network of the Republic of Bulgaria. Proceedings of International Scientific Conference "Defense Technologies – DefTech 2025", Faculty of Artillery, Air Defense and CIS, NMU, Shumen, pp. 1038–1042, ISSN 2815-4282.