“VASIL LEVSKI” NATIONAL MILITARY UNIVERSITY

“ARTILLERY, AIRCRAFT DEFENSE AND CIS” FACULTY

INTERNATIONAL SCIENTIFIC CONFERENCE “DEFENSE TECHNOLOGIES” 2022

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

SOCIAL STUDIES

GEODESY

Shumen, Bulgaria
2022

TO THE READERS

This collection is divided in three parts and includes science papers presented on the International Scientific Conference "DEFENSE TECHNOLOGY FORUM 2022" 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. G.KALEV, *Ph.D., NMU*
Col. Eng. Assoc. Prof. A. L. ATANASOV, Ph.D, NMU
Colonel Eng. Assoc. Prof. V. GANEV, Ph.D., NMU
LTC Eng. Assoc. Prof. M. LAMBEVA, Ph.D., NMU
Col. Eng. Assoc. Prof. C. CONEV, Ph.D., NMU
LTC Eng. S. I. ANTONOV, Ph.D., NMU
Assoc. Prof. PhD. R. BOGDANOV, Ph.D., NMU
Lt.col.Eng. A.C. SAVA, PhD., MTA"Ferdinand I", Romania
Col. Assoc.Prof. Eng. M. LUPOAE, Ph.D., MTA "Ferdinand I", Romania
Prof. D.sc.ing E. TEIRUMNIEKS, Faculty of Engineering, RTA Latvia
Prof. D.sc.ing. A. TEILANS, Faculty of Engineering, RTA, Latvia
Dr I. RAGIES, Hellenic Army Academy, Greece
Dr N. KARADIMAS, Hellenic Army Academy, Greece
Dr M. ARTAVANIS, Hellenic Army Academy, Greece
Dr S. SOFIOU, Hellenic Army Academy, Greece
Col. Assoc. Prof. V. SANDRU, Ph.D., Vice-Rector for research of Air Force Academy, Romania
Maj. L. GĂINĂ, "Henri Coanda" AFA
Assoc. Prof. C. CARSTEA, Ph.D., "Henry Coanda" AFA
Assoc.Prof., Ph.D. C. STRIMBU, "Henry Coanda" AFA
Assoc. Prof., Ph.D. G. CONSTANTINESCU, "Henry Coanda" AFA
LTC Assoc. Prof. Eng. B. BIERNACIK, Ph.D., WSU, Poland
LTCol. P. OSTOLSKI, Adiunkt, PhD Eng., WSU, Poland
Maj. W. MATERAK, War Studies University, Poland
LTCol. R. ZAJKOWSKI, Adiunkt, PhD Eng., WSU, Poland
LTCol. Z. LEŚNIEWSKI, Adiunkt, PhD Eng, WSU, Poland
Col. Assistant Professor doc. dr. sc. S. DOMJANČIĆ, Croatian Defence Academy „Dr. Franjo Tuđman"
Assoc. Prof. Ts. KARADZHOV, Ph.D, Technical University Gabrovo, Bulgaria
Dr. D. DUMITRU, "Spiru Haret" University, Romania
Associate Prof. Dr. R. IOAN, "Spiru Haret" University, Romania
Associate Prof. Dr. D. A. GÂRDAN, „Spiru Haret" University, Romania
R. WOŹNIAK, DSc. MUT Prof., Military University of Technology
J. JANISZEWSKI, DSc. MUT Prof., Military University of Technology
Col. A. KOZAKIEWICZ, DSc. MUT Prof., MUT
PhD. P. BERNAT, Polish Air Force University
Cpt. PhD D. MICHALSKI, Polish Air Force University
Lt. Col. D. FARAZOV, Ph.D., "G.S. Rakovski" National Defence College
Prof. Dr. Andrej STEFANOV, Faculty of Engineering, International Balkan University, Skopje, North Macedonia
Asst. Prof. Dr. Ervin DOMAZET, Faculty of Engineering, International Balkan University, Skopje, North Macedonia

© "Vasil Levski" National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, 2022.
c/o Jusautor, Shumen
ISSN 2367-7902

CONTENTS

PLENARY SESSION 9

TECHNICAL READINESS TO START NATIONAL SECURITY MANAGEMENT SYSTEM AS A REALIZATION OF STRATEGIC GOAL OF REPUBLIC OF POLAND WITH A USE OF JASMINE CRISIS MANAGEMENT SYSTEM
Bartosz Biernacik 10

CYBER THREAT INTELLIGENCE AND PREVENTION-BASED INCIDENT RESPONSE TO REAL-WORLD CYBER ATTACKS
Mihailescu Marius Iulian, Dumitru Dan 24

MACHINE LEARNING IN THE CONTEXT OF CYBERSECURITY
Stefania L. Nita 32

ACHIEVED RESULTS FROM PROJECTS UNDER ERASMUS+ KEYACTION 02
Dilyan I. Dimitrov, Linko G. Nikolov, Krasimir Slavianov, Miroslav G. Nedelchev 38

DEFENSE AND SECURITY 50

COLLECTING INFORMATION DURING THE RECONNAISSANCE INTO THE COMMAND SUPPORT SYSTEMS USING MODERN TECHNOLOGIES- EXPERIENCE FROM UKRAINIAN CONFLICT
Tomasz Surwiłło 51

CURRENT ASPECTS OF ALLIED INSTRUMENTS FOR INNOVATION
Maxim M. Alashki 63

THE POWERS
Maxim M. Alashki 69

BASIS OF ANTI-CRISIS MANAGEMENT OF THE STATE ADMINISTRATION
Dimo V. Ginev 76

COMPONENTS AND CAPABILITIES OF THE NATIONAL ANTI-CRISIS MANAGEMENT SYSTEM
Dimo V. Ginev 83

MODERN CONCEPTS OF CONDUCTING A NAVAL LANDING OPERATION
Krasimir Kostadinov 91

PARTICIPATION OF NAVAL SURVEILLANCE AND COMMUNICATION (SAC) UNITS IN MARITIME INTERDICTION OPERATION
Zhivko St. Yordanov 97

DEFENSE PLANNING MODEL
Ivo G. Radulov 102

COMPARATIVE ANALYSIS OF THE REMOTELY PILOTED AIRCRAFT SYSTEMS USED IN THE RUSSIA-UKRAINE WAR
Ivaylo Zh. Bozov 113

REMOTELY PILOTED AIRCRAFT SYSTEMS (RPAS) IN SERVICE TO ARTILLERY FORMATIONS
Ivaylo Zh. Bozov 118

CONTEMPORARY EDUCATIONAL TECHNIQUES: GAMIFICATION
Ivelin G. Katsev 122

ANALISYS OF ARTILLERY FIRE'S EFFECTIVENESS AGAINST UNITARY TARGETS: COMPARING CONTEMPORARY CONVENTIONAL PROJECTILES VERSUS PRECISION GUIDED PROJECTILES
Ivelin G. Katsev 127

ORIGIN AND DEVELOPMENT OF PSYCHOLOGICAL OPERATIONS FROM ANCIENT TIMES TO THE PRESENT DAYS
Veliko P. Petrov 133

HISTORY AND REASONS FOR THE EMERGENCE OF THE PUBLIC DIPLOMACY
Veliko P. Petrov, Stancho G. Stanchev 143

FOOD CRISES IN THE WORLD
Veliko P. Petrov, Kaloyan A. Iliev 150

ONE OPTION FOR DETERMINING THE EFFECTIVENESS OF ANTI-TANK MEASURES AGAINST ARMORED TARGETS
Atanas Stavrev Atanasov 157

SOME CONCLUSIONS ABOUT THE USE OF ARTILLERY IN THE UKRAINIAN CONFLICT
Atanas Stavrev Atanasov 164

COMBAT AERIAL VEHICLE DEPLOYMENT IN SIXTH GENERATION WARFARE
Stoyan N. Chanev 169

HYPERSONIC COMBAT AERIAL VEHICLES
Stoyan N. Chanev 178

INTERCONTINENTAL BALLISTIC MISSILE COUNTERFORCE AGAINST BALLISTIC MISSILE DEFENSE SYSTEMS
Stoyan N. Chanev 186

METHOD FOR HAZARD ANALYSIS IN INDUSTRIAL ACCIDENTS
Hristo A. Desev 196

THE MILITARY LEADER – FACTORS AND CONDITIONS FOR FORMATION
Stancho G. Stanchev, Veliko P. Petrov 201

TOOLS AND METHODS IN THE OPERATION PLANNING PROCESS
Danko D. Farazov 207

OPERATIONS DESIGN
Danko D. Farazov 211

IMPERATIVES IN THE DECISION-MAKING PROCESS
Danko D. Farazov 216

CIVIL-MILITARY COOPERATION IS A MAJOR FACTOR IN MODERN MILITARY CONFLICTS
Kaloyan A. Iliev, Veliko P. Petrov 220

DEFINITIONS FOR INFORMATION OPERATIONS, COGNITIVE WARFARE, AND RELATED TERMS
Dobril A. Radoslavov 225

WEAPONS, TECHNOLOGIES, LOGISTICS 230

BURNING CHARACTERIZATION OF HETEROGENEOUS PROPELLANT AT HIGH PRESSURES
Florin-Marian Dîrloman, Traian Rotariu, Adrian-Nicolae Rotariu, Gabriel-Flavius Noja, Mihai-Ionuţ Ungureanu, Daniel-Neculai Zvîncu, Alexandra-Ioana Dan 231

ASSESMENT OF A NEW THERMOMARIC SOLID COMPOSITION USED IN EFP-TB TANDEM AMMUNITION
Liviu C. Matache, Andrada M. Runceanu, Adrian N. Rotariu, Florin M. Dirloman, Răzvan M. Mircioagă, Cristian Moldoveanu, Pamfil Şomoiag 238

THE CONCEPTION OF A NON-STANDARDIZED TEST FOR ASSESSING THE EFFICIENCY OF THE INNER LAYER OF THE BALLISTIC HELMETS
Rotariu Adrian-Nicolae, Cirmaci-Matei Marius-Valeriu, Bucur Florina, Matache Liviu, Pulpea Bogdan, Florin Dirloman, Adrian Malciu, Sava Alin 246

THEORETICAL ASSESMENT OF OPTIMAL MULTIPLE ROCKETS LAUNCHING FOR LAROM PLATFORM
Neculai-Daniel Zvîncu, Pamfil Şomoiag, Cristian-Emil Moldoveanu, Florin-Marian Dîrloman, Costin-Dumitru Berechet 252

PERSONNEL BALLISTIC PROTECTION USING COMPOSITE MATERIALS
Diana-Carmen Dumitraş 260

RESEARCH ON THE AIRCRAFTS AND DRONES WAKE VORTICES AND THEIR EFFECT ON THE FLIGHT SECURITY
Camille Yaker, Arthur Tijou, Laure Velasco, Thomas Flourou, Cristian-Emil Moldoveanu, Constantin Enache, Alin-Constantin Sava, Răzvan Mircioagă 267

PARTICULATIRIES REGARDING THE UPGRADING OF AVIATION BOMBS INTO LASER-GUIDED BOMBS
Alin-Constantin Sava, Vasile Nuţu, Cristian-Emil Moldoveanu, Constantin Enache, Pamfil Şomoiag 274

RESPONSE SURFACE OPTIMIZATION, BASED ON CONTACT STATIC STRUCTURAL ANALYSIS OF NON-PNEUMATIC WHEELS WITH FOUR TYPES OF SPOKES IN THE ENVIRONMENT OF ANSYS WORKBENCH
Genadiy Y. Hinkov 278

APPLYING OPTIMIZATION METHODS IN LOGISTICS
Andrey I. Bogdanov, Vanko V. Ganev 287

ARTILLERY BLASTERS
Ivelina Angelska 293

POSSIBILITIES FOR REPLACEMENT OF THE THERMOSET PHENOLFORMALDEGYDE USED IN THE MANUFACTURE OF PRODUCTS FOR THE BULGARIAN ARMY WITH THERMOPLASTIC EQUIVALENTS
Blagovest I. Bankov 299

A STUDY OF THE VARIATION OF THE COORDINATES OF THE MIDPOINT OF HITS WHEN FIRING BULLETS WITH RADIAL GROOVES ON THE OGIVE
Krasimir G. Kalev, Rosen N. Lazarov, Miroslav St. Rashkov 304

URBANIZED ENVIRONMENT – DEFINITION AND TAXONOMY
Radoslav B. Ghalakov 309

EFFECTS OF AMMUNITION IN AN URBAN ENVIRONMENT
Radoslav B. Ghalakov 315

WEAPONEERING IN AN URBAN ENVIRONMENT
Radoslav B. Ghalakov, Andon P. Andonov 322

COMMUNICATION AND COMPUTER TECHNOLOGIES AND CYBERSECURITY 328

NEW TECHNOLOGICAL TRENDS AND IMPACT FOR FUTURE OF CYBERSECURITY
Mihailescu Marius Iulian, Dumitru Dan..... 329

ARTIFICIAL INTELLIGENCE. SAME RULES, DIFFERENT PLAYGROUND
Elena Răducan 336

THE SECURITY CULTURE WITHIN ORGANIZATIONS AND ITS RELATIONSHIP WITH INDIVIDUAL SECURITY OF EMPLOYEES IN THE CYBERSPACE
Gârdan S. Daniel Adrian, Uţă M. Cristian, Hurloiu M. Lăcrămiora-Rodica, Hurloiu I. Ion-Iulian, Ghiorghiţă V. Eugen 344

THE ROLE OF MOTIVATED EMPLOYEES IN CREATION OF COMPETITIVE ADVANTAGES THROUGH INFORMATION SECURITY WITHIN MODERN ORGANIZATIONS
Gârdan S. Daniel Adrian, Duda I. Iordan Gheorghe Iosif, Gârdan I. Iuliana Petronela, Andronie I. Mihai 350

MODERN POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS
Zhaneta N. Savova, Rosen A. Bogdanov 358

GLOBAL RELIABILITY FOR INFORMATION STORAGE VIA SOLID STATE DRIVE
Daniel R. Denev 364

ANALYZING DATA AND TESTING THE SINGLE WIRE HANDOVER CAPABILITIES OF CATEGORY 8 CABLES
Daniel R. Denev, Tsvetoslav S. Tsankov 371

APPROACHES FOR BUILDING AUTOMATED MANAGEMENT AND MONITORING SOFTWARE ARCHITECTURES OF RF SPECTRUM
Miroslav G. Nedelchev..... 381

ANALYSIS OF SPECTRUM MANAGEMENT AND MONITORING SYSTEMS
Miroslav G. Nedelchev..... 387

PREDICTIONS AND EVALUATION WITH AI IN CYBERSECURITY
Angela R. Borisova 394

CYBERSECURITY ASSESSMENT METHODOLOGY FOR E-LEARNING PLATFORMS
Radostin S. Dimov, Linko G. Nikolov, Dimitar S. Dimov 401

RESEARCH OF DIFFERENT TYPES OF DECODE ALGORITHMS OF TURBO CODES AND THEIR COMPATIBILITY WITH ENCRYPTION DEVICE
Stanimir H. Parvanov, Dimitar S. Dimov, Ivan Y. Radev..... 407

TRENDS IN DEVELOPMENT OF THE SMART GRINDS
Dobry S. Stoynov, Dimitar I. Raev, Dimitar St. Dimov..... 414

APPROACHES FOR PROVIDING CYBERSECURITY OF PRESENT POWER LINE COMMUNICATIONS
Dobry S. Stoynov, Dimitar I. Raev, Ivan Y. Radev 420

ANALYSES OF 0-DAY THREATS WITH FIREEYE EDR
Veselka Stoyanova, Martin Rakov 426

WLAN IEEE 802.11BE OPPORTUNITIES AND PERSPECTIVE IN FUTURE
Dimitar S. Dimov 431

AUTONOMOUS DRIVING – STEP IN THE FUTURE
Ivan Y. Radev, Petya N. Stefanova 436

M3R RADAR – ADVANCED COGNITION, AGILITY AND AUTONOMY CAPABILITIES
Ivan Y. Radev, Nikolay H. Kopanov, Petya N. Stefanova 439

QUANTUM IDEAS FOR PROVISION THE BEHAVIOR OF MICROSCOPIC OBJECTS
Yordanka M. Lambova, Veliko M. Lambov 441

INTRODUCTION OF TECHNOLOGIES IN MEDICINE BASED ON ARTIFICIAL INTELLIGENCE
Aleksandra K. Atanasova 446

SOCIAL STUDIES 451

SYNCHRONISATION OF THE PROCESSES OF SOCIOLOGICAL STUDY ON THE QUALITY OF EDUCATION AND THE LEARNING LESSONS PROCESS AT THE RAKOVSKI NATIONAL DEFENCE COLLEGE
Zarko I. Zdravkov, Zhivo B. Petrov, Anelia A. Atipova, Sevdalin H. Stoykov 452

FEATURES OF LANGUAGE IN PROFESSIONAL MILITARY COMMUNICATION
Valya Simeonova 462

THE EFFECT OF STRESS ON MENTAL FUNCTIONING IN VOLUNTEERS AND NAVAL SPECIALISTS
Elena Anzova 465

VIROLENCE AND MEMETIC POTENTIAL OF "CHEMICAL, ETHNIC AND BIOLOGICAL WEAPONS" IN INFORMATION WARFARE
Victor Dobrev 467

ETHNICITIES, RELIGIONS AND INTERESTS INREGIONS OF PAZARDZIK AND PLOVDIV
Daniela D. Dimitrova 472

GEODESY 476

ON THE CHOICE OF MAPPING PROJECTION IN GEOINFORMATION SYSTEMS
Petina A. Andreeva 477

ON THE ASSESSMENT OF GEODATA QUALITY AND THE CONTROL OF ERRORS IN THE DATABASE
Petina A. Andreeva 482

SOURCES OF GEODATA ON GEOINFORMATION SYSTEMS
Petina A. Andreeva 486

EXPLORING AND MODELING THE MAGNETIC FIELD IN POLAR REGIONS USING THE DATA FROM THE SWARM MISSION
Violeta R. Yordanova, Andrey I. Andreev 492

INFLUENCE AND ANALYSIS OF GEODETIC PRIMARY DATA MEASUREMENTS DURING THE IMPLEMENTATION OF A MONITORING SYSTEM IN AN OPEN MINE - ADAPTIVE PERIOD
Yasen T. Prokopov 502

MONITORING OF CONTROL POINTS POSITION IN AN OPEN MINE - SPACE-TIME RELATIONS BETWEEN THE DEFORMATION FIELD COMPONENTS
Yasen T. Prokopov 508

IDENTIFICATION OF LAND PROPERTY
Ilinka Ivanova, Yasen T. Prokopov 513

CERTAIN ASPECTS OF GEOSPATIAL ANALYSIS IN GEOINFORMATION SYSTEMS
Petina A. Andreeva 518

RASTER ANALYSIS IN GEOINFORMATION SYSTEMS
Petina A. Andreeva 525

AGAIN, THE DILEMMA ARISES TO CREATE A MODEL OF GEOID OR QUASIGEOID
Andrey I. Andreev 530

AN APPROACH TO INCREASE THE ACCURACY OF PHOTOGRAMMETRIC MEASUREMENTS IN THE ENVIRONMENT OF AGISOFT METASHAPE PROFESSIONAL
Dimitar D. Petrov 537

INACCURACIES IN LINEAR OBJECTS TRANSFERRED FROM THE MAP OF THE RESTORED PROPERTY TO THE CADASTRAL MAP
Mirem E. Niyazi-Yusuf 547

RELATIONSHIP BETWEEN IMAGE COORDINATES OF CHARACTERISTIC POINTS OF A STEREO PAIR OF PHOTOGRAPHS
Monika B. Bedzheva 560

METHODOLOGY FOR BUILDING A SINGLE PHOTOGRAMMETRIC MODEL
Monika B. Bedzheva 566

A METHOD FOR BUILDING A PHOTOGRAMMETRIC MODEL OF AN AREA PHOTOGRAPHED WITH AN UAV
Monika B. Bedzheva 572

CREATING AN ORTHOPHOTO MAP AND ELEVATION MODEL OF AN URBANIZED AREA WITH A UAV
Nikolay H. Kopanov, Ivan Y. Radev 580

PLENARY SESSION

TECHNICAL READINESS TO START NATIONAL SECURITY MANAGEMENT SYSTEM AS A REALIZATION OF STRATEGIC GOAL OF REPUBLIC OF POLAND WITH A USE OF JASMINE CRISIS MANAGEMENT SYSTEM

Bartosz Biernacik

Lt.Col. Bartosz BIERNACIK, PhD Eng.– b.biernacik@aon.edu.pl;, War Studies University, al. Gen. Chruściela – Montera 103, 00-910 Warsaw, Poland

Abstract: *Modern IT support is a must in Armed Forces as well as in public services in any country that is willing to be able to conduct operations in times of peace, crisis and war. Usage of modern ICT without creation of situation awareness of all services in the country is not enough and need to be changed. This article is about the latest improvement that was taken in War Studies University that affect the whole Polish Armed Forces and public services and allows to create national security management system as a realization of strategic goal of Republic of Poland with a use of Jasmine Crisis Management System.*

Keywords: *Command Support System, Public Services, ICT, NSS NATO, NNEC, JASMINE CMS*

Introduction

"Integrate the national security management system, including state defense management, enabling the combination of processes, procedures and operating practices, by integrating the systems that have been operating so far, in particular national security management, crisis management and cybersecurity. Ensure the ability to quickly adapt to the emerging new challenges and threats and to identify opportunities".

National Security Strategy of the Republic of Poland 2020, page 13.

So far the IT support to the common business was taken into consideration only within the organization itself, connections between various organization from "two sides" military and civilian were rarely taken into consideration. IT systems are common in almost all activities that people conduct on a daily basis. In civilian environment IT is used to every single thing. Imagine that it is not possible to solve any task without the IT system support – from buying the ticket to the bus, ending with the communication with the relatives. The same is becoming in military environment. Nowadays more and more activities are supported by specialized ICT systems.

The time to change this situation has come suddenly and in most minds unexpectedly. We write in many important documents about the interoperability, about the implementation of different NATO standards that allows us to exchange the data between all allied nations taking part in operations as a NATO or UN mandate to solve problems in different part of the world. But all of the activities takes only a view of "military part of the business". In most cases we do not take care of the other part of the security system – even bigger than the Armed Forces – civilian part of the security system. We may find plenty of tasks that public services who are a part of the civilian part of the National Security System – mentioned many times in National Security Strategy of the Republic of Poland since many years from

1989 year. The problem is that not taking into consideration this huge part of the system we may become blind in case of crisis or even worse – during the war time. Why is that possible?

The answer is easy – public services are using their ICT systems and if not asked to cooperate with military units are not willing to spend effort and labor on creating interoperability between their systems and their military counterpart while waiting for this move from the military side. Therefore we have the situation, that every service create their own solution to be used in their business. In military environment the situation is much better, because of NNEC (NATO Network Enable Capability) program and his successor – FMN (Federated Mission Network). Those programs limited lawlessness, freedom and independence of the commanders in different types of armed forces. In public services is not that nice. State Fire Service, Medical Rescue, Police and others are using different ICT systems without being asked to fulfill similar interoperability standards as it is in Armed Forces. That is why there was a strong need to change that trend and to propose a solution to create NATIONAL SECURITY MANAGEMENT SYSTEM.

Situation in Europe – the war started by Russia against Ukraine without a declaration quickly opened the eyes of those, who were declaring that conventional war will never ever happen in this part of the world… Our years of predicting (and asking for preparation to that) this scenario unfortunately had become the true. So the work on the common solution to exchange the data and to allow the principles of the nation to know what is going on speeded up.

Creation of National Security Management System

The idea of creation of this kind of solution was written in National Security Strategy of the Republic of Poland almost since the change of political system in 1989 as a one of the strategic goal of the Republic of Poland. Since then not many activities had happened – in each NSS it was mentioned, but nothing had happened until….. 24th of February 2022. Except some activities taken by NDU.

First attempt to creation of the system

National Defense University at that time (NDU)[1] took into consideration problem of exchange the data between military and civilian services. In 2010 we started our work to create solution – a tool that will allow exchange the data and give the chance to display data coming from military as well as civilian ICT systems and show that on one platform. The result was presented during the exercise PIERŚCIEŃ 2012 that took place on a military training ground in Drawsko Pomorskie (the biggest military training field in Europe)[2]. The first attempt to this problem resulted creation of the first version of JASMINE Crisis Management System (JASMINE SMC). The idea of it was to create ICT system that will present the data coming from all the ICT specialized systems used in military and civilian environment without necessity of implementation of any new solution or forcing the services to get rid of any of their systems.

Figures 1 – 4 shows the usage of the CMS during the PIERŚCIEŃ-12 exercise in the non-military elements.

[1] National Defense University – 1990 – 2016 – predecessor of War Studies University.
[2] https://csbdrawsko.wp.mil.pl/pl/ (access September 2022)

Fig. 1. Usage of the CMS during the exercise PIERŚCIEŃ – 12 in June 2012.
Source: Material from the Pierścień – 12 exercise.

Fig. 2. Usage of the CMS during the exercise PIERŚCIEŃ – 12 in June 2012. You may see the Teldat hardware solution dedicated to the different level of command.
Here - position of the district fire brigade headquarters
Source: Material from the Pierścień – 12 exercise.

Fig. 3. Usage of the CMS during the exercise PIERŚCIEŃ – 12 in June 2012.
You may see the Teldat hardware solution dedicated to the different level of command.
Source: Material from the Pierścień – 12 exercise.

Fig. 4. Main window of the CMS during the exercise PIERŚCIEŃ – 12 in June 2012.
Source: Material from the Pierścień – 12 exercise.

At the time of 2012 year there was an idea to present posiibility to collect data from military as well as civilian systems and show them on the web portal based ICT solution. In the bacground there was Share Point solution used as a new at the time tool used in military environment. That was the new approach, because Polish Armed Forces was implementing the new ICT instead of WISE which was then withdrawn from NATO and from Poland as well.

The scenario (figure 5) shows that the first exercise the following Crisis Management levels were used: Szczecin as a voivodship level; Drawsko Pomorskie as a county level and the and rescue teams at the scene of the operation

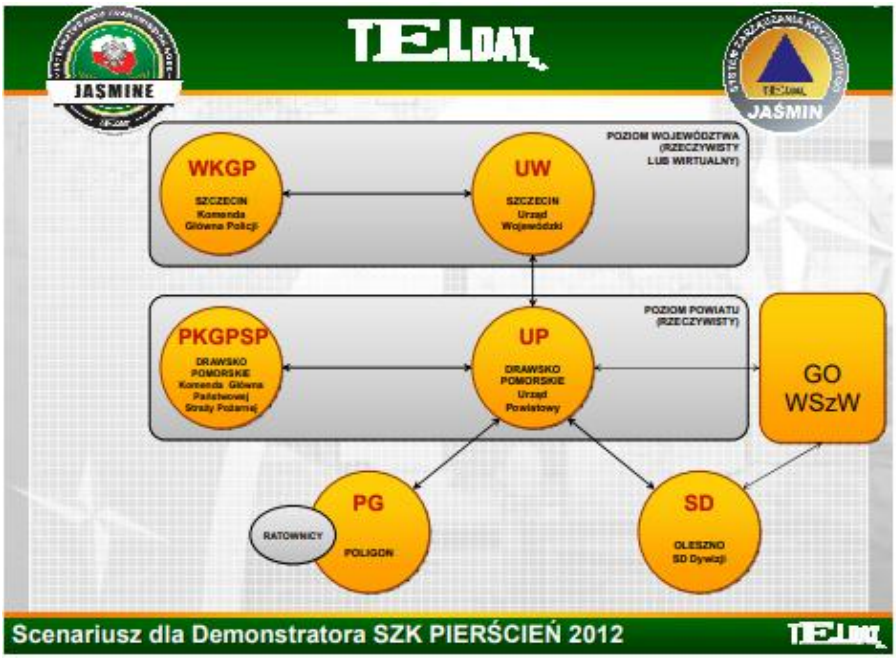


Fig. 5. Scenario of usage of the CMS during the exercise PIERŚCIEŃ – 12 in June 2012..
Source: Material from the Pierścień – 12 exercise.

For that exercise the Teldat company created special set of tools for the real rescue teams. Starting from the laptop in ruggedized version for the vehicle (Tactical terminal T4), smaller laptop for the commanders of rescue teams (T1000) and a marker for a rescuer or a vehicle participating in the action. First two gives the chance to be active users of the system – user of the laptop was able to see what is going on during the rescue action. The marker was established for the rescuer or a vehicle that not necessarily need to be an active user of the system – they only was sending their position and (if necessary) details of the unit they represent (see figure 6).

Fig. 6. Equipment used for CMS during the exercise PIERŚCIEŃ – 12 in June 2012..
Source: Material from the Pierścień – 12 exercise.

The end result scenario map was presented on figure 7.

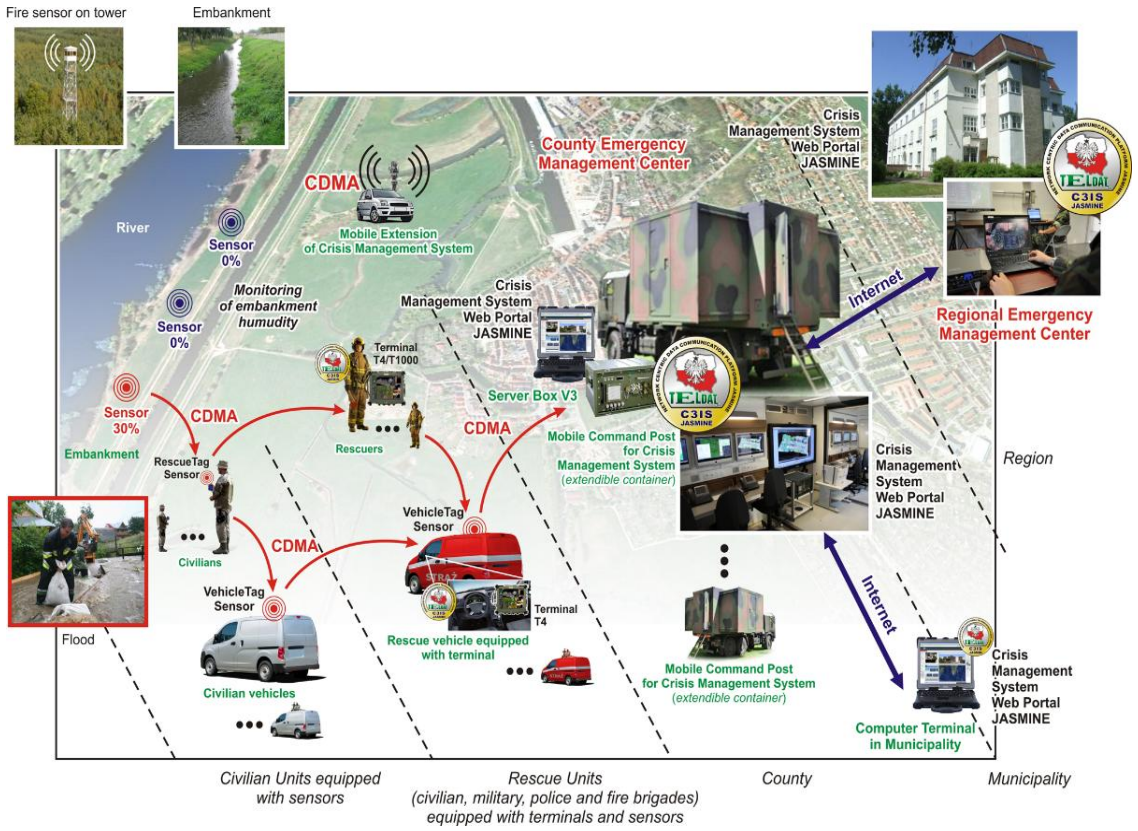


Fig. 7. Scenario of usage (with marked levels of support and the means of communication) of the CMS during the exercise PIERŚCIEŃ – 12 in June 2012.
Source: Material from the Pierścień – 12 exercise.

Results of the exercise were very impressive, and all taking in that event sides were under pressure of possibilities of that system. But as always… time passed and those willing did not speak. Until beginning of 2022…

Second attempt - Implementation of JASMINE Crisis Management System in a new version (2022)

As a result of plenty of presentations and real and practical usage of the family of the JASMINE systems (DSS, BMS, HMS, JFSS and more) the public services started to be interested (again) in implementation of this kind of tool that allows them to collect data form all civilian as well as military services and show it on one big screen for the commanders.

The Government's Security Center (GSC) which is the higher civilian institution that is responsible for crisis management in Poland requested a real time presentation of the possibilities of the JASMINE CMS. The plan was to provide the exercise on… 24th of February 2022. Yes. That day we provided a presentation of possibility of the JASMINE CMS for the public services representatives.

As an unexpected situation, the main representative was asked to come back from his way to the event… and he saw the results later – during the XXX anniversary International Military Exhibition in Kielce when he visited War Studies exposition – we were showing this year JASMINE CMS as a proposal to improve the National Security…

Scenario of the exercise was simple – one teenage girl disappear form home and is in danger. The information that was created on Police station is put into the Police system and then managed by police officer – he selected which data may be transferred to the JASMINE CMS. Then there is a commander

of the rescue group that decide to send three different teams into the terrain and search it – close to the latest possible position of the searched person.

Fig. 8. Screens from the exercise taken on 24th February 2022.
Source: Material from the Teldat.

Since the first attempt the equipment has changed. Now the rescue teams have different possibilities to choose the right stuff for each action. Some of them stay the same as they were proposed in 2012 – like in example the marker for the rescuer. The others present much better performance than those from 2012. It is shown on figure 9.

Fig. 9. Mobile components for the JASMINE CMS used in case of action or training.
Source: Material from the Teldat.

There are more changes in the second attempt to implement the system. As it was mentioned the first version of the JASMINE CMS was based on SharePoint software. This time the platform has changed. Under the consideration was taken fact that in most cases the specialists from civilian crisis management are the previous officers. It makes big difference, because during their service time they spent a lot of time using HMS C3IS JASMINE system – version of Command Support System dedicated to the military (see Figure 10).

If so it is much easier for them to start using similar kind of application when they retire from the military service and starts their new position as a crisis managers in civilian part of the national security system. So the application now is based on the same core services as our military system. The difference is in the signs the put on the map (and of course some more things like less restrictions in communication than in military environment). That is why now the application for the end user is more predictable for the retired officers.

If you ask what about those, who are not retired officers – the answer is simple – we have the training of HMS C3IS JASMINE system implemented in Armed Forces that may be simply adjusted to the civilian symbolism. Instead of APP6-A, B, C or D for the military symbols we nay use civilian symbols defined by our Ministry of Internal Affairs and Administration (see Figure 11).

Just to remind – the training system was implemented in Polish Armed Forces in 2019 and consist of the six level of courses as a result of the decision taken by the Chief of Staff of the Polish Armed Forces in 2018 about implementation of HMS C3IS JASMINE system as a primary Command Support System.

As an answer War Studies University prepared extended version of training of HMS C3IS JASMINE. The extension was necessary to implement to speed up with the number of operators trained with this system. Until the new training system all the University students were trained with the HMS C3IS JASMINE system during the education process during the academic year. New training system was dedicated to the whole soldiers from Poland (and also the NATO countries).

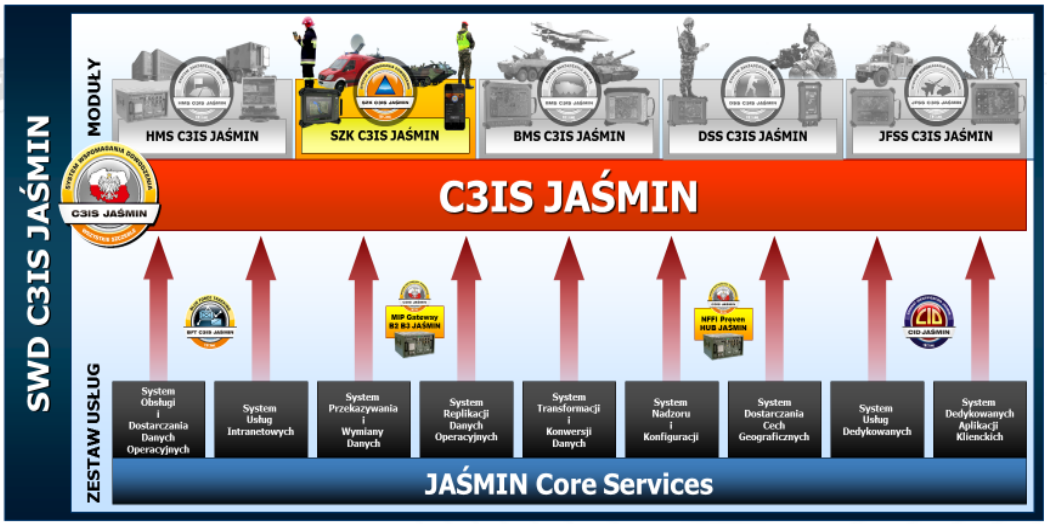


Fig. 10. Core services on which JASMINE CMS is based.
Source: Material from the Teldat.

Fig. 11. Training system implemented into the Polish Armed Forces in 2019.
Source: Author's materials.

The training system consist a few levels of the knowledge of the HMS C3IS JASMINE system:

- 1st level – BASIC COURSE is dedicated to the operators that do not know anything about the CSS system. It takes 5 working days (ap. 30 hours) and give the knowledge to operate the system;
- 5th 2nd level – ADVANCED COURSE is dedicated to those who accomplished the 1st level course and give the advance knowledge of the system. It is more concentrated on MDMP showing the operator role during each of the phase of the process;
- 3rd level – PREPARATION AND CONDUCT OF THE MILITARY EXERCISE with the HMS C3IS JASMINE system is dedicated to the teams that are responsible to prepare and conduct the military exercise. To accomplish this level candidate must accomplish the 1st and 2nd level of the training;
- 4th level – OPERATIONAL ADMINISTRATOR of HMS C3IS JASMINE system is dedicated to the operators that are responsible for support the Operators on the Command Post with the system running. To accomplish this level it is required to accomplish all previous courses;
- 5th level – INSTRUCTOR of the HMS C3IS JASMINE system is dedicated to the persons that are going to organize in their military units the courses at the first level. Thank to this there will be more instructors and it will be much more popular to get the first level course.
- 6th level – INTENSIVE COURSE FOR INSTRUCTOR of the HMS C3IS JASMINE system is dedicated to those who are prescribed by Unit Commanders to become trainer and are going to organize the courses from first level.

What is important to be mention at that place is that we may easily adopt this training system implemented in Armed Forces and spread it into the public services conducting crisis management using i.e. JASMINE CMS. Therefore we may say that another of the milestone is in place ready to be used (first milestone – technical readiness; second milestone – training system).

We need to remember that technical readiness to create system is not enough. We need to change the mindset of the operators, decision makers. There is a need to change the culture of the security culture[3].

[3] P. Ostolski, Culture functions for creating security culture, Security dimensions, No. 37; 2021 (78-90)

Juliusz Piwowarski in the article: *"The security (culture) rhombus. Redefining security environment"*, based on his research, proposes a new way of perceiving the security environment. *"I present and justify an alternative to the narrow approach to security environment, which is based on the narrow definition presented in the White Book on National Security of the Republic of Poland"*[4]. His considerations exceed the framework of the White Book of National Security of the Republic of Poland and provides evidence for a wider definition of the research area in security sciences. This point of view is justified. The confirmation is in the National Security Strategy of the Republic of Poland. *"Today's security environment is increasingly complex and insecure"*[5] .

Security is a state in which its subjects are in a constant balance between the objective and subjective perception of the surrounding reality. Any elements that make up the security environment. The level of our security culture depends on many factors. The most important of them are the constituent elements of culture[6].

By usage of modern ICT we are able to strengthen certain desirable leadership qualities mentioned by many classics of military strategy like Clausewitz, Sun Tzu, Sun Pin and many others[7]. One of the leadership qualities that should be strengthened is determination, understand as an ability to take a decision in the limitation of time and lack of information without hesitation and doubts using his intelligence and wisdom. If the system is able to create situation awareness, collect data in a real or close to the real time and display it on a digital map, satellite picture or any other operator require, any alarm is created and spread within the system in a seconds, commanders are aware about the holdings they are available for their teams – all of this change an approach to decision makers and increases the level of accuracy of decisions made based on that data.

Coming back to the creation of National Security Management System we have to mention the June 2022. That time commanders of provincial divisions of the State Fire Service asked to provide similar presentation that was provided to the Government's Security Center in February. With a small difference – they asked to provide presentation of use of CMS during the fire and action made by Fire Brigades.

The second presentation has taken place in June 2022 and is presented on figure 12.

Fig. 12. Screens from the exercise taken in June 2022.
Source: Material from the Teldat.

We did not have to wait for a long time for the results of that presentation. Almost immediately the decision from the Fire Service was taken to use this system during the exercise. The exercise was not just an exercise – it was 30th anniversary of the biggest forest fire in Poland. It was provided since 30th of August until the 1st of September. During the time one of the system used to create situational awareness was JASMINE CMS. Figure 13 shows the exercise. The exercise took place in Kuźnia Raciborska Southen-East part of Poland.

Separate forces and resources of the Central Operating Defense took part in the exercises. In total, it was about 100 rescue and firefighting vehicles and special vehicles and over 400 firefighters from the

[4] J. Piwowarski, *The security (culture) rhombus. Redefining security environment*, "Kultura Bezpieczeństwa", 2019, no. 34, p. 141 [in] Ostolski P., Culture functions for creating security culture, Security dimensions, No. 37; 2021 (78-90), p.79
[5] National Security Strategy of the Republic of Poland 2020, page 5.
[6] P. Ostolski, Culture functions for creating security culture, Security dimensions, No. 37; 2021 (78-90), p.79
[7] P. Ostolski, Cechy przywódcze kadr systemu bezpieczeństwa narodowego, p.164-175

following voivodships: Śląskie, Małopolskie, Podkarpackie, Świętokrzyskie and the Central School of the State Fire Service in Częstochowa. Representatives of the Security and Crisis Management Department of the Silesian Voivodship Office, State Forests (including 1 Dromader type fire-fighting aircraft) and the police also participated in the exercises[8].

The main objective of the exercises was to determine the degree of preparation of the forces and resources of the Central Operating Support to extinguish large-area fires in forest complexes, including, in particular, the supply of water over long distances. In addition, the exercises are aimed at checking the organization and work of the staff at the strategic level and the organization of logistic facilities for the needs of the activities carried out[9].

Fig. 13. Screens from the exercise in Kuźnia Raciborska.
Source: Material from the Teldat

The latest version of the system may be independent application installed on the computer as a working station (it can be installed on desktop computer, laptop, netbook, tablet) or may be used as a web access and displayed on every single equipment with display and access to the Internet (desktop computer, laptop, netbook, tablet, mobile phone).

The list of the components prepared for the end user is as long as it is in military HMS C3IS JASMINE version.

The following modules can be included among the most important components:

- Map Component;
- Document Component;
- Printing Component;
- Combat Log Component;
- Aggregation Component;
- Video Component;
- Communication Component;
- Simulation Component;
- And many more…

Those modules gives a chance for collaborative work within the rescue team, command post or the higher command.

[8] https://www.gov.pl/web/kppsp-raciborz/krajowe-cwiczenia-ratownicze-pk-kuznia-raciborska-2022 (access September 2022)
[9] Ibidem.

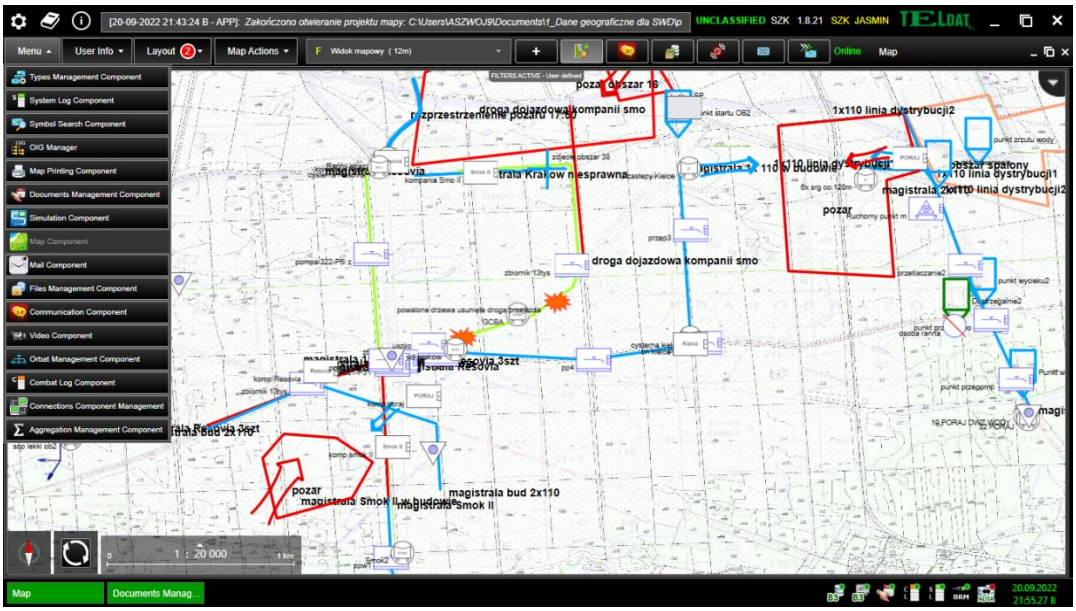


Fig. 14. Menu in JASMINE Crisis Management System. You may see the long list of available components for the operator.
Source: author's material.

The results of our tests and CMS JASMINE performance was presented during the 30th International Defense Industry Exhibition MSPO in Kielce that took place from 6th until the 10th of September 2022.

Fig. 15. War Studies University exhibition stand during the 30th International Defense Industry Exhibition MSPO.
Source: Teldat materials.

That was the possibility to present War Studies University experience in providing the technical possibilities to use the joint ICT systems and create National Security Management System based on CMS JASMINE.

The last (for now) example of usage JASMINE CMS was the exercise provided for medical rescue teams in the middle of September 2022, after the Military Exhibition in Kielce. That was the chance to present the performance of the JASMINE CMS to the medical specialists that on a daily basis helps people.

Fig. 16. Screens from the exercise in Bydgoszcz with Medical rescue teams conducted in September 2022.
Source: Material from the Teldat

Summary

The unstable time has come. We need to prepare to what may be hardly predicted. Nobody is able to predict what will happen and how much time has left to the unpleasant and unwanted situations. To be at least a little more prepared we need to act quickly and in intelligent way.

War Studies University is the highest University in providing the studies and courses for the Polish Armed Forces. To our University comes officers with an experience from units and their knowledge and experience combined with the knowledge of academic teachers and the system producer gives the chance to constantly develop better and better Command Support System – System of Systems.

The latest exercises conducted in 2022 and planned in 2023 shows that there is a strong need on the public services side to implement modern, sophisticated ICT system but on the other hand well known for operators, easy to use and time reducing to take the decision. This is what JASMINE Crisis Management System exactly is. Well known and used in Polish Armed Forces, easy to use for those, who had contact with any NATO Command Support System as well as with our Polish HMS C3IS JASMINE system. We have the training system implemented (so far in The Army but it may be changed).

To summarize the cooperation between military and business started in 2010 gave a lot of experience to us as a military experts and let us change the approach to the conducting Military Decision Making Process now is giving new feedback – new possibilities of use in non-military environment in crisis management. Starting from typical military system – HMS C3IS JASMINE we are ready to use the JASMINE Crisis Management System. The most important is to keep the way that we discovered and implement the best practice into the national security system.

Nowadays, NATO and the Polish Armed Forces place great emphasis on the development of network-centric capabilities, including the interoperability of ICT solutions used in the Alliance countries. In response to this, the Academy actively conducts practical research on the possibilities and methods of using its military systems, which is included in the results of the conducted experiments. Their results enable the update of the regulations and doctrinal documents. They are also guidelines for determining the further development direction of the foregoing Polish systems.

As we may see the Ukrainian conflict shows that modern systems are the must not only for the Army but (and maybe even more) also for the civilians, who must be protected against the enemy activity as only it is possible.

Moreover, the need to secure civilian infrastructure must also be taken into account, and the use of the discussed solution significantly facilitates this. This system can be used to protect both the critical

infrastructure of the state as well as, for example, cultural monuments and places of particular importance to the citizens of a given country.

The capability of the automated data exchange between JASMINE CMS and public services systems used on a daily basis provides invaluable benefits in the way of carrying out the Crisis Management tasks and shortening the time from detecting the problem/danger situation to reaction to it, which in the current conditions of the 21st century is one of the most important features that determines the success or failure.

Once again we must enhance the message that we have technical readiness to establish National Security Management System as a realization of strategic goal of Republic of Poland with a use of JASMINE Crisis Management System.

References

[1] Biernacik B., Grel L., Surwiłło T., Vademecum użytkownika oprogramowania HMS C3IS Jaśmin Zautomatyzowanego Systemu Zarządzania Walką poziomu operacyjnego/taktycznego w wersji klienckiej. Poziom podstawowy, WSU, Warsaw, 2021
[2] Biernacik B., Integracja informacji w służbach publicznych na potrzeby reagowania kryzysowego, [in] Paradygmaty badań nad bezpieczeństwem. Zarządzanie kryzysowe w teorii i praktyce, WSB, Poznań 2013
[3] Biernacik B. Wsparcie informatyczne procesów informatycznych w podstawowej jednostce organizacyjnej uczelni wojskowej, AON Warsaw, 2013
[4] Ostolski P., Halicka B., Military leadership: case studies, Security. Theory and practice, Cracov 2022, No. 3 (XLVIII)
[5] Ostolski P., Culture functions for creating security culture, Security dimensions, No. 37; 2021 (78-90)
[6] Ostolski P., Kaźmierczak D., Geneza bezpieczeństwa, Astudia Administracji i Bezpieczeństwa, 2021, https://studia.administracji.i.bezpieczenstwa.ajp.edu.pl/resources/html/article/details?id=226943
[7] Piwowarski J., *The security (culture) rhombus. Redefining security environment*, "Kultura Bezpieczeństwa", 2019, no. 34, p. 141
[8] Strategia Bezpieczeństwa Narodowego 2020, BBN, Warsaw 2020
[9] https://www.targikielce.pl/en/mspo
[10] https://www.teldat.com.pl/aktualnosci/2021/439-istotny-rozwoj-systemu-ksztalcenia-kadr-szkoleniowo-uzytkowych-hms-c3is-jasmin.html
[11] https://www.teldat.com.pl/aktualnosci/2021/442-nastepni-instruktorzy-hms-c3is-jasmin-sa-juz-w-dyspozycji-wp.html
[12] https://www.teldat.com.pl/aktualnosci/2022/461-szk-jasmin-w-zainteresowaniu-organizatorow-systemu-zarzadzania-kryzysowego.html
[13] https://www.teldat.com.pl/images/news/135/www_aon_edu_pl_2015_03_05.pdf
[14] https://www.gov.pl/web/kppsp-raciborz/krajowe-cwiczenia-ratownicze-pk-kuznia-raciborska-2022
[15] https://www.teldat.com.pl/oferta/produkty/systemy/319-szk-jasmin.html
[16] https://www.teldat.com.pl/do-pobrania/publikacje-naukowe.html
[17] https://csbdrawsko.wp.mil.pl/pl/

CYBER THREAT INTELLIGENCE AND PREVENTION-BASED INCIDENT RESPONSE TO REAL-WORLD CYBER ATTACKS

Mihailescu Marius Iulian, Dumitru Dan

Faculty of Engineering and Computer Science, SPIRU HARET University, Bucharest, Romania,
m.mihailescu.mi@spiruharet.ro, d.dumitru.mi@spiruharet.ro

***Abstract**: Due to the latest events (pandemic situation and military tensions between Ukraine and Russia) that marked postively and negatively our existence, private and professionaly, the attacks on institutions and organizations increased significantly everyday, and new experiences were faced and they caught many professionals with the guard down. Many lessons were taught but not all of them were applied accordingly everyday in their activity. The objective of the current work is to bring into discussion a set of aspects that are well-known by professionals in field of cybersecurity but they are not used properly due to a variety of reasons. Based on a wide analysis of the most important concepts, technologies and frameworks on which cybersecurity risk management is based, we will need in the future to treat with a maximum responsability the way that we are applying and integrating cybersecurity within organizations. Re-designing the way that we are treating cybersecurity, how it twill fit within the CSIRTs teams, will represent the way if the battle against attacks will be won or not.*

***Keywords**: cyber threat intelligence, prevention-based, incident, cyberattack, cybersecurity.*

Introduction

Cybersecurity is the defense against harmful attacks by hackers, spammers, and cybercriminals against internet-connected devices and services. Companies employ the procedure to safeguard themselves against phishing scams, ransomware attacks, identity theft, data breaches, and monetary losses. According to Forbes, a variety of alarming cyber security concerns will face us in 2022[1], including supply chain disruption, greater threats from smart devices, and a continuous shortage of cyber security experts. According to Cybercrime Magazine[2], cybercrime will have a big impact on the costs on the globe, around $10.5 trillion yearly by 2025. In addition, during the following four years, costs associated with cybercrime are expected to increase globally by about 15% annually.

We increase our human capability through technology, whether it be to respond to a natural disaster, protect against a cyberattack, or fulfill the enormous demands to enable the largest workforce to work remotely. For example, at Microsoft, cybersecurity serves as the cornerstone for assisting businesses in preserving business continuity when things change.

When working with enterprises from around the world who need to enable people to work efficiently and safely from a range of non-traditional settings, the teams should share this transformative vision. We have learned a lot about the role cybersecurity plays in assisting businesses in maintaining business continuity as we adjust to this new reality through these conversations. As a result, we can see five paradigm shifts in cybersecurity that will enable the development of work in a way that emphasizes inclusion of people and data.

[1] See https://www.forbes.com/sites/emilsayegh/2022/01/06/predicting-what-2022-holds-for-cybersecurity/?sh=1b29ea0c2b72
[2] See https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

From beginning it is important to clear the goal of each field in such way that we can understand their boarders within cybersecurity risk management and not creating confusions between the responsibilities.

Threat Intelligence represents those processes through which the data that is gathered, processed, and analyzed to identify the goals, targets, and attack tactics of a threat actor. Threat intelligence empowers us to take quicker, more data-driven security decisions and shift from reactive to proactive behavior in the face of threat actors.

The structure of the paper is described as follows:

- *Section 1. Introduction.* In this section we will specify the context and place the study within the new tendencies on which cybersecurity professionals should focus in the next years. Moving forward with *How does Cybersecurity can be defined nowadays and how it works?,* we will discuss those technologies, procedures, and techniques that should be include in cyber security risk management for Mobile Security (see Section 1.1) and Network Security (see Section 1.2).
- *Section 2. Cyber Threat Intelligence*. The section will give a short overview on what is Cyber Threat Intelligence (CTI) and how CTI should be used within different organizations and institutions. Due to the fact that the topic is wide and there are so many things to be discussed, we will provide only how CTI is impacting the processes behind the organizations/institutions.
- *Section 3. Prevention-based Incident Response*. In this section we will discuss about prevention-based incident response (PIR) which from professionals point of view is a paradigm shift game and many of security solutions should be focus on this paradigm. The section will point out the main importance and it can be game changer in cybersecurity.
- *Section 4. Artificial Intelligence vs Cybersecurity. Impact of Artificial Intelligence in Cybersecurity.* The section will discuss about the importance of AI in cybersecurity, and from developing solutions, the AI in cybersecurity is a hot point for many developers, engineers and researchers, the main reason is due to the fact that the AI solutions should be always adapting to the needs and trends in terms of new attacks [10], [11].
- *Section 5. Machine Learning vs Cybersecurity.* Learning from attacks and anticipating other attacks based on the behaviour of the networks and users, is very challenging and interesting, and brings new important challenges for developers, from tagging and classifying the attacks to decision models. The section will discuss general aspects from which we can draw an important conclusion for developing such solutions and algorithms.
- *Section 6. Deep Learning vs. Cybersecurity.* An attack has different behaviours, the mission of security solutions is to identify properly the behaviour of the attack and to figure out what he will impact within the organizations. The role of deep learning is to analyse in-depth the attack and to find more about it and how it can be isolate in such way that none of the resources and users will be affected. For this a solution for user trainings is necessary to be made available to them at any time [2].
- *Section 7. Conclusion.* The section will present a short summary of what it has been discussed, the main challenges that were experienced during this work and what are some possible future research directions, that researchers, engineers, and developers should have in mind as future trends. It is important to understand that we always need to update the solutions and to anticipate the needs of future.

How does Cybersecurity can be defined nowadays and how it works?

The technologies, procedures, and techniques used in cyber security include those that protect networks, data, and computer systems from intrusion. Below we will discuss about two important subdomains in which to explain how cybersecurity works and why it is important to focus on these two subdomain nowadays.

Mobile Security

Today, as more people rely on mobile devices, mobile security is a major issue. This subdomain guards against dangers including unauthorized access, device loss or theft, malware, viruses, and more for both organizational and individual data kept on portable devices like tablets, smartphones, and laptops. Mobile security also makes use of authentication and training to strengthen security.

The way individuals connect to the internet has changed dramatically thanks to portable devices like smartphones and tablets. Platforms, however, also play a part in the growth and sophistication of cyber attacks. As a result, there is a constant arms race among software businesses. In response to the constantly evolving nature of threats, new, cutting-edge security systems are being introduced. Although it's challenging to keep up with the stricter regulations that legislators are introducing, they are doing their part. Because of this, mobile device cybersecurity is more crucial than ever.

Attackers that never give up are constantly looking for the next big hack. On mobile devices, attacks that were wildly successful on desktop computers are now being used.

The most important types of attacks from 2022, are related to ransomware and mobile phisihing, and cross-platform banking attacks. *Ransomware and mobile phishing* - The mind of an attacker is unlimited. This being said, the goal of an attacker consist in using social engineering for obtaining access to sensitive information without permission. This is achieved through SMS messages to inject malware. In Check Point Press Release[3], one of the most important attack from 2022 is related to the Easter phishing scams that helps emotet assert its dominance. Emotet is very advanced, self-propagating and modular trojan which is using different methods for keeping his persistence and evasion technique to avoid being detected. *Cross-platform banking attacks* - In some literatures this may be known as *man in the browser* attack, a technique that is based on the deployment process of malware on the mobile device. According to Palo Alto[4], in 2022, Black Basta attack managed encrypt files on the target machine using extortion technique and demand ransoma for making the decryption possible.

Other types of attacks that took place in 2022 and their significance is important, are related to *infiltrating nearby devices, cryptocurrency mining attacks,* and *countering mobile threats.*

Network Security

The Covid-19 outbreak drove the majority of businesses to quickly transition their workforces to remote labor. Numerous studies indicate that a sizable segment of the workforce will continue to work remotely after the epidemic.

Most of the studies made on security flaws, shows that a crucial trend for cyber security is based on the processes that should be used by a business in such way that the main focus should be concentrated on the security issues associated with remote workforces. This include discovering and addressing fresh security flaws, enhancing systems, putting in place security rules, and making sure that monitoring and documentation are done properly. For more information and suggestions, read our comprehensive guide to working securely from home.

One of the most important trends in cyber security is working from home, which presents new cybersecurity threats. Compared to centralized offices, which typically have more secure routers, firewalls, and access control systems managed by IT security teams, home offices are less safe but with the right solution the environment could be configured to provide a strong security. E-mails are quite critical, especially due to their attachments with images, and solutions for scanning the images should be taken into consideration as well [12], [13].

[3] See https://www.checkpoint.com/press-releases/march-2022s-most-wanted-malware-easter-phishing-scams-help-emotet-assert-its-dominance/
[4] See https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/

One of the most important trends in the cyber security business is still cloud vulnerability. Once more, the pandemic's broad embrace of remote work has dramatically raised the need for cloud-based infrastructure and services, with security consequences for enterprises.

Scalability, effectiveness, and cost savings are just a few advantages that cloud services provide. However, attackers also view them as a prime target. Insecure interfaces, account theft, and data breaches are all frequently brought on by improperly configured cloud settings. Because a data breach costs $3.86 million on average, businesses need to take precautions to reduce cloud hazards.

In addition to data breaches, enterprises face the following network security trends and cloud security challenges:

- Guaranteeing compliance with the latest regulations with respect for each jurisdiction.
- Using all the necessary and required IT expertise for handling the requirements for cloud computing.
- Handling the issues related to cloud migration.
- Handling possible potential entry points for attackers.
- Insider threats.

Cyber Threat Intelligence

When analyzing a cyber threat, analysts frequently focus on the triad of actors, intent, and capability, taking into account each actor's motivations, tactics, techniques, and procedures (TTPs), as well as their access to the targets they are targeting. Making knowledgeable, forward-looking strategic, operational, and tactical evaluations is frequently feasible by understanding this triad.

From senior executives, such as Chief Information Security Officers (CISOs), police chiefs, and policy makers, to those on the ground, like information technology specialists and law enforcement officers, cyber threat intelligence has proven useful to state, local, tribal, and territorial (SLTT) government entities at every level. It also benefits other professionals, such as security guards, accountants, and terrorism and criminal analysts.

When used properly, cyber threat intelligence can offer increased understanding of cyber risks, enabling resource creation and allocation as well as a quicker, more targeted response. For example, it can help decision-makers identify acceptable business risks, create controls and budgets, decide on equipment and staffing, and more (strategic intelligence). Additionally, operational and technical intelligence can advance the use of indicators by validating, prioritizing, and defining the duration of an indicator's validity (tactical intelligence).

Prevention-Based Incident Response

When used properly, cyber threat intelligence can offer increased understanding of cyber risks, enabling resource creation and allocation as well as a quicker, more targeted response. For example, it can help decision-makers identify acceptable business risks, create controls and budgets, decide on equipment and staffing, and more (strategic intelligence). Additionally, operational and technical intelligence can advance the use of indicators by validating, prioritizing, and defining the duration of an indicator's validity (tactical intelligence). Uncontrolled incident activity can grow into a greater issue, which could result in data breaches, exorbitant charges, or system disruptions. Organizations can reduce losses, address exploited vulnerabilities, restore services and operations, and reduce the risk of subsequent incidents by acting swiftly after an occurrence.

SANS is a private company that conducts research and informs the public about security-related topics. The incident response process (see Figure 1) is broken down into six phases under the SANS framework: preparation, identification, containment, eradication, recovery, and lessons learned.

Figure 1: SANS framework[5],
image source: https://www.gadgetaccess.com/sans-incident-response-planning/)

NIST is a US government organization that creates standards for the technology and security sectors. A thorough incident response strategy was created as part of their cybersecurity work (see Figure 2). It contains information on developing communication plans, incident response teams, incident response plans, and training situations.

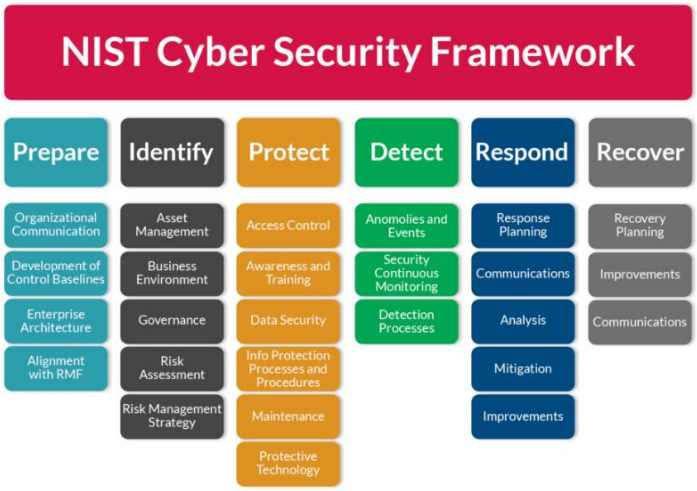


Figure 2: NIST framework, image source: https://netgaincloud.com/blog/new-nist-framework-strengthens-risk-management/

An incident response plan is a document that lists the security procedures to be followed in the event of an incident and the people in charge of responding to the incident. The following information is often included in an incident response plan: methods and approaches for responding to incidents; how crisis response may further the overall objective of your organization requisites for each level of the incident response process; roles and duties for carrying out incident response tasks; routes of communication between the organization's rest and the incident response team; and metrics to measure incident response effectiveness.

AI vs Cybersecurity. Impact of Artificial Intelligence in Cybersecurity

Cybersecurity is only one of the many domains where AI offers benefits and applications. AI and machine learning can assist in keeping up with hackers, automating threat detection, and responding more efficiently than traditional software-driven or manual procedures in today's world of quickly developing cyberattacks and rapidly multiplying gadgets [1].

For online dangers and potentially criminal activity, artificial intelligence plays an important role and it is used with success in the process of identification. The volume of the new malware that is occur-

[5] See https://www.gadgetaccess.com/sans-incident-response-planning/

ring each week, represents an important challenge for the traditional software applications to handle, so artificial intelligence is very helpful in this situation, providing in-depth analysis of everything that is happening. The systems based on artificial intelligence are designed and developed with respect for training in such way that they are capable to detect malware, to realize and obtain pattern recognition, and to identify the smallest characteristics for malware or ransomware attacks before they are launched with success within the system/networks. Another important aspect is represented by natural language processing, which collects data by itself and by accessing articles, news stories, and research on cyber-threats, were artificial intelligence comes and enables a higher predictive intelligence. This will help us in having access to information related to the new and most awkard tactics and attacks. In this situation we should not underestimate the cybercrminals, as they are the first ones that are following the trends.

Machine Learning vs Cybersecurity

Effective cybersecurity technology cannot be implemented today without a significant machine learning component. However, machine learning cannot be used successfully without a thorough, in-depth, and thorough approach to the underlying data [3].

Cybersecurity systems can use machine learning to examine patterns and learn from them to help stop similar assaults and react to altering behavior. It can assist cybersecurity teams in being more pro-active in thwarting threats and quickly responding to ongoing attacks. It can shorten the time spent on repetitive work and make it possible for enterprises to employ their resources more wisely. In machine learning, patterns are created and then modified using algorithms. Because the data must represent as many different outcomes from as many conceivable scenarios as possible, you need a lot of rich data from all over the place to establish patterns [4]. Applications employ machine learning techniques to recognize and respond to assaults. Big data sets of security events can be analyzed to find patterns in harmful activity and help with this. When similar events are found, ML makes it so that the trained ML model can automatically handle them.

Organizations can better allocate resources by using quantitative methods to assign risk rankings to different network segments. ML may be used to analyze datasets of prior cyberattacks and identify the network components that were most frequently exploited in specific assaults [5]. With regard to a specific network area, this score can help estimate the likelihood and impact of an attack. Assisting organizations lower their chance of becoming victims of such attacks.

Deep Learning vs Cybersecurity

Organizations struggle with the majority of cybersecurity being reactive. They rely on signatures or indicators of compromise for the threat detection capabilities of the technologies they use to safeguard their environment. Because they are only useful for identifying risks they are already aware of, those technologies are useless against zero-day or other unknown attacks [6].

Here is where deep learning can alter the course of events. Machine learning has a subfield called deep learning. Machine learning algorithms are excellent for using data analysis to find solutions, but they have several drawbacks. "Deep-learning algorithms handle the same problem utilizing deep neural networks, a form of software architecture inspired by the human brain," according to PC Magazine[6] claiming (though neural networks are different from biological neurons) [7].

Layers upon layers of variables make up neural networks, which can identify photos and translate speech to text by adjusting to the characteristics of the input they are trained on. Since deep learning is a relatively new discipline, there aren't many players that are specifically interested in it. Only a few deep learning neural networks are in operation, and only one of those is being used to address the present cybersecurity concerns. Deep Instinct owns the deep learning framework in question [8].

[6] See https://www.pcmag.com/news/what-is-deep-learning

Automation is essential for defending against the enormous amount of risks that businesses must deal with, but ordinary machine learning is too constrained and still needs a lot of tweaking and human involvement to produce the desired outcomes. Deep learning goes above and beyond to keep improving and learning over time so that it can foresee hazards and stop them before they happen.

Conclusion

The current paper discussed those topics that represents the most important technologies on which cybersecurity professionals should focus and researchers should take into considerations when they are designing and implementing new security modules.

Everything from now on should be treated with maximum responsibility, taking into consideration technologies such as artificial intelligence and machine learning for detecting and investigating any behaviour within complex networks, focusing more on prevention-based incident response, in such way that CSIRTs should have a deeper analysis of what is going within the attacks and impact on their organizations.

The challenges experienced during this study were overcomed, and most of them were focused on the advantages and disadvantages of artificial intelligence, machine learning and deep learning technologies together with their algorithms. We have tried to provide a summary of the main positive features that should be taken into consideration when developing such solutions and use them within institutions/organizations through a cloud environment as cloud solution or other complex applications from different fields, such as applied physics [14] and thermodynamics.

As for future, a research plan should include a psychological user profile which can help us to identify in what mood the user is accessing the machine within the network with help of specific keyboards and mouse’s, using more artificial intelligence and machine learning algorithms and methods for learning more out from the attacks.

References

1. N. S. Loredana, "On recommendation systems applied in big data," 2016 8th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2016, pp. 1-6, doi: 10.1109/ECAI.2016.7861068.
2. F. Postolache and C. Ș. Dumitriu, "Reshaping the LMS IT Architecture and Educators Methodology through Blended Learning Approach," 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2021, pp. 1-6, doi: 10.1109/ECAI52376.2021.9515134.
3. D. Dragos and S. Schmeelk, "What are they Reporting? Examining Student Cybersecurity Course Surveys through the Lens of Machine Learning," 2020 19th IEEE International Conference on Machine Learning and Applications (ICMLA), 2020, pp. 961-964, doi: 10.1109/ICMLA51294.2020.00156.
4. B. Ghimire and D. B. Rawat, "Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things," in *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8229-8249, 1 June1, 2022, doi: 10.1109/JIOT.2022.3150363.
5. F. O. Olowononi, D. B. Rawat and C. Liu, "Resilient Machine Learning for Networked Cyber Physical Systems: A Survey for Machine Learning Security to Securing Machine Learning for CPS," in IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 524-552, Firstquarter 2021, doi: 10.1109/COMST.2020.3036778.
6. A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi and R. Ahmad, "Machine Learning and Deep Learning Approaches for CyberSecurity: A Review," in IEEE Access, vol. 10, pp. 19572-19585, 2022, doi: 10.1109/ACCESS.2022.3151248.

7. Tarek Berghout, Mohamed Benbouzid, S.M. Muyeen, Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects, International Journal of Critical Infrastructure Protection, Volume 38, 2022, 100547, ISSN 1874-5482, https://doi.org/10.1016/j.ijcip.2022.100547.
8. Hanan Bahassi, Nahid Edddermoug, Abdeljebar Mansour, Azmi Mohamed, Toward an exhaustive review on Machine Learning for Cybersecurity, Procedia Computer Science, Volume 203, 2022, Pages 583-587, ISSN 1877-0509,https://doi.org/10.1016/j.procs.2022.07.083.
9. K. Y. Nikolskaia and V. B. Naumov, "The Relationship between Cybersecurity and Artificial Intelligence," *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 2021, pp. 94-97, doi: 10.1109/ITQMIS53292.2021.9642782.
10. Daniel Ventre, "Artificial Intelligence and Defense Issues," in *Artificial Intelligence, Cybersecurity and Cyber Defence* , Wiley, 2020, pp.105-186, doi: 10.1002/9781119788195.ch3.
11. Daniel Ventre, "On the Origins of Artificial Intelligence," in *Artificial Intelligence, Cybersecurity and Cyber Defence* , Wiley, 2020, pp.1-43, doi: 10.1002/9781119788195.ch1.
12. R. Vasil, F. M. Frigura-Iliasa, M. Iorga, H. Filipescu, M. Rogobete and M. Nen, "Digital Image Processing and Recognition in Industrial and Public Environments," 2019 2nd International Conference of Intelligent Robotic and Control Engineering (IRCE), 2019, pp. 37-41, doi: 10.1109/IRCE.2019.00015.
13. M. G. Rogobete, "An improvement of the time method for signal approximation. Electrocardiogram case study," *2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2022, pp. 1-7, doi: 10.1109/ECAI54874.2022.9847427.
14. V. Marascu, C. Stancu, V. Satulu, A. Bonciu, C. Grisolia, G. Dinescu, Material erosion and dust formation during tungsten exposure to Hollow-Cathode and Microjet Discharges, APPLIED SCIENCES-BASEL, Volume: 10, Issue: 19, Article Number: 6870, Published: OCT 2020. DOI: https://doi.org/10.3390/app10196870.

MACHINE LEARNING IN THE CONTEXT OF CYBERSECURITY

Stefania L. Nita

Department of Computers and Cybersecurity, Military Technical Academy "Ferdinand I", Bucharest, Romania, stefania.nita@mta.ro

***Abstract**: In this paper, we will discuss machine learning in the context of cybersecurity, focusing on data science for cybersecurity, where the data is collected from different sources that are relevant to cybersecurity. The current work will bring into discussion various research challenges, which are open for improvements, and point out the most challenging future research directions. Altogether, the purpose is not limited to discussing data science within the cybersecurity context and relevant methods/algorithms, but also to focus on the applicability of taking the most intelligent decisions based on data to protect the systems against cyber-attacks.*

***Keywords**: Machine learning, Artificial intelligence, Cybersecurity, Cyber risk management*

Introduction

The field of cybersecurity is complex and dynamic. In the last two years, cyber-attacks have intensified massively, these being facilitated by the move of many activities to the online environment, due to the COVID-19 pandemic. Thus, with a wide range of activities and such a large amount of data moved online, more security breaches than normal were created or found. This is shown by statistical reports released by different specialized organizations. For example, a report by the European Union Agency for Cybersecurity (ENISA) published in July 2022 shows that monthly, through ransomware, the attackers steal more than 10 terabytes of data and in 95.3% of cases it is unknown how attackers gained initial access to the targeted organization [1]. Another report released by the Identity Theft Research Center shows that the year 2021 has been a record-breaking year, with the number of data breaches compared with the end of the third quarter of 2020, exceeding by 17% [2]. It is predicted that by 2025 the costs of ransomware attacks will reach $10 trillion [3]. On the other hand, Capgemini Research Institute shows in the report [4] that 61% of organizations are not able to identify critical threats without artificial intelligence and machine learning and 69% of them consider that artificial intelligence is critical in responding to cyber-attacks.

As technology advances, the methods of protection against cyberattacks become better. On the other hand, through the advancement of technology, cyberattacks are becoming more complex and sophisticated, too. Therefore, businesses need to stay on top of the most recent trends if they want to protect themselves from cyberattacks. Among ones of the most relatively new ways to do this is incorporating data science within digital protection techniques. Data science is the process through which new knowledge is discovered by drawing conclusions from a set of unprocessed data. One of the strongest tools in the data scientist's arsenal for this strategy is machine learning.

Cybersecurity offers guidelines, procedures, instruments, and strategies for safeguarding digital information against unauthorized use, access, or knowledge. Depending on the specific work, there are various reasons why protecting an organization's data and digital infrastructure is important. Machine learning can be used to train security models and systems to look for potential security flaws or breaches. Machine learning can be used in a variety of cybersecurity domains, for example, to improve security processes and make it simpler for security analysts to quickly identify, prioritize, deal with, and remedi-

ate new attacks. This will help security analysts better understand past cyber-attacks and develop appropriate defense responses.

Taking these into consideration, the paper aims to present the basics of machine learning techniques and point out where they can be used in cybersecurity. The rest of the paper is organized as follows: the next section presents basic information about machine learning. In Section 2 we will present use cases of cybersecurity tools and techniques that incorporated machine learning algorithms, while in Section 4 we will present adversarial machine learning techniques. Lastly, we will present the conclusions of the paper.

Machine Learning

In this section, we present basic information about machine learning, covering the types of machine learning and the processes included in machine learning techniques [5]. Machine learning is a branch of artificial intelligence that uses algorithms to find patterns in data. As more data is gathered and becomes historical data, the algorithm modifies itself to make predictions that are more and more precise.

A machine mainly needs three elements so it can learn: datasets (similar entities/values are grouped as one entity), which can be structured or unstructured, features (characteristics of the data), which are established regarding the purpose of the analysis, and algorithms (collection os steps/rules used in problem-solving).

Supervised and unsupervised learning are the two different categories of learning methods used in machine learning. It is referred to as supervised machine learning when models are trained on data that has already been tagged, so the input is labeled and it is known the corresponding output. Unsupervised machine learning extracts patterns from a dataset by analyzing it without using prior classifications, so the input is not labeled. Another type of learning is a combination of these two, namely semisupervised learning, in which some data is labeled and other data is not labeled. And lastly, there is reinforcement learning, a type of learning based on feedback: reward score when the machine takes the right decision and punishment score when the machine takes a bad decision. As a parallel with the human learning process, supervised learning is related to experience, while unsupervised learning is related to instinct. Two of the common uses of machine learning are data classification and data clustering. Having some labeled initial data and knowing which is the output, the algorithm should classify correctly new previously unknown entries (classification). Having the initial raw data and knowing nothing about it, the algorithm should figure out how to cluster the data, i.e. how to group entries with similar characteristics (clustering).

A larger family of machine learning techniques built on artificial neural networks and representation learning is deep learning. Unsupervised, semi-supervised, and supervised learning are all possible approaches when used with deep learning. In deep learning, artificial neural networks have multiple hidden layers, while a traditional artificial neural network consists of only one layer.

Machine learning involves several processes, as follows:

Data collection. According to the purpose of the machine learning system, the raw data is collected. In other cases, organizations own a bunch of raw data and want to gather some insights from it.

Data preparation. The raw data is cleaned or features are extracted in order to be used in the analysis process.

Choosing the model. According to how the input data looks (for example, labeled or unlabeled) and with the purpose of analysis, a machine learning model is chosen (supervised, unsupervised, semi-supervised, or reinforcement).

Training the model. Mainly, the model is applied to the input data.

Evaluating the model. If the training process reaches a high level of accuracy, then it can be applied to new previously unknown entries, otherwise, the next phase is required.

Parameter tuning. If the training process does not reach the desired level of accuracy, then the parameters of the model are adjusted until the desired degree of accuracy is obtained.

Predictions. Once the desired degree of accuracy is achieved, the model can be applied to new previously unknown entries.

However, once the new entries become historical data, the model can be tested or retrained from time to time.

Use of Machine Learning in Cybersecurity

Using open-source software [6] or proprietary third-party datasets [7], machine learning can be applied to cybersecurity to draw conclusions from current data, for instance, when vulnerabilities are most likely to develop or when attackers are most likely to initiate attacks. We may create and put into use solutions for malware detection, antiviruses, identifying zero-day vulnerabilities, and digital forensics that use machine learning algorithms. Building a machine learning pipeline begins with deciding what should be measured. For instance, using machine learning in cybersecurity is driven by the desire to stop Denial-of-Service (DoS) attacks [8] or count the number of spam or virus-infected emails sent daily. The next stage is to figure out how to arrange the data so that it has as many useful characteristics as is practical for the study. Samples of emails from public servers or datasets can be labeled based on their headers, which will then be used further in the training process. More data to train the model leads to a higher degree of accuracy. Finally, utilizing patterns discovered in the dataset, the machine learning system is trained to differentiate between spam and malware information. Both labeled and datasets are used in the training phase. This technique functions really well in antivirus software. Another and appealing (theoretical and real-world) solutions are suggested [9], as well as [10] which includes a good space performance.

Generally, supervised machine learning covers methods of classification and regression, which are used in cybersecurity to categorize things like network attacks or predict future behaviors, such as a network's behavior. The principal applications of supervised learning are in intrusion detection systems. For example, in [11] the authors use supervised learning for an intrusion detection system based on a Multi-layer perceptron Neural Network. Another result in this direction is achieved in [12], where the authors suggest a novel and straightforward black-box attack technique called the brute-force attack method (BFAM) to more accurately assess how well machine learning-based cybersecurity systems can withstand adversarial cases, analyzing algorithms as linear regression. Other cybersecurity studies that involve supervised learning are [13]-[15].

Unsupervised learning is used to discover patterns and hiding knowledge structures in processed data. In cybersecurity, unsupervised learning can be used to detect attacks, such as malware. Clustering, which uses methods to find hidden insights within raw data, is the primary unsupervised learning methodology used in cybersecurity. A result in this direction is presented in [16] in which the authors use clustering methods, and the authors provide a way for choosing security features based on an importance score. Another result in this direction is achieved in [17], where the authors present CAMLPAD, a solution that instantly determines whether a certain environment is in danger of a breach resulting from the existence of anomalies by processing a range of different types of cybersecurity datasets in real-time using algorithms like isolation forest or k-means clustering.

Generally, machine learning can be used in cybersecurity in the following areas: SMS scams [18], securing mobile endpoints [19], enhancing human analysis and safeguarding against human errors, antivirus software and malware detection (for example, BitDefender[1], ESET[2], Avira[3], Cylance Protect[4], etc.), email monitoring [20], against bots [21], network threat detection [22], and threat mitigation [23].

[1] https://www.bitdefender.com
[2] https://www.eset.com
[3] https://www.avira.com
[4] https://www.blackberry.com/us/en/products/cylance-endpoint-security/cylance-protect

Other studies [24], [25] propose cybersecurity frameworks based on artificial intelligence and machine learning.

However, there are several challenges when implementing a cybersecurity system that uses machine learning: security games (this technique usually helps to prove the security of a proposed system and it is played between an attacker and a challenger, but it is specific for a certain attack, not covering the rest of the potential attacks), absence of tagged data (data is gathered from different resources and often these are unstructured and not labeled, meaning additional work needs to be made in order to bring the data to a "good" form), or transferring an efficient defense strategy from one domain to another.

Adversarial Machine Learning

In the previous sections, we saw that machine learning can be applied in many areas of cybersecurity and brings value and great results in this direction. The development of technology helped to solve many problems and brought innovative solutions. On the other hand, the technological advance can also be used for negative purposes by attackers or malicious users. In this section, we will see the other edge of machine learning in the form of adversarial machine learning. The context is simple and can be applied not only in the field of cybersecurity but in any other field that uses machine learning models. The scenario is as follows: the steps described in section 2 were followed to find the right model for the problem we want to solve. But in this case, how can we protect our model? How can we prevent situations in which the model is intentionally misled, so that the obtained results will not reflect reality? In such situations, adversarial machine learning intervenes. In other words, adversarial machine learning aims to trick the machine learning model by providing deceptive input data. An example is given in [26], in which the authors present an example in which they created the impression of a line on the road by placing three stickers there, tricking a Tesla Model S into changing lanes and driving into oncoming traffic. The car's computer vision read the stickers as indicating that the lane was leaning left and therefore directed the vehicle in that direction. When the machine learning model is compromised the best solution is to suspend it, but in reality, this is not possible for all machine learning models due to the specificity of the systems in which it is applied [27].

Common adversarial machine learning attacks are [28]:

- *Poisoning attacks*. Attacks that poison training data are intended to make a learning model make costly errors during testing. The two types of poisoning attacks are targeted (it can lead to a learning model misclassifying a certain kind of valid emails, for example) or nontargeted (decreases a learning model's accuracy).
- *Evasion attacks*. This is the most frequent type of adversarial attack because generally, the attackers do not have access to the training phase. Therefore, they create adversarial samples to deceive learning algorithms or trick classifiers into misclassifying the injected data during testing.

Besides these, there are other types of attacks on the machine learning model that are more sophisticated and can cause great damage. A comprehensive study related to recent adversarial machine learning is given in [29]. Therefore, when working with machine learning models, an extremely important thing is the protection of the model itself.

Conclusions

We have seen that machine learning is a trending technology nowadays, which has applications in many domains, from medicine to the arts. The cybersecurity domain is no exception and we have seen lately cybersecurity approaches that incorporate machine learning models. In this paper, we discussed about machine learning basics and we have seen where it can be applied in cybersecurity. Also, an important aspect is the security of the model itself, a fact that brought into discussion the branch called adversarial machine learning.

References

1. *ENISA Threat Landscape For Ransomware Attacks* (2022). https://tinyurl.com/4ztmnwh5
2. *Number of Data Breaches in 2021 Surpasses All of 2020* (2021). https://tinyurl.com/2p9d5kpn
3. Dossett, J. (2021). *A timeline of the biggest ransomware attacks.* https://tinyurl.com/2p8p7ub5
4. Reinventing Cybersecurity with Artificial Intelligence (2019). https://tinyurl.com/3fdv9jkr
5. Mahesh, B. (2020). Machine learning algorithms-a review. International Journal of Science and Research (IJSR).[Internet], 9, 381-386.
6. Sennaike, O. A., Waqar, M., Osagie, E., Hassan, I., Stasiewicz, A., Porwol, L., & Ojo, A. (2017, September). Towards intelligent open data platforms: Discovering relatedness in datasets. In 2017 Intelligent Systems Conference (IntelliSys) (pp. 414-421). IEEE.
7. Haas, L. (2017, April). Leveraging Data and People to Accelerate Data Science. In 2017 IEEE 33rd International Conference on Data Engineering (ICDE) (pp. 4-4). IEEE.
8. Fadhlillah, A., Karna, N., & Irawan, A. (2021, January). IDS Performance Analysis using Anomaly-based Detection Method for DOS Attack. In 2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS) (pp. 18-22). IEEE.
9. Chavan, A., Kerakalamatti, K., & Srivastva, S. (2021, June). Implementation of Portable Antivirus System using Signature-based Detection and Heuristic Analysis. In 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 1481-1486). IEEE.
10. Min, B., Yoo, J., Kim, S., Shin, D., & Shin, D. (2021). Network anomaly detection using memory-augmented deep autoencoder. IEEE Access, 9, 104695-104706.
11. Mebawondu, J. O., Alowolodu, O. D., Mebawondu, J. O., & Adetunmbi, A. O. (2020). Network intrusion detection system using supervised learning paradigm. Scientific African, 9, e00497.
12. Zhang, S., Xie, X., & Xu, Y. (2020). A brute-force black-box method to attack machine learning-based systems in cybersecurity. IEEE Access, 8, 128250-128263.
13. Teixeira, M. A., Salman, T., Zolanvari, M., Jain, R., Meskin, N., & Samaka, M. (2018). SCADA system testbed for cybersecurity research using machine learning approach. Future Internet, 10(8), 76.
14. Chesney, S., Roy, K., & Khorsandroo, S. (2020, September). Machine learning algorithms for preventing IoT cybersecurity attacks. In Proceedings of SAI Intelligent Systems Conference (pp. 679-686). Springer, Cham.
15. Seneviratne, S., Shariffdeen, R., Rasnayaka, S., & Kasthuriarachchi, N. (2022). Self-Supervised Vision Transformers for Malware Detection. arXiv preprint arXiv:2208.07049.
16. Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning based cyber security intrusion detection model. Symmetry, 12(5), 754.
17. Hariharan, A., Gupta, A., & Pal, T. (2020, March). Camlpad: Cybersecurity autonomous machine learning platform for anomaly detection. In Future of Information and Communication Conference (pp. 705-720). Springer, Cham.
18. Prusty, S. R., Sainath, B., Jayasingh, S. K., & Mantri, J. K. (2022). SMS Fraud Detection Using Machine Learning. In Intelligent Systems (pp. 595-606). Springer, Singapore.
19. Sjarif, N. N. A., Chuprat, S., Mahrin, M. N. R., Ahmad, N. A., Ariffin, A., Senan, F. M., ... & Saupi, A. (2019, October). Endpoint Detection and Response: Why Use Machine Learning?. In 2019 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 283-288). IEEE.
20. Ahmed, N., Amin, R., Aldabbas, H., Koundal, D., Alouffi, B., & Shah, T. (2022). Machine learning techniques for spam detection in email and IoT platforms: analysis and research challenges. Security and Communication Networks, 2022.

21. Heidari, M., James Jr, H., & Uzuner, O. (2021, April). An empirical study of machine learning algorithms for social media bot detection. In 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS) (pp. 1-5). IEEE.
22. Mahindru, A., & Sangal, A. L. (2021). MLDroid—Framework for Android malware detection using machine learning techniques. Neural Computing and Applications, 33(10), 5183-5240.
23. Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. Journal of Cybersecurity and Privacy, 2(3), 527-555.
24. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 7(1), 1-29.
25. Mihailescu, M. I., & Nita, S. L. (2023). Towards Data Science for Cybersecurity: Machine Learning Advances as Glowing Perspective. In Proceedings of SAI Intelligent Systems Conference (pp. 26-48). Springer, Cham.
26. Tencent Keen Security Lab. (2019). Experimental security research of Tesla autopilot. https://tinyurl.com/ycky7rjj
27. Kumar, R. S. S., Nyström, M., Lambert, J., Marshall, A., Goertzel, M., Comissoneru, A., ... & Xia, S. (2020, May). Adversarial machine learning-industry perspectives. In 2020 IEEE Security and Privacy Workshops (SPW) (pp. 69-75). IEEE.
28. Rosenberg, I., Shabtai, A., Elovici, Y., & Rokach, L. (2021). Adversarial machine learning attacks and defense methods in the cyber security domain. ACM Computing Surveys (CSUR), 54(5), 1-36.
29. Xi, B. (2020). Adversarial machine learning for cybersecurity and computer vision: Current developments and challenges. Wiley Interdisciplinary Reviews: Computational Statistics, 12(5), e1511.

ACHIEVED RESULTS FROM PROJECTS UNDER ERASMUS+ KEYACTION 02

Dilyan I. Dimitrov, Linko G. Nikolov, Krasimir Slavianov, Miroslav G. Nedelchev

Artillery, Air Defense and Communication and Information System faculty, NMU "V. Levski" Shumen, decanat@aadcf.nvu.bg

***Abstract**: Achieved results from projects "Digital Competences for Improving Security and Defense Education (DIGICODE) - project NO 2020-1-PL01-KA226-096192", „Implementation of digitalization in defence higher education (DDHE) 2020-1-RO01-KA226-HE-095411 and*

***Keywords**: Erasmus program, digital competence, higher education, technical semester*

Introduction

In this paper are given the achieved result from three Erasmus projects under the second action – Erasmus + Key action 02. The main idea of the projects is to support digitalization in higher education especially in military area and create a common modules and common semesters.

1. Digital Competences for Improving Security and Defense Education - DIGICODE

The project DIGICODE lasts 2 years, starting on 30.04.2021 and end term on 29.04.2023. The aim of the DIGICODE project is to improve the security and defence education quality by using digital tools in the didactic activities and by developing digital competences of teachers. The main objectives of the project are: to conduct a survey and collecting detailed information in a group of students and lecturers from international universities and to conduct a comparative analysis in order to compare the processes, strategies, and methods used by the respondents and to identify the best practices and competencies ensuring safe and effective online teaching in Security and Defence; to develop a Best Practices Handbook, including a collection of best practices and solutions used by universities in the times of COVID-19; to develop a teacher tool-kit including a toolkit for digital competences for teachers in the Security and

Defence field and open online training courses to support teachers and trainers in using specific digital learning environments for education, different kinds of digital tools, and in adopting innovative and adaptive methodologies like problem solving, problem-based teaching, learning by doing, formative and data-driven automatic assessment with interactive and immediate feedback, collaborative learning, team working; to design and develop a curriculum for a summer school "Systems for Command and Control in Security and Defence Field" which plays a critical role in helping teachers to have an integrated vision of the security and defence education system; to apply the teacher tool-kit prepared especially for the digital education in order to explain the systems functionality, replacing the classic laboratory activities; to improve the digital competences and to improve the communication skills in online environment of at least 16 teachers and 16 students from security and defence education institutions; to build the critical mass of knowledge and resources in partner institutions in order to foster the use of digital education in military academies.

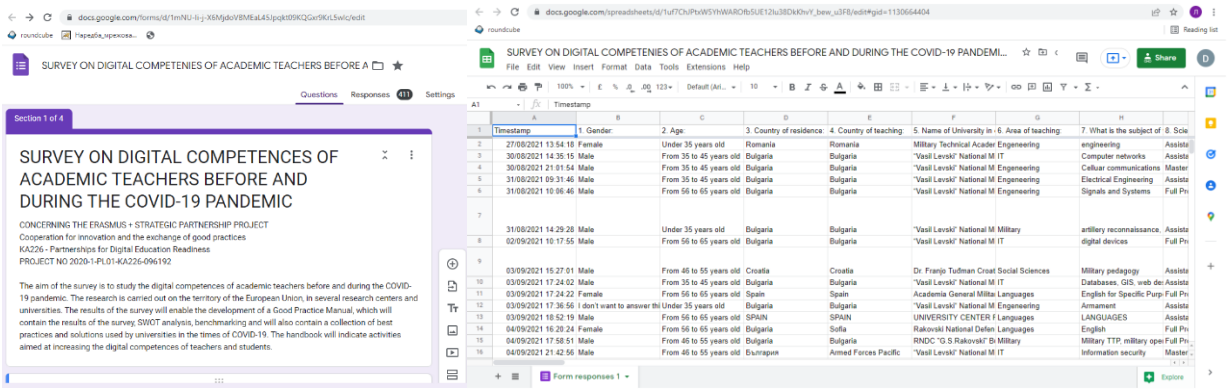


Figure 1: Survey questions

Until now, 3 Intellectual outputs (IO) are finished:

IO-01 – Data collection about the best practices already adopted

before and during the Covid19-Crisis – a survey is prepared, analyzed and the results are being adopted during the project pilot schools;

IO-02 – eacher tool-kit for developing digital competences in Security

and Defence Education - an online teachers' tool-kit is developed and uploaded, available on https://www.digicode.unito.it/login/index.php, yet credentials are required for authorized access control.

IO-03 – Cybersecurity requirements for e-learning platforms in digital

Security and Defence Education – a cybersecurity policy is being developed after cyber tests and analysis.

For IO-01 the work in brief may be presented as preparation of survey questions, disseminating the survey amongst partner institution teachers and others, connected to education system and to security and defence; a statistical analysis of the survey results (a SWOT analysis); benchmarking the characteristics and description of best approach.

As a further output, two scientific papers were published in worldwide indexed conference "eLSE" (https://www.elseconference.eu/pages/view?page=indexed_by , ISSN 2066-026X):

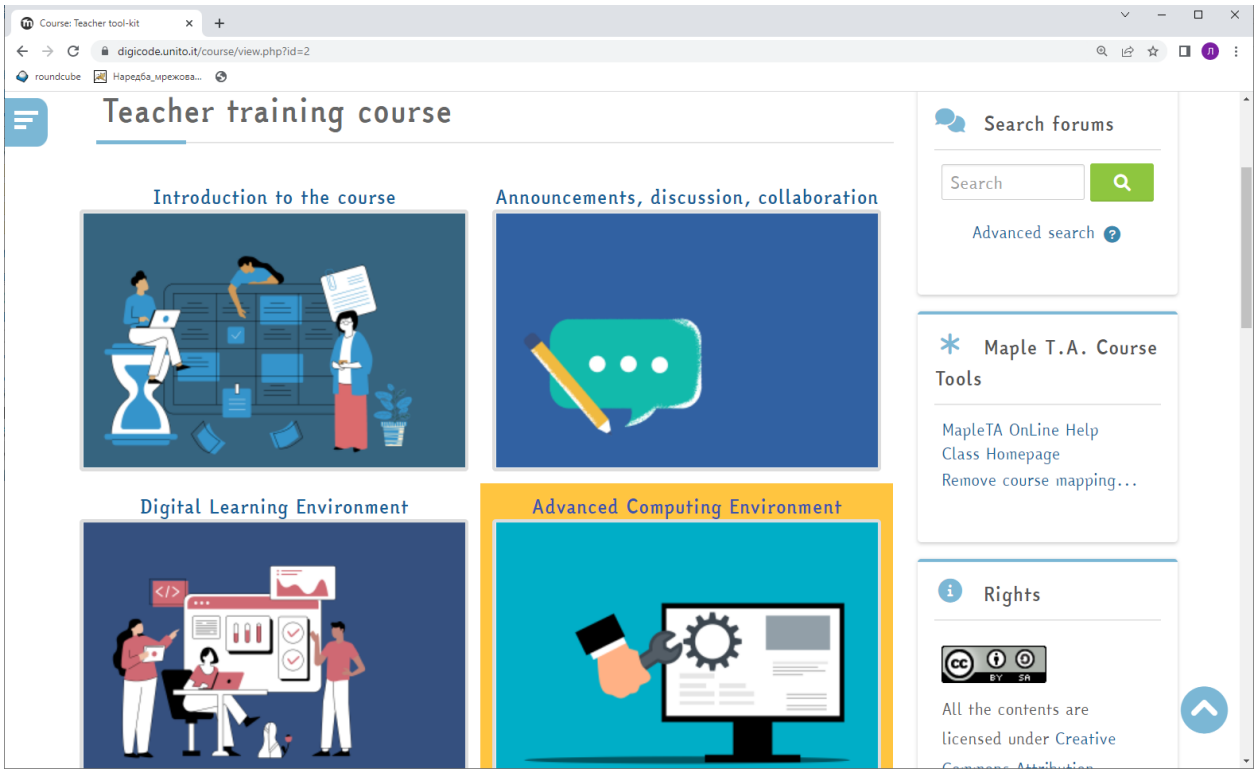


Figure 2: Teaching training course

Teachers' digital competences before and during the covid-19 pandemic for the improvement of security and defence higher education;

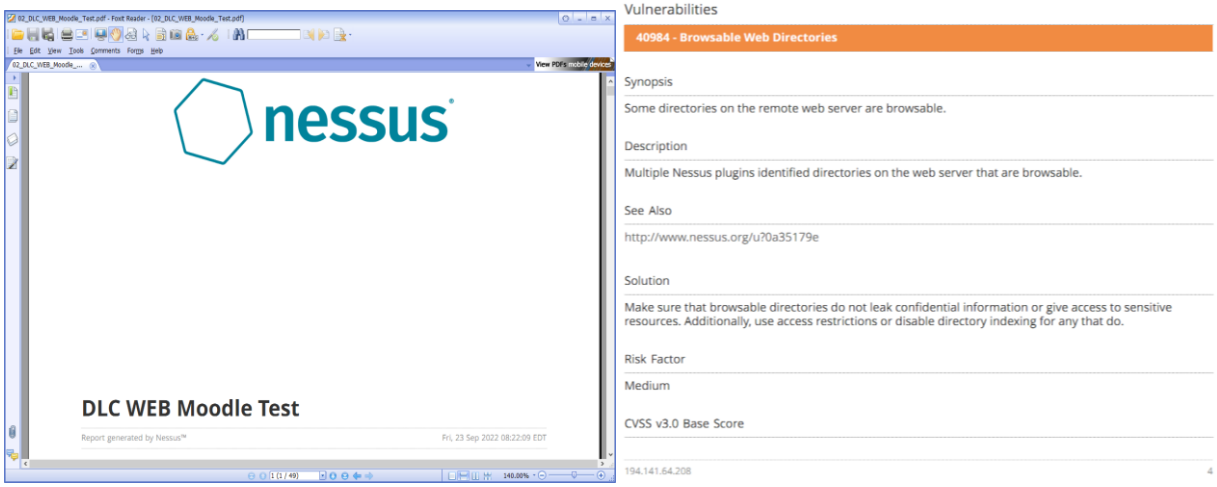


Figure 3: Cyber tests

Advantages and disadvantages of digital remote education in the security and defence contexts.

For IO-02 the result is a platform for e-learning with enhanced capabilities – Maple software for mathematical calculations and Mobius automatic assessment system. The proposed tool-kit is focused on helping students for autonomous problem solving skills acquirement and team work in online environment.

The IO-03 was prepared in 3 consequential phases:

1. creation of methodology for cyber tests;
2. performing cybertests over real implemented e-learning platform;

3. analysis of the performed cybersecurity tests and preparation of Cybersecurity policy.

The Methodology was offered for publication in the DTF2022 conference in Shumen, Bulgaria. The cyber tests were made with a variety of software. The cybersecurity policy will be the final result after the analysis of weak infrastructure points.

2. Implementation of digitalization in defence higher education - DDHE

In the 21st century the entire world as well as every individual state is faced with numerous challenges, including hybrid threats. The nature of these threats has forced states to revise their traditional systems of defense and state security. According to "Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization", the modern security environment encompasses a broad and changing set of challenges to the security of territories and populations. To provide their security, Member States must ensure an appropriate level of defense education. Consequently, graduates have to acquire the ability to respond to natural disasters, critical infrastructure failures and military threats. This principle was confirmed in Art. 3 of the NATO Treaty as developing the individual and collective capacity of society to resist and quickly recover from these disturbances, combining civil, economic, commercial and military factors.

The pandemic period we have been going through has highlighted the fact that we are never sufficiently prepared. It has been shown that not all teachers have sufficient digital skills but also that not all educational resources are suitable for online use.

Military universities train a relatively small number of cadets for specific tasks and their e-learning platform were not well prepared for providing practical exercises and trainings.

Another weak point is the difficulty of transferring practical laboratory activities in digital format and the development of these classes compared to the teaching materials dedicated to real classes.

This reality was felt more acutely when many military universities were forced to improvise systems and methods dedicated to online education. The existence of this platform proves strong need for electronic teaching materials (course, laboratory/workshop educational resources) dedicated to all disciplines in the curricula

All these must be thought in the context in which the pandemic period is prolonged (threat) and the teaching/learning program will be carried out online.

The improvisations made failed to meet the necessary standards for obtaining high scores in the teaching/ learning process. This is one of the weaknesses discovered throughout all interval of time by all partners in project № 2020-1-RO01-KA226-HE-095411 „Implementation of digitalization in defence higher education (DDHE) ".

Project scopes and activities

Meanwhile modern technologies results in constant improvement and searching for new solutions in the field of security studies. For example many platforms for distance learning were opened for free use enabling effective online education.

In this context, universities are trying to find their own way to be up to date with new teaching/learning methods.

After analysis, follow needs were identified:

Transfer in digital format of all materials and auxiliary materials destined to lectures.

Introduction of a section dedicated to electronic books in university libraries.

Development of IT applications to help users acquire practical skills.

To cover these needs it was proposed:

Developing teachers' skills for using IT systems so that each teacher can create digital materials needed for their course.

Co-opting a librarian, an IT specialist from each university partner in the project for the development of this goal.

Introduction of VR (virtual reality) or AR (augmented reality) systems for practical applications.

Target groups are those of teachers and students.

A main beneficiary for the first one is opportunity to participate in such a project and involvement in its necessary scientific research. That helps them to develop professionally by obtaining the skills needed to use high-performance IT systems. Regardless of the level we are talking about, obtaining these skills is a key action for the professional development of each teacher.

The professional development of teachers, the adaptation and the design of teaching materials to online teaching methods but especially their achievement at high standards led to the consolidation and improvement of higher education. This translates into continuous development and openness to new synchronous and asynchronous teaching, especially virtual (VR) and augmented reality (AR) technologies.

For students it was the opportunity to participate in the project and develop their ability to understand the process of developing teaching materials and scientific research.

Scope of project № 2020-1-RO01-KA226-HE-095411 „Implementation of digitalization in defence higher education (DDHE)".

Its multidimensional, multidisciplinary and transnational approach.

Multidimensional - through the proposed objectives that start from the design of course support in digital format and reach the use of VR or AR technologies for online laboratory activities.

Multidisciplinary - through the diversity of disciplines for which teaching and technical materials will be designed, some of the disciplines bearing a strong technical profile while others are of humanistic/management profile.

Transnational – due to the universities involved in the project

Introduction of VR or AR systems in teaching/learning processes is an innovation in the education system.

Simulation programs that can be used in different technical disciplines in the curricula, the intensive use of e-learning platforms and conduct of questionnaires/interactive exams/online assessment are the way to verify the use of educational resources developed in the project by teachers, librarians and students.

Teaching materials have been written in English. Finally each discipline will have educational resources for their teaching activities (lecture/workshop/laboratory), in a ratio corresponding to the universities' existing study plans.

In case of laboratory activities VR or AR applications have been developed.

Co-opting university librarians for introducing digital courses in university libraries and creating a common platform where project materials can be accessed.

Co-opting students in the research/development process of IT systems, VR or AR applications.

Development of AR or VR applications for teaching or practical activities.

Impact and satisfaction studies, questionnaires to observe and verify the achievement of specific objectives but also the degree of satisfaction.

Visibility of the project by disseminating the project results creating a website for this project and creating other dissemination materials.

Organization for achieving all these goals includes:

Management and administration activities;

Selection of human resources with care and transparency;

Meetings of the steering committee elected from the academic teams to serve to the real-time management of the project and to set corrective measures;

Organizing virtual mobility in order to verify implementation of the project;

Multiplier events (workshops, seminars).

-Dissemination of the project results that aim to adopt EU directives for high quality and inclusive digital education and training through and good practices ;

Figure 4: DDHE cycle

For each stage, specific sub-activities are performed as it shown on fig.4:

Planning each stage of the project/proposed activities - Institutional Managers under the coordination of the Project Manager.

Designing objectives - Project Teams under the coordination of the Institutional Managers.

Project implementation phase - Project Teams under the coordination of the Institutional Managers and a person responsible for each discipline.

Assessment of partial results or completion of an activity - Project Teams (self-assessment/activity report), Institutional Managers (assessment reports), Project Manager (in the assessment process)

Testing the partial or final results through demo lessons – it provides feedback to improve the level of project quality.

Dissemination of partial and final results of activities throughout the project - this category include actions and papers that were published in various conferences, but also actions to design the project's website page and the project's logo.

Completion and opening of the digital library to the universities in the project but also to their partners.

The activities for monitoring the progress of the project are based on the qualitative and quantitative accomplishment indicators of the planned activities.

3. European Common Technical Semester for Defense and Security - EuCTS_DS

The project EuCTS_DS lasts 2 years, starting on 01.12.2020 and end term on 30.11.2022. Considering the Amendment no 1 to the Grant Agreement No 2020-1-RO01-KA203-080375 concluded between the Coordinator and the Romanian Erasmus+ National Agency (National Agency for Community Programmes in the Field of Education and Vocational Training), the duration of the Project is 32 (thirty-two) months and it has to be implemented in the time period December 01, 2020 – July 31, 2023.

The objectives of the project (EuCTS_DS) are the development, testing and design of a new modular curriculum for the international technical semester of defense and security, at the bachelor's level, for

the European Union, as well as the development of a network of teachers with technical systems competencies for defense and security.

All member institutions of the project are accredited as state higher education institutions of national ministries of defense of each country, integrated into their national education systems, and among their missions aim to prepare future officers engineers in the field of engineering:

- Ferdinand I Military Technical Academy, Bucharest, Romania (MTA Bucharest),
- Military University of Technology, Warsaw, Poland (MUT Warsaw),
- Faculty of Artillery, Air Defense and CIS of "Vasil Levski" National Military University (NMU Bulgaria),
- Attica Greek Air Force Academy, Athens, Greece (HAFA Athens),
- Salon de Provence Air and Space Force Academy, France (FASFA France).

Basic activities:

The main activities of the project are organized in 9 work packages:

WP1 - Project management and implementation

Planning, implementation, evaluation and dissemination activities, coordinated by MTA Bucharest, based on a common work plan and action plans agreed during meetings and telephone / videoconferences or e-mail communication);

WP2 - Professional network in the field of technical systems for defense and security Establishment of professional networks of lecturers and researchers for the modules (fig. 5.):

1 - basic engineering sciences,
2 - military sciences for engineers,
3a - mechanical and aerospace engineering,
3b - electronic and computer engineering.

WP3 - Development of a curriculum for the international technical semester

Curriculum with common subjects in the EU in the field of technical systems for defense and security (fig. 6.);

WP4 - Description of the subjects of the international technical semester

Detailed description of each subject included in the curriculum;

WP5 - Preparation of teaching materials

Preparation of teaching materials (support of courses and applications prepared for use during teaching / teaching activities within the international semester);

WP6 - Interdisciplinary preparation of a research project / included in the semester program /

Teaching activities included in the international semester, using a project-based learning methodology providing competencies in various engineering fields;

WP7 - E-learning platform

Using a modern tool for sharing learning materials and supporting learning activities in the international semester;

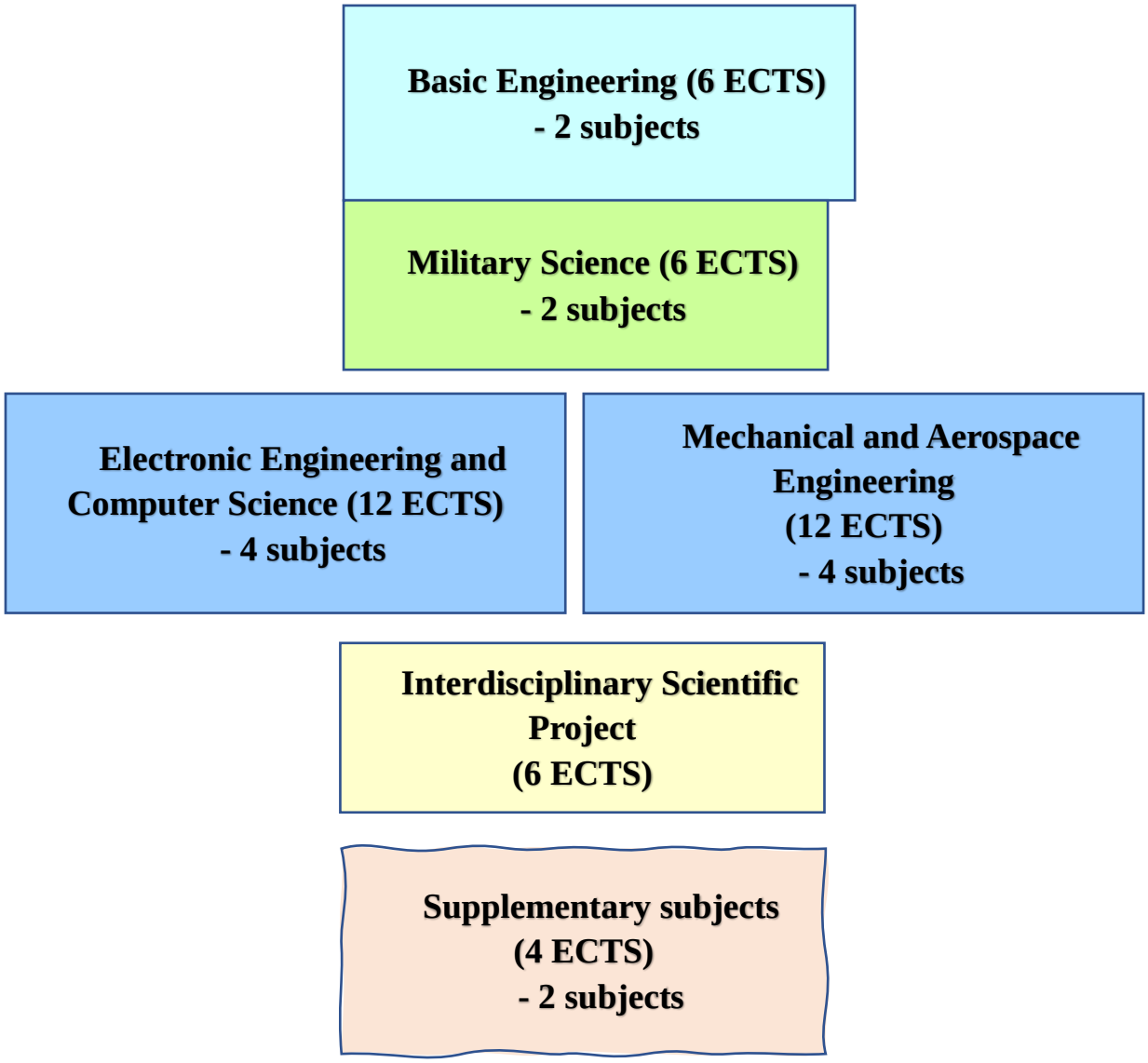


Figure 5: EUCTSDS Curriculum modules

WP8 - Teaching / learning activities for testing the international technical semester

Intensive learning activities organized to test the curriculum, subject description, teaching materials and e-learning platform prepared for the international semester;

WP9- Impact and dissemination

Dissemination activities organized to share the results of the project, including two events (conferences) to announce and promote the results.

The main goals are 6:

1. Design and development of the EuCTS_DS curriculum

Team leader: RO MTA

2. Creating a network of teachers and a set of teachers for EuCTS_DS

Team leader: FR FAFA

3. Description of subjects and educational materials for EuCTS_DS

Team leader: BG NMU

4. Methodology and guidance for the interdisciplinary research project

Team leader: GR HAFA

5. E-learning platform

Team leader: PL MUT

6. Methodology and Guide for implementation of EuCTS_DS

No.	Subjects	ECTS
1	Applied Informatics – RO MTA	3
2	Applied Automation for Engineering Systems – PL MUT	3
3	Integrated Weapon Systems – RO MTA	3
4	Common Security and Defence Policy for Technical Systems - FR FASFA	3
5a	Computer Networks – BG NMU	3
6a	Programming Languages – RO MTA	3
7a	Signal Processing – GR HAFA	3
8a	Microcontrollers – RO MTA	3
5b	Propulsion Systems – GR HAFA	3
6b	Dynamic of Flight – PL MUT	3
7b	Mechanics and Material Science – GR HAFA	3
8b	Computer-Aided-Design and Numerical Analysis – BG NMU	3
9	Interdisciplinary Scientific Project – GR HAFA	6
10	Intercultural Communication (Bulgarian/French/Greek/Polish/Romanian)	2
11	Physical Education and Sports	2
TOTAL		34

Figure 6: EuCTS_DS Curriculum

Team leader: RO MTA

Trans-national Project Meetings - 5:

During the implementation of the project (fig. 7), 5 transnational meetings will be organized with one representative from each institution, one transnational meeting at the beginning of the project and then 2 transnational meetings each year.

TPM 1. Planning of the activities under the EuCTS_DS project

Place: PL MUT

TPM 2. Evaluation of the curriculum and the network of teachers

Venue: GR HAFA

TPM 3. Description of subjects and educational materials for EuCTS_DS

Place: BG NMU

TPM 4. Interim results for intensive training programs

Venue: FR FAFA

TPM 5. Evaluation of intensive training courses

Location: RO MTA

Learning / Teaching / Training Activities:

During the implementation of the project will be organized 5 intensive training programs with the participation of teachers and students from the partners.

The target groups of this activity are teachers with competencies in the specific module for defense and security. The minimum number of participants is 6, 4 from the partner institutions and 2 from the host institution. The main goal of the activity is to test all intellectual results obtained during the project implementation, in connection with the subjects from the module of the international semester curricu-

lum. The results of the project will include products, methods, exchange of experience and more. For each discipline taught during the intensive curriculum, course provision and relevant presentations will be edited. The study materials will be provided in advance to the students and will then be published on the e-learning platform.

1. Intensive curriculum for teachers and cadets "Basic Engineering"
   Leader and place: RO MTA
2. Intensive curriculum for teaching staff and cadets "Military Science"
   Leader and place: FR FAFA
3. Intensive curriculum for teachers and cadets "Mechanical and aerospace engineering"
   Leader and place: PL MUT
4. Intensive curriculum for teaching staff and cadets "Electronic Engineering and Computer Science"
   Leader and place: BG NMU
5. Intensive curriculum for teachers and cadets "Interdisciplinary research project"
   Leader and place: GR HAFA

Multiplier Events

During the implementation of the project, two public events (conferences) will be organized, each uniting at least 70 participants: national and transnational specialists from academia, industry, MoD, research companies.

E1 European Forum of Defence and Security Technical Systems 2022

E2 European Forum of Defence and Security Technical Systems 2023

Benefits of the project

The cadets/students will have the chance of gaining experience of working in an international and interdisciplinary environment, having in the same time available the engineering part and the military science component, that is not usually available in a regular study programme that could be followed by students in Erasmus mobilities;

The teachers will benefit through the exchange of ideas and best practice in the area of technical systems for defense and security and didactical methods.

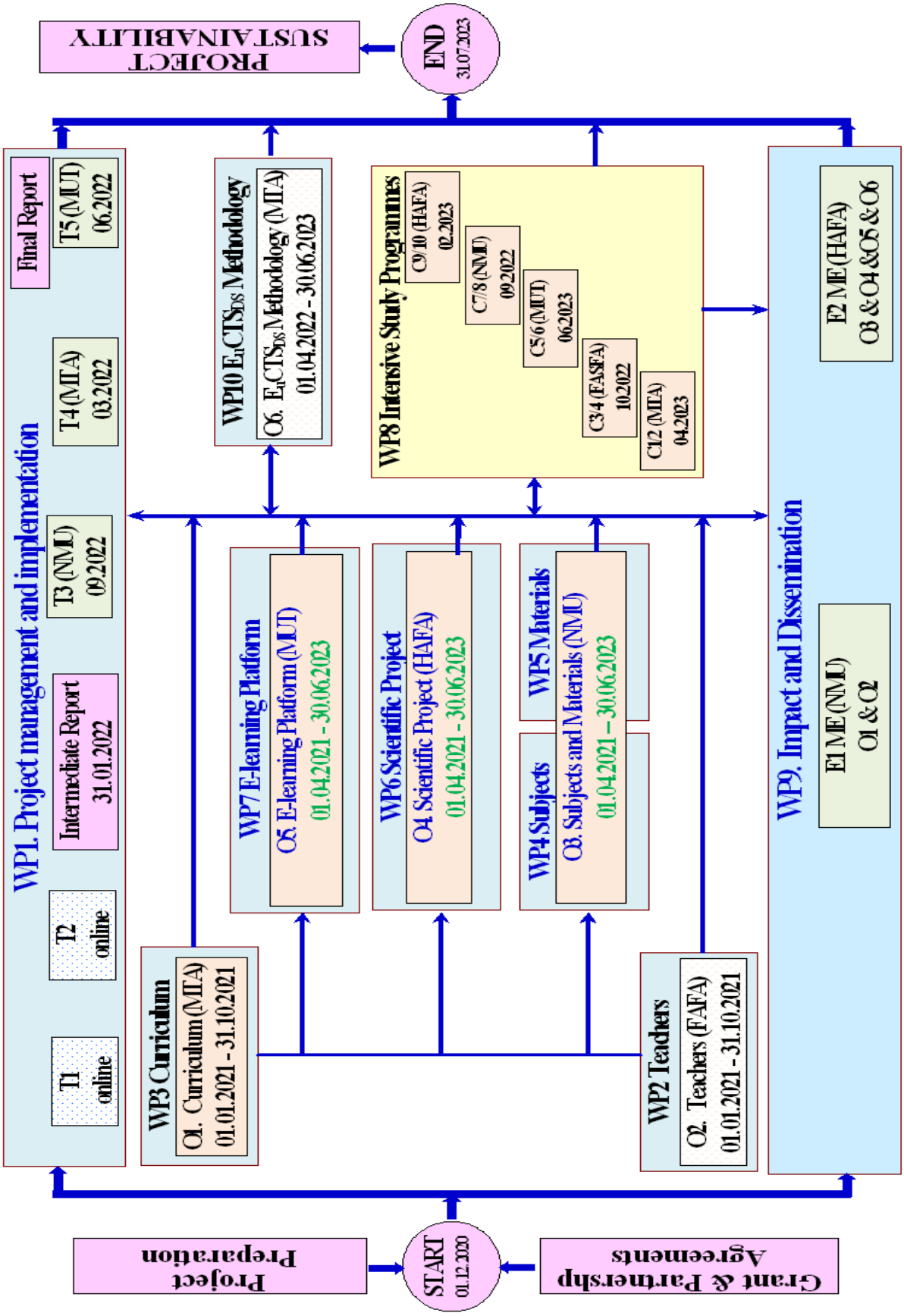


Figure 7: EuCTS_DS project activities.

The Interdisciplinary Scientific Project will provide to the teachers and students a wider perspective over the field of technical systems for defence and security and will enhance their skills in the area of didactical and pedagogical methods.

The implementation of the European Common Technical Semester for Defence and Security in each of the consortium member institutions will increase the internationalization at home and will lead to a possible future network of universities, European University for Defence and Security;

The new EuCTS_DS will facilitate creation and development of partnerships in the field of teacher and student mobility, as well as in the field of international scientific research project between the consortium members and other EU and NATO military academies.

The project will provide experience and new skills in the field of management and coordination of international cooperation projects.

References

1. NATO 2022 strategic concept, Adopted by Heads of State and Government at the NATO, Madrid, 29 June 2022
2. Sobon A., 2022, DDHE – Synchronous or asynchronous didactic in higher education, AFASES 2022, ISSN 2247-3173, pp103-106
3. https://www.elseconference.eu/pages/view?page=indexed_by/ ISSN 2066-026X

DEFENSE AND SECURITY

COLLECTING INFORMATION DURING THE RECONNAISSANCE INTO THE COMMAND SUPPORT SYSTEMS USING MODERN TECHNOLOGIES- EXPERIENCE FROM UKRAINIAN CONFLICT

Tomasz Surwiłło

t.surwillo@akademia.milpl;, War Studies University,
al. Gen. Chruściela – Montera 103, 00-910 Warsaw, Poland

Abstract: *Modern IT support is a must in Armed Forces in any country that is willing to be able to conduct in other than safe conditions. The article concerns recognition in command support systems with the use of modern technologies.*

Keywords: *Command Support System, Military Decision Making Process, Training System, NATO, COP.*

Introduction

The analysis of the available literature related to all threats to international security should begin with the realization of the conditions that conflicts are a consequence of conscious decisions of people in power. War and the ways in which it is conducted are tools that evolve along with the formation of a new international order. The conflict in Ukraine and the related to that topic of the article *"Reconnaissance into the Command Support Systems using modern technologies- experience from Ukrainian conflict"* is to make the average *"Smith"* aware that reconnaissance information equals to be or not to be. Information at the present time is something without which we cannot imagine normal functioning in the digital world. The effectiveness of the use of new technologies, including mainly IT tools, depends on the method of organizing IT support for the command process.

Historical background – creation Department of Communications and Teleinformatics

The Department of Communications and Teleinformatics is a unit of the Institute of Information Activities (I^2A) of the Military Faculty (MA) of the War Studies University (WSU) in Warsaw. The Department continues the traditions of the former Department of Communications, Department of Communication Systems and Information Technology, Department of Teleinformatics Systems and Department of Teleinformatics.

It was established as a result of the restructuring and transformation of the Teleinformatics Department on the basis of Ordinance No. 12 of the Rector-Commandant of ASzWoj of 22/03/2022. Its creation is an expression of the desire to more fully use the capabilities of modern communication and ICT systems in the military command process. The department conducts a broadly developed teaching, scientific and journalistic activity, the main focus of which is the issues of teleinformation systems, communications and IT in military applications and the development of military teleinformation, telecommunications and IT systems. At the time the article was written, there were 4 employees working in the department.

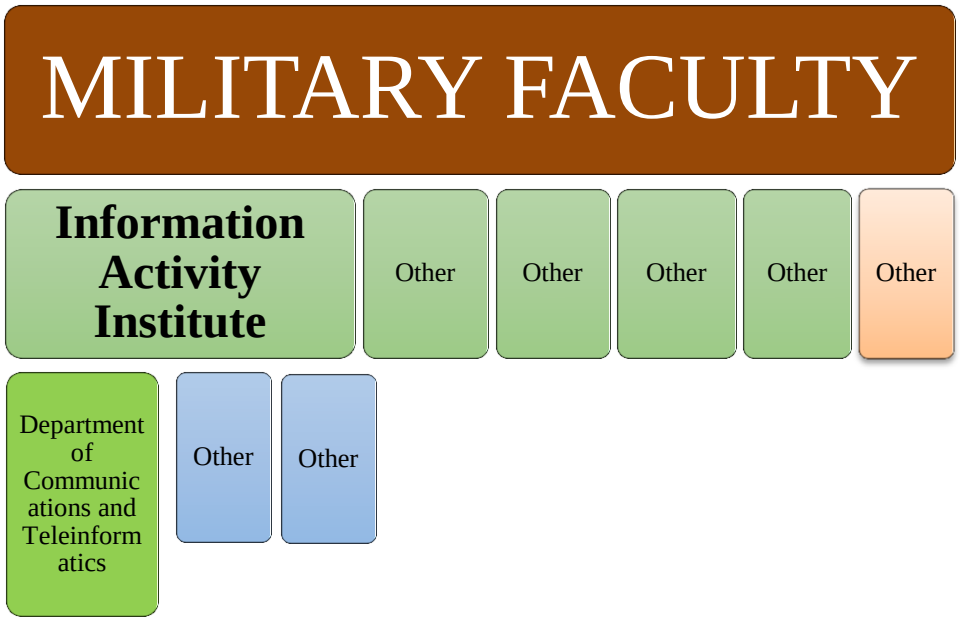


Fig. 1. Structure Department of Communications and Teleinformatics
Source: Author's picture.

Fig. 2. Entrance to the CSS Laboratory in Polish Armed Forces in 2016
Source: Author's picture.

The causes of the conflict in Ukraine from the point of view of modern technologies

When considering the causes and reasons for the Russian-Ukrainian conflict, its evolution in relation to the conflict of 2014 should be emphasized. The occupation of Crimea by the Russian Federation and its subsequent joining to its territory was opposed by most countries and organizations in the world. Conflict 2014. was a surprise for Ukrainians who were not prepared for the war with Russia. It should be emphasized that the time that has passed since then has not been wasted by the Ukrainian authorities. At this point, one should mention the policy pursued by the Polish government, which warned international opinion against Russia and its energy policy. This policy is aimed at the dependence of EU countries on Russian natural resources. The first action performed by the Ukrainian authorities was to increase the number of armies and partially modernize the equipment and equipment. Tensions in relations between Russia and Ukraine due to the latter's willingness to join NATO or the EU. The armed attack by the Russian Federation on Ukraine was a surprise both for the Ukrainian political elite and the local society,

and for the international community, even though it was a natural consequence of Russia's policy towards Ukraine. It was another example of starting a war without declaring it officially.

Explaining the reasons for the armed conflict in Ukraine from the point of view of modern technology, the author assumed, on the basis of the available factual material, the following reasons:

- Ukraine is part of Russia and should not exist outside of Russia;
- Ukraine is to blame for the collapse of the Soviet empire and the failures of Russia caused by it;
- Russia without Ukraine is geopolitically incomplete and cannot be reborn as a "superstate" in the international arena;
- Ukraine is the engine of modern technological thought in Russia.

The use of modern technologies allowed the Ukrainians to heroically repel the Russian invasion. Putin's troops counted on a very easy passage in Ukraine. The country was to be occupied in a few days and the Ukrainian army was completely destroyed. The realities turned out to be completely different, and the Ukrainians organized Putin's army in their country a second Afghanistan. But if not for the technological assistance from the West - such a heroic defense of Ukraine would not be possible at all.

Deliveries of intelligent weapons such as NLAW launchers, Javelin, Piorun and Krab missiles or access to American and Turkish shock drones allowed the Ukrainian army to thin the ranks of Russian soldiers unprepared for combat, who did not expect such strong resistance from the Ukrainians. The support of the American intelligence (on the basis of satellite data, to which Ukraine normally did not have access) and Elon Musk - who made Starlinks available to the Ukrainian army, through which it can continuously communicate with each other, is also very important. It is this method of communication that translates into the possibility of providing food to the population, and the Kyiv Digital application, which before Putin's invasion of Ukraine, served the inhabitants of the Ukrainian capital, among others to pay for city services and parking. The smartphone program currently popular in Kiev is used as a map showing users the closest shelters they can use, as well as places where they can stock up on the most important goods, such as food, medicines or gasoline.

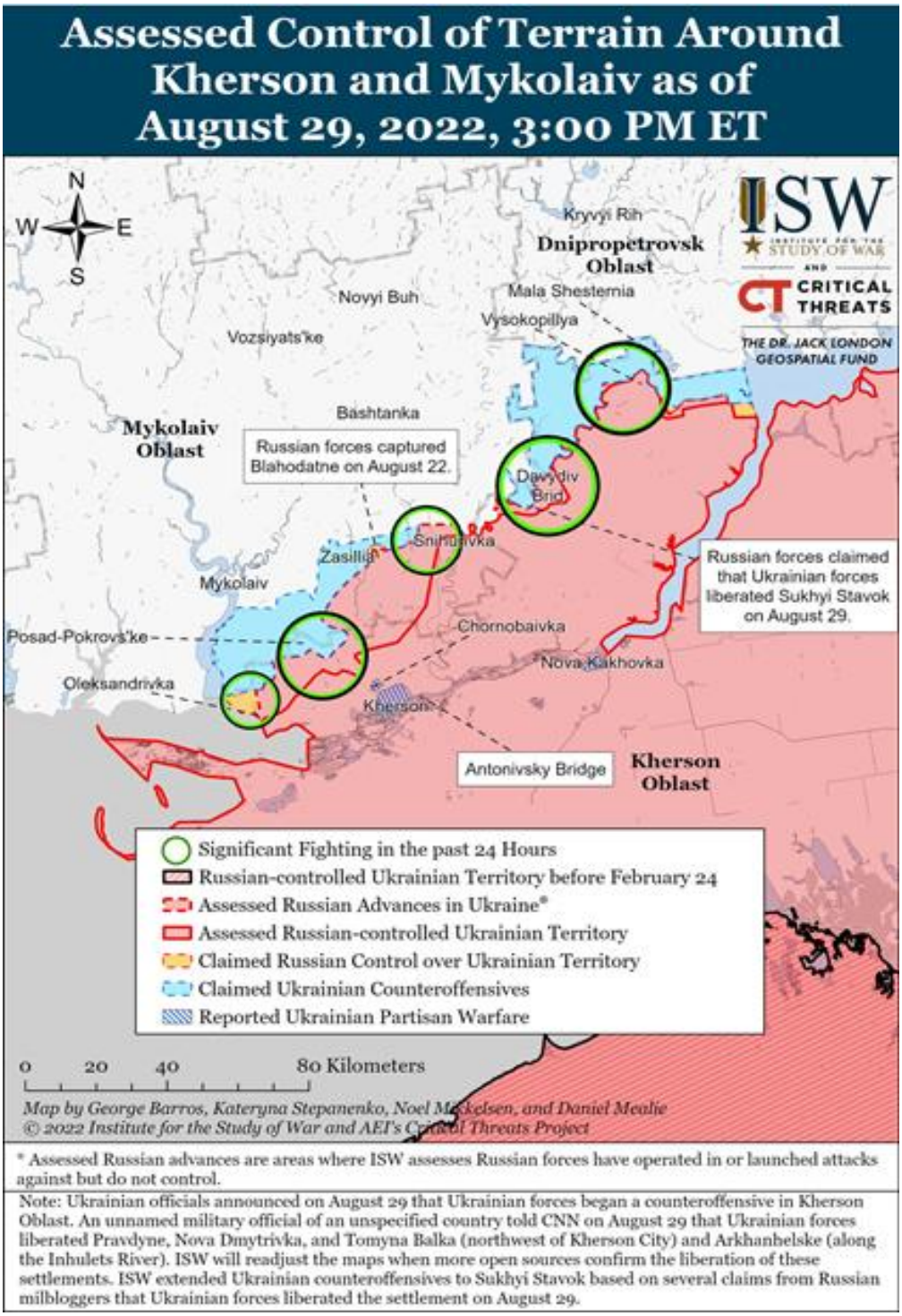


Fig. 3. Site assessment during the conflict in Ukraine
Source: https://www.polsatnews.pl/wiadomosc/2022-08-30/wojna-w-ukrainie-trwa-kontrofensywa-w-obwodzie-chersonskim-isw-pisze-o-wyzwoleniu/

Fig. 4. Results of use of modern technology during the conflict in Ukraine

Source: https://tvn24.pl/swiat/rosja-grozi-ukrainie-minister-obrony-ukrainy-moskwa-nie-sformowala-na-razie-ani-jednej-grupy-uderzeniowej-przy-granicy-5606744

IT tools used to illustrate the reconnaissance situation in command support systems

Building an information advantage on the contemporary battlefield and adopting an operational program related to the integrated command support systems and C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) operational program resulted in the need to acquire a system for the Polish Armed Forces. It includes command systems integrated with communication and reconnaissance systems, supported by information technologies. Its goal is to achieve the required operational capabilities necessary for the effective command and control of the Armed Forces of the Republic of Poland in the entire spectrum of tasks performed.

Operating in a network-centric environment, the program integrates both automated command and control systems for combat and reconnaissance means, as well as decision-making centers. To obtain a full picture of the issues under consideration, it is necessary to present the classification of information systems in NATO, where mainly acronyms or abbreviations of system names are used:

- C2IS - Command and Control Information System,
- C2ISR command and control, intelligence, surveillance and reconnaissance,
- C4 - command, control, communications and computers,

and

- C4I - Command, Control, Communications, Computers and Information,
- C4I - Command, Control, Communications, Computers and Intelligence
- C4ISR - Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance.

In the acronyms C4I and C4ISR, the term "computers" should be understood as "automated", because automation is the implementation of activities without human intervention and modern automation is computerization. With regard to the national nomenclature, the acronym C4 (Command, Control, Communications, Computers, Information) should be understood as an automated command system, hence the C4I automated command systems and the C4ISR automated reconnaissance data collection, processing and distribution system.

Provides information about resources and uses mechanisms that allow for real-time data transfer while ensuring business continuity and an appropriate level of security

The imaging of the operational and tactical situation in an electronic form with the use of a dedicated IT system is carried out with the use of standardized military symbols and digital maps. The display of information is carried out with the use of a software IT tool, which can be generally called application software or a computer application.

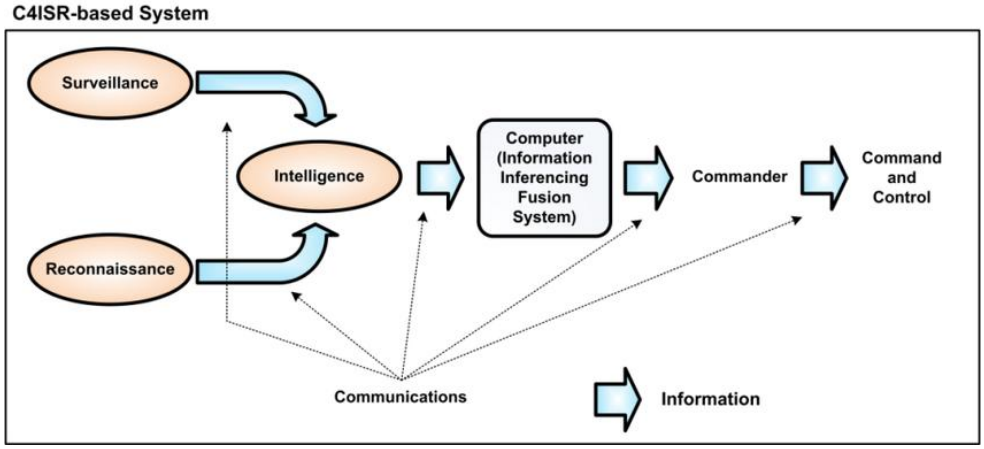


Fig. 5. The-scheme-of-information-flow-in-C4ISR-based-systems

Source: https://www.researchgate.net/figure/The-scheme-of-information-flow-in-C4ISR-based-systems-11-III-Maximum-Score-of-the_fig4_233951956

An important element of the picture of the situation is the creation of a Common Operational Picture as a uniform picture of information relevant to the domain of combat operations, shared between commands or command systems, which facilitates team planning and supports the acquisition of situational awareness at all levels of command. The pictures below (fig.7,8,9,10) show examples of the use of the system HMS C3IS JASMIN during exercises organized in a Military Faculty.

Fig. 6. The C4ISR class system, a product of TELDAT

Source: https://defence24.com/technology/continous-development-of-polish-automated-c2-systems-for-military-operations

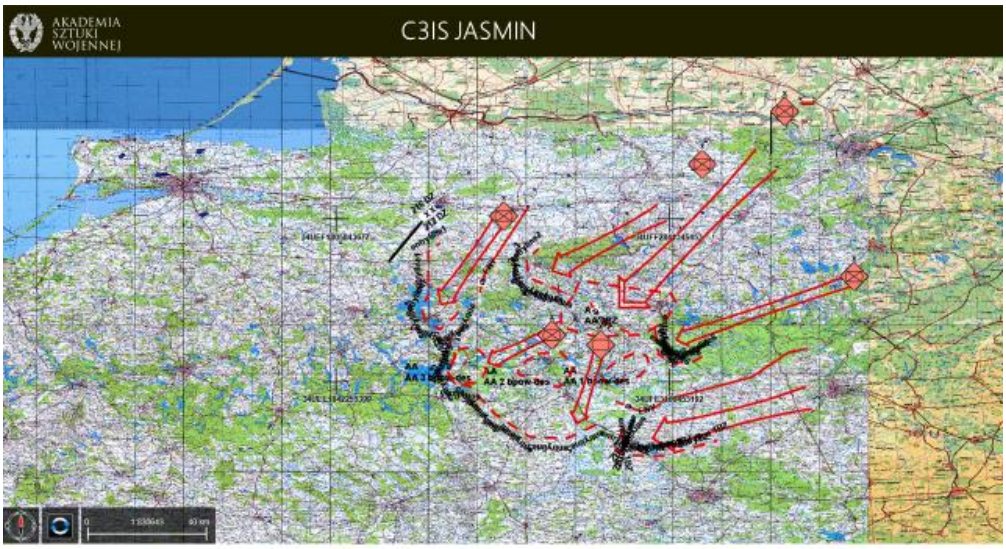


Fig. 7. The situation from exercises at the military faculty
Source: Author's picture.

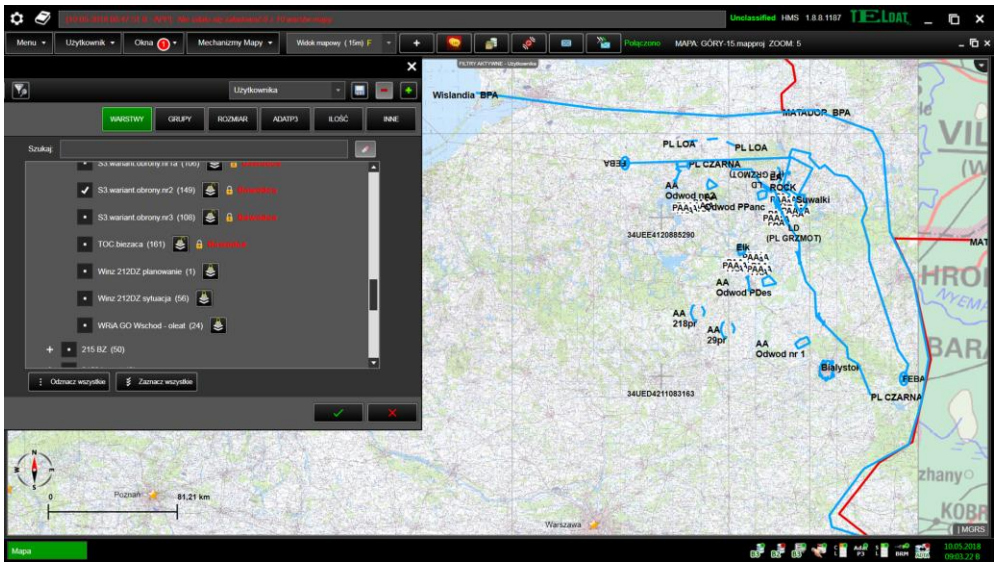


Fig. 8. The situation from exercises at the military faculty
Source: Author's picture.

Fig. 9. Preparation of the systems for the practical tests on the vehicles during the BRAMA-21 exercise in May 2021.

Source: author's own materials.

Fig. 10. Preparation of the HMS JASMINE for the practical tests on the vehicles during the BRAMA-21 exercise in May 2021

Source: author's own materials.

The system that has been successfully used at WSU since 2010 is the HMS C3IS JASMINE version. On the basis of the contract in force with the software manufacturer TELDAT and the Academy, it is possible to modernize and improve the C4ISR class software, which from July 2018 was introduced for

use in the Polish Armed Forces. As a consequence of introducing the system to the Polish Armed Forces, it was forced on the University authorities to create a system of courses and training at various levels of advancement.

Training system with the use of modern technologies at the Military Fakulty of ASzWoj

In 2018 there was a decision taken by the Chief of Staff of the Polish Armed Forces HMS JASMINE system was implemented into the Polish Armed Forces as a primary Command Support System. There was a decision that until December 2020 Polish Armed Forces is supposed to be ready to use this system.

As an answer War Studies University prepared extended version of training of HMS C3IS JASMINE. The extension was necessary to implement to speed up with the number of operators trained with this system. Until the new training system all the University students were trained with the HMS C3IS JASMINE system during the education process during the academic year. New training system was dedicated to the whole soldiers from Poland (and also the NATO countries).

New training system was implemented in 2019 and consist of the five level of courses. It is shown on figure 10. The changing situation in 2020-2021 related to the pandemic forces the creation of a level 6 course for an instructor lasting 30 days.It is shown on figure 11.

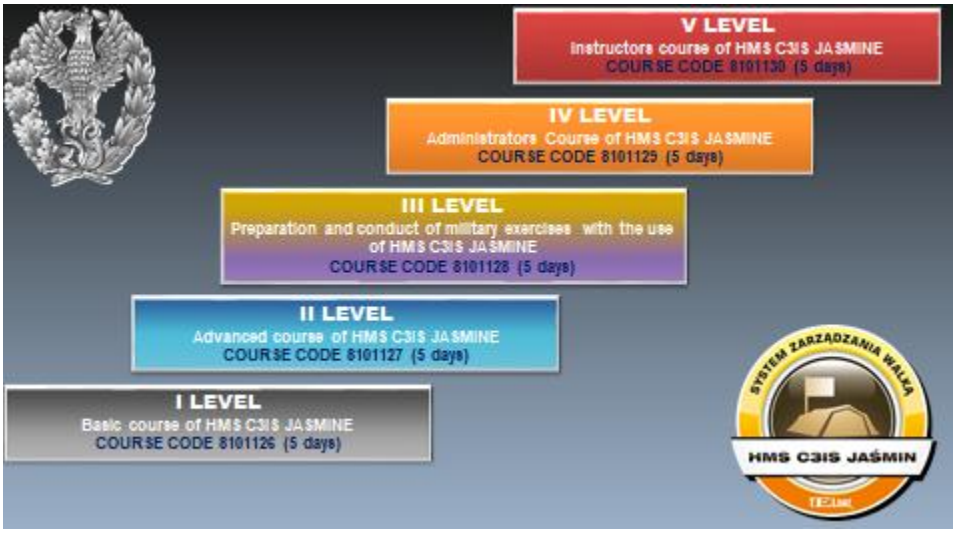


Fig. 11. Training system implemented into the Polish Armed Forces in 2019.
Source: Author's and Teldat materials.

The training system consist a few levels of the knowledge of the HMS C3IS JASMINE system[1]:

– 1st level – BASIC COURSE is dedicated to the operators that do not know anything about the CSS system. It takes 5 working days (ap. 30 hours) and give the knowledge to operate the system;

– 5th 2nd level – ADVANCED COURSE is dedicated to those who accomplished the 1st level course and give the advance knowledge of the system. It is more concentrated on MDMP showing the operator role during each of the phase of the process;

– 3rd level – PREPARATION AND CONDUCT OF THE MILITARY EXERCISE with the HMS C3IS JASMINE system is dedicated to the teams that are responsible to prepare and conduct the military exercise. To accomplish this level candidate must accomplish the 1st and 2nd level of the training;

[1] Biernacik B., A training system implemented in War Studies University of HMS C3IS JASMINE Command Support System in the time of the Covid-19 [in] International scientific conference 2021. Collection of papers security and defense weapons, technologies, logistics communication and computer technologies cybersecurity social science - Shumen, Bulgaria : "Vasil Levski" National Military University ; "Artillery, Aircraft Defense and CIS" Faculty, 2021 - s. 8-18

– 4th level – OPERATIONAL ADMINISTRATOR of HMS C3IS JASMINE system is dedicated to the operators that are responsible for support the Operators on the Command Post with the system running. To accomplish this level it is required to accomplish all previous courses;

– 5th level – INSTRUCTOR of the HMS C3IS JASMINE system is dedicated to the persons that are going to organize in their military units the courses at the first level. Thank to this there will be more instructors and it will be much more popular to get the first level course.

– 6th level- Instructors course of HMS C3IS JASMINE system is dedicated to the pesons, who are provided for training in the home unit, staff assigned to work during the exercise on CP. During the course, students learn topics from level I to V, inclusive, in a 30-day course.

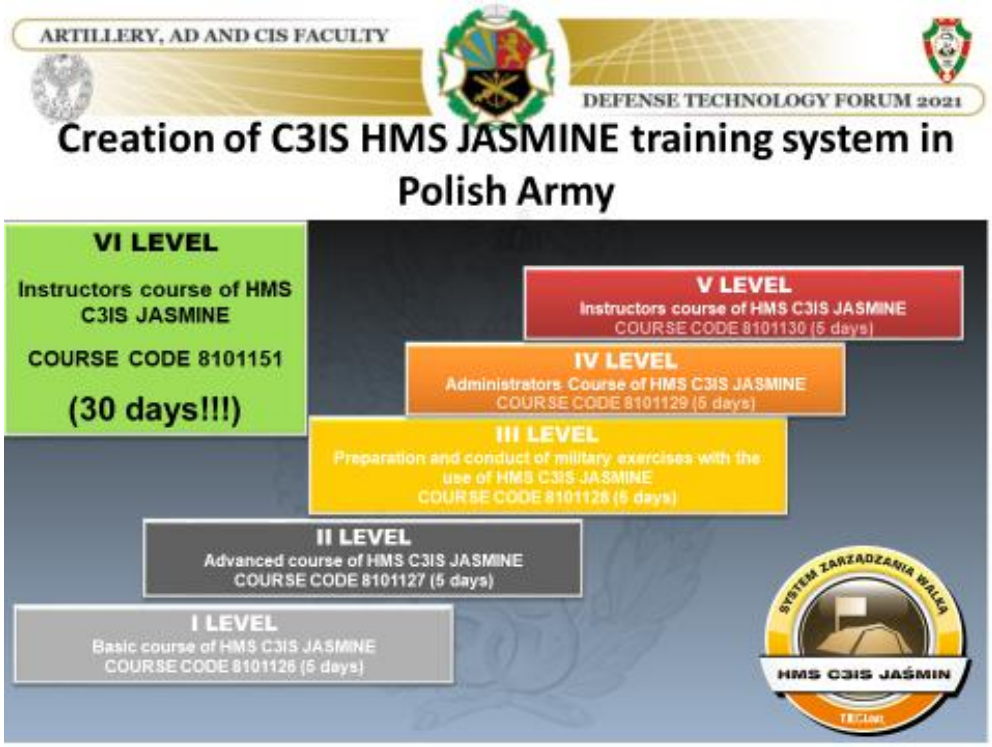


Fig. 12. Training system implemented into the Polish Armed Forces in 2021.
Source: Biernacik B., A training system implemented in War Studies University of HMS C3IS JASMINE Command Support System in the time of the Covid-19 [in] International scientific conference 2021. Collection of papers security and defense weapons, technologies, logistics communication and computer technologies cybersecurity social science - Shumen, Bulgaria : "Vasil Levski" National Military University ; "Artillery, Aircraft Defense and CIS" Faculty, 2021 - s. 8-18

The solution was (shown on the figure 12) implementation of very intensive course for the instructors that are planned for the position of the trainer in their military units. The idea was to create a course that will in one time train operator form "zero" to instructor level. That was possible only when we spend 30 working days with 8 hours per day of practical hours spend with the teacher and the HMS C3IS System. That gave the chance to speed up with the training the operators in the Polish Armed Forces to be ready as an Army to use in an appropriate way the CSS system and to be able to take advantage of the opportunity given by the system.

First edition of this course started in May 2021 and ended on 2nd of June. Course was accomplished by 14 new instructors that since then are independent in providing their own courses at level 1. Figures 13 , 14 shows the ceremony of the end of the first edition of intensive instructor course.

Fig.13. An end of first Intensive Instructor's course ceremony – 2nd June 2021.
Col. Robert Ryczkowski (on the left) reports to the acting Rector – Commandant Col. Tadeusz Zieliński) *Source: Teldat materials.*

Fig.14. An end of first Intensive Instructor's course ceremony – 2nd June 2021.
Member of the Teldat Board Robert Pałka is giving to the one of the new instructor the certificate and the award for the 3rd place of the results during the course.
Source: Teldat materials.

There were provided 8 editions of the 6th level course and almost 180 new instructors are ready to teach within the Polish Armed Forces.

The rest of the instructors not involved in intensive course were trying to train as many as possible operators within the Army.

Summary

War Studies University is the highest University in providing the studies and courses for the Polish Armed Forces. To our University comes officers with an experience from units and their knowledge and experience combined with the knowledge of academic teachers and the system producer gives the chance to constantly develop better and better Command Support System – System of Systems.

The training system implemented in the Polish Armed Forces as well as practical experiments give the better understanding of the CSS and WS and lead us to the changes in procedures and tactics of the specialists supporting the fighting units. This will short the time form detection of the target to the answer from our side.

The depiction of the reconnaissance situation is a complex undertaking, in fact, it is mainly associated with the graphic representation of the situation of the reconnaissance and electronic warfare forces using tactical signs on the basis of a digital map. The implementation of this activity is relatively simple and can be performed using the HMS C3IS JASMIN system available in the Polish Armed Forces for every soldier. Its ability to visualize the reconnaissance situation by means of tactical signs on a digital map background. The functionalities of, in particular, the integrated HMS C3IS JASMIN tool software are impressive in terms of both creating information resources in various recording formats, i.e. text documents, graphic documents, photos and their display as information resources for the user in graphical form. Very extensive functionalities allow you to create a variety of images.

In conclusion, it should be stated that the IT tools for creating the image of the reconnaissance situation are available in the Polish Armed Forces. Proper imaging requires not only having the right software or IT systems, but also appropriate digital maps, the richness of which is very large. It is also necessary to know the norms in the field of tactical signs and the limitations of what often translates into misunderstandings in this area.

References

[1] Biernacik B., A training system implemented in War Studies University of HMS C3IS JASMINE Command Support System in the time of the Covid-19 [in] International scientific conference 2021. Collection of papers security and defense weapons, technologies, logistics communication and computer technologies cybersecurity social science - Shumen, Bulgaria : "Vasil Levski" National Military University ; "Artillery, Aircraft Defense and CIS" Faculty, 2021

[2] Biernacik B., Grel L., Surwiłło T., Vademecum użytkownika oprogramowania HMS C3IS Jaśmin Zautomatyzowanego Systemu Zarządzania Walką poziomu operacyjnego/taktycznego w wersji klienckiej. Poziom podstawowy, WSU, Warsaw, 2021

[3] https://www.teldat.com.pl/aktualnosci/2021/439-istotny-rozwoj-systemu-ksztalcenia-kadr-szkoleniowo-uzytkowych-hms-c3is-jasmin.html

[4] https://www.teldat.com.pl/aktualnosci/2021/442-nastepni-instruktorzy-hms-c3is-jasmin-sa-juz-w-dyspozycji-wp.html

[5] https://www.polsatnews.pl/wiadomosc/2022-08-30/wojna-w-ukrainie-trwa-kontrofensywa-w-obwodzie-chersonskim-isw-pisze-o-wyzwoleniu/

[6] https://tvn24.pl/swiat/rosja-grozi-ukrainie-minister-obrony-ukrainy-moskwa-nie-sformowala-na-razie-ani-jednej-grupy-uderzeniowej-przy-granicy-5606744

[7] https://www.researchgate.net/figure/The-scheme-of-information-flow-in-C4ISR-based-systems-11-III-Maximum-Score-of-the_fig4_233951956

[8] https://defence24.com/technology/continous-development-of-polish-automated-c2-systems-for-military-operations

CURRENT ASPECTS OF ALLIED INSTRUMENTS FOR INNOVATION

Maxim M. Alashki

State expert in the Armaments Policy Directorate, Ministry of Defence and Associate Professor of strategic management, project management and acquisition of the national security at the Higher School of Security and Economics (VUSI) - Plovdiv, m.alashki@mod.bg

***Abstract**: Briefly presented are the currently active innovation initiatives - programs and a number of other diverse in our nature, principles, approach and end goals tools related to building and developing defence capabilities or achieving interoperability at the national, European or NATO level.*

***Keywords**: NATO, European Union, European Defence Agency, innovation, defence capabilities, initiatives, tools, cooperation, defence industry.*

АКТУАЛНИ АСПЕКТИ НА СЪЮЗНИТЕ ИНСТРУМЕНТИ ЗА ИНОВАЦИИ

доц. д-р инж. Максим М. Алашки

държавен експерт в дирекция „Политика по въоръженията" - Министерство на отбраната, доцент по стратегическо управление, управление на проекти и аквизиция на националната сигурност във Висшето училище по сигурност и икономика (ВУСИ) – гр. Пловдив, m.alashki@mod.bg

***Резюме:** Представени са накратко актуално действащите иновационни инициативи – програми и редица други разнообразни по своята същност, принципи, подход и крайни цели, инструменти, свързани с изграждане и развитие на отбранителни способности или постигане на оперативна съвместимост на национално, европейско или на ниво НАТО.*

***Ключови думи:** НАТО, Европейски съюз, Европейската агенция по отбрана, иновации, отбранителни способности, инициативи, инструменти, сътрудничество, кооперация, отбранителна индустрия.*

Съвременните предизвикателства в световен мащаб предизвикаха адекватна реакция в рамките на Европейския съюз, Европейската комисия и в частност на Европейската агенция по отбрана (EDA), както и в Северноатлантическия алианс. Тя се изрази в производството на модерни и по своят характер радикални решения за създаването на нови инициативи и/или инструменти, и свързани с тях програми и проекти, както и насочването им да работят по съгласуван и ефикасен начин, което пък чисто организационно и практически представлява още по-голямо предизвикателство. Тези инициативи са все с цел насърчаване на сътрудничеството и кооперацията в областта на отбранителната индустрия, науката, изследванията и развитието на технологиите, които трябва да се съсредоточат върху съвместно договорени приоритети, да бъдат ориентирани към резултатите (тоест да задействат съвместни проекти, произвеждащи нови технологии и оборуд-

ване) в областта на сигурността и отбраната, както и да бъдат съгласувани процесите, свързани и с планирането за постигане на необходимите отбранителни способности.

Различните инициативи – програми и редица други разнообразни по своята същност, принципи, подход и крайни цели инструменти, свързани с изграждане и развитие на отбранителни способности или постигане на оперативна съвместимост на национално, европейско или на ниво НАТО се финансират от държавите-членки, участващи в тях. По отделно страните, в това число България, не разполагат с възможност за използване на фондовете на Алианса и европейските структурни и кохезионни фондове за цялостно или частично финансиране на национални и съвместни програми, проекти и други дейности, свързани със сигурността и отбраната. Същевременно, и НАТО и Европейския съюз разполагат с инициативи, програми и инструменти, които позволяват на научни организации, които са второстепенни разпоредители с бюджет на пряко подчинение на министъра на отбраната и на частни компании да участват самостоятелно или в консорциуми, които да кандидатстват за финансиране по проекти свързани с иновациите в сектора на сигурността и отбраната.

Накратко, предвид времето, което е предоставено за докладване, ще Ви запозная с тези инструменти:

А. НАТО:

- Ускорител за иновации в отбранителния сектор в Северноатлантическия регион (Charter of the NATO Defence Innovation Accelerator for the North Atlantic - DIANA)

Ускорителят е създаден да подпомага технологичното сътрудничество и обмена на информация между съюзниците като развие мрежа от структури и способности за иновация и поема рисковете, свързани с иновативните технологии. Той включва всички страни-членки на Алианса и се ръководи от Борд на директорите, който одобрява двугодишни Стратегически указания, вземайки предвид недостига от способности и изискванията, идентифицирани от Процеса на планиране на отбраната в НАТО (NDPP) и от Военните органи на НАТО. Ще бъдат изпълнявани Програми за предизвикателства (Challenge Programs), които ще подпомагат разкриването на напредък и постигането на приемливи решения за конкретни проблеми в областта на сигурността и отбраната, особено за ключови отбранителни нужди. Ускорителят за иновации ще изпълнява задачите си, чрез мрежа от съставни и афилиирани елементи, като последните се състоят от тестови центрове и мрежа за създаване на иновации. Голяма част от предложените тестови центрове са в областта на данните, изкуствения интелект и автономността. България кандидатства с 3 центъра, които са одобрени: Института „Големи данни в полза на интелигентното общество" (Big Data for Smart Society – GATE), който кандидатства за два тестови центъра – в областта на големите данни и в областта на изкуствения интелект и автономните системи; и Института по отбрана „Проф. Цветан Лазаров" за тестови център в областта на изкуствения интелект и автономните системи.

- Фонд на НАТО за иновации

Фондът се създава с цел многонационално финансиране на стартъпи, работещи по нововъзникващи и революционни технологии (Emerging and Disruptive Technologies - EDT) и технологии с двойна употреба, в ключови за Алианса области, които са с потенциал за прилагане. Към момента 21 държави от НАТО са се присъединили към фонда. Разработеното Споразумение на участващите съдружници (Limited Partnership Agreement (LPA)) включва следните основни параметри: седалище в Люксембург; размер на финансовите средства около 1 млрд. евро за общ период от 15 години; 80% от средствата ще се използват през първите 8 години (по 100 млн. евро), а останалите в следващите 7 години; моделът на финансиране ще следва формулата 60 % от годишния бюджет на равни вноски и 40 % спрямо БВП за всяка страна-участник; управлението ще

се осъществява чрез Комитет на участващите съдружници (LPAC) в два формата – на партньорите (P-LPAC) и на субфонд (SF-LPAC); освен страни-членки във фонда могат да участват и партньори или юридически лица от съюзници, но с не повече от 25 % от общата стойност; при разпределяне на инвестициите ще се прилага балансирана географска диверсификация; няма да са възможни преки инвестиции в рискови компании; фондът ще инвестира в стартъпи в областта на нововъзникващите технологии, с приоритет във физическите технологични решения, пред софтуерните разработки и др.

Б. ЕВРОПЕЙСКИ СЪЮЗ:

- Хъб за иновации в европейската отбрана (Hub for EU Defence Innovation - HEDI)

Този хъб е одобрен на заседанието на Направляващия борд на Европейската агенция по отбрана (EDA) във формат „министри на отбраната" на 17.05.2022 г. с цел EDA да използва тристепенна рамка за работа спрямо иновациите – идентификация, анализ и прилагане. Хъбът ще бъде пресечната точка на дейностите в иновационната рамка, служейки като катализатор и ускорител. Той ще стимулира и укрепва иновационните дейности на агенцията, създавайки ясни връзки в съществуващите работни направления, инициирайки нови дейности и предоставяйки стимули за финансиране и прозрачност и ще „стартова площадка", за гарантиране на предоставянето на иновативни решения за способностите на въоръжените сили на Европейския съюз. Хъбът ще координира сътрудничеството в областта на иновациите в отбраната между държавите-членки, като същевременно гарантира синергия със свързани дейности на Европейската комисия и съгласуваност с инициативите на НАТО за иновации. Персоналът му ще бъде интегриран в съществуващите дирекции на EDA. Първоначалното портфолио на хъба е включва 6 групи дейности (4 са предназначени да идентифицират и разработят нови идеи и решения за нуждите и недостига от способности, 2 за осигуряване на необходимата осведоменост за решения, методологии и пр. за заинтересованите страни). Сред основните дейности на хъба са: изграждане на мрежа от организации за иновации в отбраната; учредяване на награди за иновации; иновационни предизвикателства; доказателство на концепцията/демонстратори; европейско представяне за иновации в отбраната; усвояване на иновациите.

- Европейската програма за промишлено развитие в областта на отбраната (European Defence Industrial Development Programme – EDIDP)

Тя е приета с Регламент на Европейския парламент и на Съвета през 2018 г. за подкрепа на европейската отбранителна индустрия, която да действа през 2019 – 2020 г. с бюджет от 500 млн. евро. В рамките на програмата през 2020 г. Министерството на отбраната подкрепи 2 проекта, които получиха финансиране с бенефициенти Института по отбрана „Проф. Цветан Лазаров" и Висшето военноморско училище „Никола Й. Вапцаров". Проектите включват: Информационна система за осигуряване на подводни интервенции (Comprehensive Underwater Intervention Information System - CUIIS), планиран да завърши през 2024 г., с бюджет от 5,7 млн. евро, от които Европейската комисия ще покрие 5,5 млн. евро; и „Европейско решение за бъдещо огнево поразяване" (Future Indirect fiRes European Solutions - FIRES) с координатор Франция, който обхваща изследване и дизайн за разработване на програмируеми и управляеми боеприпаса за прецизно насочване, като конкретно се фокусира върху разработване на европейско решение за артилерийски боеприпаси, с бюджет 3,5 млн. евро и срок на завършване 2023 г. България участва и в два ад-хок проекта от портфолиото на EDA за 2022 г. – „Програма за обучение и подготовка от-

носно енергетичните материали" и „Иновативни материали за базирани на способности изследвания за високотехнологична европейска отбрана".

- Европейски фонд за отбрана (European Defence Fund - EDF)

Европейският фонд е приет с Регламент на Европейския парламент и на Съвета от 2021 г. в рамките на действащия програмен период 2021-2027 г., с бюджет от 8 млрд. евро и включва набор от мерки с икономическа и индустриална насоченост за насърчаване на конкурентоспособността и иновативния капацитет на отбранителната индустрия на съюза, подкрепа и оптимизиране на сътрудничеството между предприятия при разработването на продукти и технологии в областта на отбраната, преодоляване на дистанцията между научните изследвания и иновациите и насърчаване на всички форми на иновации. Той цели и подпомагане на държавите-членки при разработването и придобиването на съвместни ключови отбранителни способности, по-бързо и икономически по-ефективно, като се насърчават инвестициите в съвместни разработки и се стимулира развитието на единна европейска конкурентоспособна и иновативна индустриална база. Основание за идентифициране, финансиране и реализация на проект в рамките на фонда е съответствие с приоритетите за отбранителните способности, договорени от държавите членки в рамките на Общата политика за сигурност и отбрана (ОПСО) и по-специално в контекста на Плана за развитие на способностите. Вземат се под внимание и ангажименти и приоритети на държавите членки в сферата на отбраната и отбранителните способности в рамките на регионални и международни формати, като например НАТО. Проектите, които ще бъдат финансирани имат пряка връзка с различни текущи и бъдещи проекти по Постоянното структурирано сътрудничество в областта на отбраната на Европейския съюз (PESCO), за който ще стане дума специално. Съгласно целите и условията на Европейския фонд за отбрана, Министерството на отбраната не може да бъде пряк бенефициент по проекти, финансирани от фонда, същевременно научни организации, второстепенни разпоредители с бюджет и на пряко подчинение на министъра на отбраната, могат да участват пълноправно в консорциумите, които кандидатстват за финансиране по фонда.

- Европейска програма за финансиране на научни изследвания и иновации в областта на сигурността „Хоризонт Европа" (Horizon Europe)

В допълнение на ролята, която имат в рамките на EDF, организации, второстепенни разпоредители с бюджет в Министерството на отбраната, участват в проекти в рамките на „Хоризонт Европа". Към момента има 13 действащи проекти.

- Постоянно структурирано сътрудничество на Европейския съюз в областта на отбраната (Permanent Structured Cooperation - PESCO)

В края на 2017 г. Съветът на Европейския съюз прие решение за установяване на това Постоянно структурирано сътрудничество, а България се включи в него с подписване на общата нотификация от 25 държави-членки на съюза. на 13 ноември 2017 г. До момента участваме в шест проекта като „член" и в пет като „наблюдател". Разходите за участие се поемат от държавите-членки и няма директна възможност за използване на програми и инструменти на Европейския съюз. Проектите са както следва: проект за подобряване на военната мобилност (Military mobility) с водеща нация Холандия; проект за изграждане на логистични хъбове в подкрепа на операции (Network of Logistic Hubs in Europe and Support to Operations) с водеща нация Германия; проект за надграждане на системата за морско наблюдение (Upgrade of Maritime Surveillance) с водеща нация Гърция; проект за изграждане на мрежа от водолазни центрове (European Union Network of Diving Centres) с водеща нация Румъния; проект за федеративна мрежа от кибер полигони (Cyber Ranges Federations) с водеща държава Естония. България е водеща нация на проект

„Модулен елемент за бързо развръщане за подводни интервенции" (Deployable Modular Underwater Intervention Capability (DIVEPACK). След изтичане на периода за представяне на проектни предложения Секретариатът на Постоянно структурираното сътрудничество ще организира два синхронизиращи работни семинара (ноември 2022 г. и януари 2023 г.), с цел да подпомогне предлагащите държави-членки в набирането на подкрепа за техните предложения, като до тогава нови проектни предложения няма бъдат приемани.

- **Комуникация на Европейската комисия относно анализ на недостига на инвестиции в европейската отбрана и свързаните с него последващи действия**

Документът е фокусиран върху развитие на европейската отбранителната индустрия чрез развитие на отбранителните способности на държавите-членки на Европейския съюз. Целта е повишените инвестиции за отбрана да допринесат за по-силна индустриална база. Държавите членки се насърчават за съвместно придобиване на способности от европейски производители, чрез различни стимули вкл. и финансови (напр. отпадане на ДДС). Предвижда се картографиране на европейските производствени възможности и повишаване на капацитета им, както и финансиране от европейския бюджет, насочено към европейската индустрия. Тази комуникация се явява елемент на провежданата политика на съюза за т.нар. „дефрагментиране" на европейския отбранителен пазар и насърчаване координацията и сътрудничеството между държавите членки при развитието на отбранителни способности. За това допринасят и останалите съюзни отбранителни инициативи като EDF, PESCO, Координирания годишен преглед на отбраната (CARD) и Плана за развитие на способностите (CDP). По същество, в основата на подхода е заложен пазарния механизъм за търсене и предлагане – чрез повишаване на търсенето на отбранителни продукти, чрез министерствата на отбраната на държавите-членки на база на съответните политики на ниво Европейския съюз ще се стимулира повишаване на предлагането и съответно развитието на отбранителната индустрия.

- **Работна група на Съвета по въпросите на отбранителната индустрия**

В началото на юни Френското председателство на Съвета на Европейския съюз разпространи документ за дискусия с предложение за създаване на нова Работна група на Съвета по въпросите на отбранителната индустрия. Предложението се мотивира с възложената от Европейския съвет от 30 и 31 май 2022 г. задача към Съвета спешно да проучи възможностите за координиране на бързо придобиване на отбранителни способности с цел запълване на резервите на държавите-членки, особено в контекста на предоставената на Украйна подкрепа, както и за краткосрочно укрепване на европейските отбранителни способности чрез съвместно придобиване на доброволна основа. Предвижда се групата да функционира под ръководството на Комитета на постоянните представители (КОРЕПЕР), както и да подпомага дейността на Съвета във формат външни работи/отбрана в рамките на ОПСО, както и при необходимост и другите формати на Съвета в зависимост от характера на конкретния въпроса за обсъждане.

- **Работна група за съвместно придобиване/възлагане на поръчки (Defence Joint Procurement Task Force)**

В непосредствена перспектива ще бъде създадена съвместна работна група за обществени поръчки в областта на отбраната, която да работи с държавите-членки, с цел осигуряване на координиран подход и премахване на конфликта на техните краткосрочни нужди от обществени поръчки, за справяне с новата ситуация свързана със сигурността, вкл. координацията относно военната помощ за Украйна. Наред с това се предвижда групата да осъществява и тясна комуникация с отбранителната промишленост на Европейския съюз, за да се повиши осведомеността на държавите-членки относно промишления капацитет на съюза и как той може да отговори на тех-

ните нужди. Групата ще има за задача да координира и насърчава подхода за сътрудничество, като се даде възможност за съвместно възлагане на обществени поръчки, които отговарят на условията за финансиране по краткосрочния инструмент (500 милиона евро през периода 2022-2024 г.).

В заключение може да се посочи, че сътрудничеството в областта на развитието на иновациите, както на национално, така и на съюзно ниво, е едно от най-перспективните направления за придобиване, вкл. изграждане и развитие на необходимите отбранителни способности, и участието на отбранителния индустриален капацитет в този процес. Иновациите, при тяхното подходящо управление и надграждане са способни да носят необходимия синергичен ефект както на отбранителните способности, ерго на сигурността, така и на свързаната с тях отбранително-индустриална база.

References

1. Регламент (ЕС) 2018/1092 на Европейския парламент и на Съвета от 18.05.2022 г.
2. https://www.eda.europa.eu/what-we-do/our-current-priorities/permanent-structured-cooperation-(PESCO), 04.07.2022.
3. https://www.eda.europa.eu/webzine/issue18/cover-story/european-defence-fund-(edf), 04.07.2022.
4. https://www.eda.europa.eu/what-we-do/our-current-priorities/permanent-structured-cooperation-(PESCO)/pesco-and-other-eu-defence-initiatives, 04.07.2022.
5. https://ec.europa.eu/growth/content/2019-calls-proposals-european-defence-industrial-development-programme-edidp_en, 04.07.2022.
6. https://www.eda.europa.eu/what-we-do/activ 04.07.2022.
7. ities/activities-search/pilot-project-and-preparatory-action-for-defence-research, 04.07.2022.
8. https://eda.europa.eu/what-we-do/activities/activities-search/capability-development-plan, 04.07.2022.
9. https://www.eda.europa.eu/webzine/issue18/cover-story/josep-borrell-member-states-need-to-make-the-most-out-of-the-new-eu-defence-tools, 21.08.2020.

THE POWERS

Maxim M. Alashki

State expert in the Armaments Policy Directorate, Ministry of Defence and Associate Professor of strategic management, project management and acquisition of the national security at the Higher School of Security and Economics (VUSI) - Plovdiv, m.alashki@mod.bg

***Abstract**: An examination of the concept of the three types of powers has been carried out, with their peculiarities and characteristics, as they are understood in their historical development from Montesquieu to the present day, with a reference to our country. In order for the review to be complete, they were added, with their accolades, and the so-called "fourth power" – the media, as well as the power of society.*

***Key words**: power, legislature, executive power, judiciary, fourth power, power of society*

ВЛАСТИТЕ

Максим М. Алашки

държавен експерт в дирекция „Политика по въоръженията" - Министерство на отбраната
доцент по стратегическо управление, управление на проекти и аквизиция на националната сигурност във Висшето училище по сигурност и икономика (ВУСИ) – гр. Пловдив, m.alashki@mod.bg

***Резюме:** Направен е преглед на концепцията за трите вида власти, с техните особености и характерни черти, така както те са разбирани в историческото им развитие от Монтескьо до наши дни, с референция към нашата страна. За да бъде прегледът пълен, към тях са добавени, със своите отличия, и т.нар. „четвърта власт" – медиите, както и властта на обществото.*

***Ключови думи:** власт, законодателна власт, изпълнителна власт, съдебна власт, четвърта власт, власт на обществото.*

Разделението на властите е доктрина, според която трите функции на държавното управление – законодателна, изпълнителна и съдебна – трябва да бъдат разделени и изпълнявани от различни органи, определени от Конституцията. Съответстващите им изпълнителна, законодателна и съдебна власт се осъществяват от независими институции, но в своите функционални отговорности те взаимно се контролират. Тези направления на държавното управление са автономни, макар и да са взаимообвързани, без да се реализира каквато и да е подчиненост едно на друго. Разделението (разпределението) на правомощията е такова, че не може едното направление на властта да упражнява власт, която влиза в отговорностите на друго. Задължително всички власти, включително съдебната власт, която е независима от политическо влияние при осъществяване на функциите си, са с осигурена мандатност.

Аристотел[*], в своя трактат „Политика"[**], споменава за първи път идеята за смесено управление, и така се явява предшественик на разделението на властите. Там се говори за комбинация от демокрация и аристокрация. Теорията за разделение на властите, вече като цялостно и завършено учение, е формулирана от Шарл дьо Монтескьо[***] през 1748 г. По-късно принципът на разделение на властите е възприет от всички демократични конституции, включително от съвременните. Този принцип съдържа две основни начала: първо, той обособява три власти - законодателна, съдебна и изпълнителна, които трябва да бъдат независими, и второ - за да няма възможност за злоупотреба с властта, е необходимо да има баланс между тях. Според автора на теорията ако властите са обединени а не разделени, би съществувал произвол, затова те трябва да бъдат разпределени между различни институции. Ако законодателната и изпълнителната власт са съсредоточени в едно лице, не може да има свобода, не може да има свобода и ако съдебната власт не е отделена от законодателната и изпълнителната.

Монтескьо задава, че законодателната власт е общата воля на държавата, а изпълнителната се грижи за изпълнението на тази воля. Законодателната власт би трябвало да принадлежи на целия народ, но понеже това е невъзможно, е необходимо народът чрез свои представители да прави това. Изводът, който той прави е, че народът „трябва да участва в управлението само като избира свои представители, което е напълно по силите му". Представителното събрание трябва да създава закони и да съблюдава те да се изпълняват. Изпълнителната власт, от своя страна, трябва да бъде съсредоточена в единоначалието (тогава - монарха). Така политическият идеал на Монтескьо е конституционната монархия. Според него съдебната власт е „най-малко" власт, и тя е съсредоточена в ръцете на независимия съд като висококомпетентен орган, който не може да бъде овластяван пряко, и по тази причина се овластява от другите власти.

Целта на разделението на властите се състои в следното: да има политическа свобода, с други думи да няма тирания; да не се злоупотребява с властта и властите трябва да се възпират една друга, тоест да има контрол от страна на гражданите; да се защити свободата като се изключи възможността един човек да обедини всички власти в ръцете си; властите да са в интерес на гражданите.

Разделението на властите цели ефективното и резултатно функциониране на управлението, тъй като се предполага, че различните видове институции осъществяват по-добре определените си функции. Смята се например, че единна изпълнителна власт, водена от премиер или президент по-добре може да работи за прилагането на законите, отколкото законодателната власт, изградена от много индивиди, представящи различни интереси и идеи.

В управлението на една държава и трите власти играят еднакво важна роля. Гражданите избират малцинство (представители), което да управлява мнозинството, но хората (мнозинството) са тези, които овластяват своите представители. В конституциите на съвременните държави не се среща абсолютно разделение на властите (например в някои страни на изпълнителната власт са дадени големи законотворчески правомощия), но в конституциите на демократичните държави този принцип се спазва в много голяма степен.

---

[*] *Аристотел (гр. Ἀριστοτέλης) е древногръцки философ и учен, един от най-големите гении на Античността, наричан „Баща на науката", ученик на Платон и учител на Александър Велики, пише за естетика, етика, икономика, метафизика, политика, психология, реторика и теология, съчиненията му са на практика енциклопедия на древногръцкото познание.*

[**] *„Политика" (гр. Πολιτικά) е произведение на Аристотел, което е в допълнение към неговите разработки по етика, отнасящи се към индивида. В текста на трактата думите полис (πόλις) – град и политейа (πολιτεία) – държавно устройство представят съвременните тогава идеи за държава, гражданска общност и общество.*

[***] *Шарл Луи дьо Монтескьо (фр. Charles-Louis de Montesquieu) е френски висш аристократ, писател, юрист, социолог, известен преди всичко като историк–философ и държавен мислител, един от основоположниците на френското Просвещение, характеризиращо се с вярата в разума, доверието в науката и в рационализма, основоположник на теорията за разделение на властите, залегнала в много конституции по света.*

Погледнато исторически, Монтескьо не е първият, който говори за разделение на властите, но той първи превръща тази идея в цялостна и завършена теория, която пряко влияе на създателите на първите демократични конституции в Европа.

Ако обаче се навлезе в генезиса на разделението на властите се вижда, че то не е едноплановo. Например, разделение има между суверена и субекта (държавния апарат). Ако вземем нашата конституция, съгл. чл. 1, ал. 2 цялата власт се осъществява непосредствено от народа и от органите, предвидени в нея. Суверенът е носител на властта, но той участва и в нейното реализиране, чрез два вида управленски решения, които дават съдържанието на пряката демокрация - избори и референдум. С акта на изборите суверенът учредява държавната власт и я предоставя на определена политическа сила, или политическа коалиция. От една страна той определя конкретно своите представители, а от друга им делегира правото да реализират неговата власт чрез своите решения. Референдумът пък е начин за осъществяване на пряко участие на гражданите в управлението на държавата, но въпреки, че националният референдум от теоретична гледна точка е висша форма на пряка демокрация, чисто практически неговото приложение е силно ограничено.

Държавната власт се разделя на законодателна, изпълнителна и съдебна, от друга страна държавните органи се разделят на представителни и на органи, които управляват без делегация (ex officio[*]). Този трети вид разделение има значение при решаването на теоретичния спор относно съотношението „власти – функции".

Съществува принципен (а и теоретичен) спор дали разделението на властите е всъщност разделение на функциите. Някои изследователи считат, че държавният апарат осъществява значително количество функции, които обогатяват дейността на трите основни титуляри на властта – парламент, правителство и съд. Други считат, че всяка власт е функция, но не всяка функция е власт, според тях принципът на разделение на властите визира само трите власти, свързани с т.нар. „битие" на закона: законодателна, изпълнителна и съдебна. Развитието на държавното управление води до създаване на нови титуляри на властнически функции, а именно – президент, конституционен съд и други, чиито дейности не са власт, а следва да се означат само като функции.

Както учението за суверенитета на народа, така и учението за разделението на властите се развива непрекъснато и претърпява редица промени с течение на времето. Разделение на законодателната от изпълнителната власт е налице само в президентските републики и донякъде при силни полупрезидентски режими. При парламентарните републики, каквато е нашата, има друг вид разделение, което съобразно изказаната теоретична постановка е следното: парламентът е „власт", а правителството е „изпълнителна власт", което осъществява само дейност. От тази теоретична гледна точка изпълнителната и съдебната власти не произтичат от суверена, но така суверенът губи контрола си върху тях. Получава се един своего рода парадокс – суверенът контролира властите, а дейностите са безконтролни.

Различието между власти и дейности предпоставя и неравенството между тях. Разглеждано като съвкупност от сили, обществото може да бъде в състояние на равновесие при равенство между силите – те трябва да са равни и да се възпират. Разделението на властите се проявява като разделение на управлението, необходимо, за да осигури баланс между институциите. Единна в своето учредяване и съществуване, държавната власт се разделя в процеса на своето осъществяване. Това е друг парадокс - на генезиса на разделението: парламентаризмът, който е основен двигател за разделението на властите, в известен смисъл го обезсмисля. Парламентарното мнозинство приема законите, избира правителството и участва във формирането на съдебната власт. Когато парламентарното мнозинство е еднопартийно, институционалното разделение на властите се събира в партийното управление, ерго на практика няма никакво разделение на властите.

Според Конституцията си Република България е единна парламентарна република с местно самоуправление и с ясно изразено разделение на властите: законодателна, изпълнителна и съдеб-

[*] *ex officio* – лат. *по длъжност, служебно, по задължение*

на. Страната се управлява според върховният закон – Конституцията и законите на страната, а политическият живот се основава на принципа на политическия плурализъм.

Съгласно нашият върховен закон президентът е държавен глава, който олицетворява единството на нацията и представлява страната в международните отношения. Той е върховен главнокомандващ на Въоръжените сили и председател на Консултативния съвет за национална сигурност (КСНС). Макар да не притежава законодателна власт или законодателна инициатива, той има право да върне законопроект за преразглеждане, упражнявайки правото си на налагане на вето. Негово правомощие е да отправя обръщения към народа, да обнародва законите в Държавен вестник, да дава и отнема българско гражданство, да упражнява право на помилване и др.

Къде обаче е мястото на нашия президент, измежду трите власти? В неговите правомощия се преплитат функции: освен, че е върховен главнокомандващ на Въоръжените сили и председател на КСНС, негова е последната дума при назначаване на посланици и висш ръководен състав на Въоръжените сили (по предложение на Министерския съвет), на главния прокурор и ръководителите на върховните съдилища, има квоти в редица органи, като Конституционния съд, съвети и регулатори, както и функции при обнародване на закони, при обявяване на парламентарни и местни избори и прочие. Най-силно се усеща неговата власт при „служебните" правителства, които се назначават от него и в техния мандат практически изпълнителната власт е негова, при това с отсъствие на законодателната власт. Но, като цяло, правомощията на президента, дадени му от конституцията, не са особено много, за разлика от т.нар. „президентски републики" (Франция, Русия, САЩ, Турция и др., където той посочва министър-председателя) и правят неговата фигура само на крачка по-нагоре от тези, където президентът има само протоколни функции (Германия, Гърция, Италия и др., в които той се избира от парламентите).

От своя страна Министерският съвет (Правителството) е основният орган на изпълнителната власт в Република България. Той е съставен от министър-председател (премиер-министър, заместник министър-председатели и членове – ресорни министри (с министерства или без, т.нар. „без портфейл"). Министерският съвет ръководи и осъществява вътрешната и външната политика на страната, осигурява националната сигурност, вкл. обществения ред и ръководството на Въоръжените сили, провежда управлението на държавната администрация чрез създадените от него министерства, агенции и комисии. В своята дейност правителството е под прекия контрол на Народното събрание, като отделните министри и министър-председателят са задължени да отговарят на питания на отделните народни представители.

Българският еднокамарен парламент, наречен Народно събрание, осъществява законодателната власт в страната и упражнява парламентарен контрол. То се състои от 240 депутати, избирани за срок от 4 години. Гласува се за списъци от кандидати на партии или коалиции за всеки от 31-те многомандатни избирателни района. За да бъде представена в Народното събрание, дадена партия или коалиция трябва да спечели най-малко 4% от гласовете. В отговорностите на Народното събрание са приемането на закони, одобряването на държавния бюджет, установяването на данъците и размерите им, насрочването на президентски избори, избора и отзоваването на министър-председателя и другите членове на Министерския съвет, обявяването на война, разполагането на войски извън България, ратифицирането на международни договори и споразумения и др.

Законодателният процес от Народното събрание се осъществява въз основа на Конституцията и на приет от него правилник. Право да внасят законопроекти имат народните представители и Министерския съвет.

Третата власт - съдебната защитава правата и законните интереси на гражданите и на държавата[7]. Висшият съдебен съвет се състои от 25 члена, избирани за срок от 5 години, които образуват пленум, чрез който осъществяват правомощията си. Заседанията им се председателстват от министъра на правосъдието. Самото правосъдие се осъществява от: Върховен касационен съд, Върховен административен съд, районни, окръжни, апелативни, военни съдилища – военно-окръжни и военно апелативни, и специализирани съдилища (които понастоящем са в процес на отмяна). По конституция към съдебната власт се числят и прокуратурата и следствието.

Конституционният съд, създаден през 1991 г., въпреки, че се именува съд, не е част от съдебната система на страната ни. Той дава тълкувания на конституцията, обявява в противоконституционност, решава спорове за компетентност между властите и др.

Тъй наречената „местна" власт - местните органи на управление - на практика са част от изпълнителната власт. Общините, които към момента са 265, са основната административно-териториална единица и чрез тях се реализира местното самоуправление. Орган на това самоуправление в общината е общинският съвет, а управлението в областта се осъществява от областен управител, подпомаган от областна администрация. Орган на изпълнителната власт в общината е кметът, който се избира от населението или от общинския съвет. Съставни административно-териториални единици в общините са кметствата и районите, като в общините се избират общински съвети и кметове на общини, в кметствата се избират кметове, а в районите - районни съвети и кметове.

За да бъде обзорът на властите съвсем пълен и засягащ всички аспекти ще посочим, че съществуват и други, неофициално наименовани „власт", но все пак „власт", ерго със своето съответно влияние, сила и възможности да определят развитието на процесите в страните по света – това е властта, наричана нарицателно „четвърта власт", както и властта на обществото.

Четвъртата власт са медиите. Те са необходимост, важна част от развитието на обществото, те дават информация, позиция и гледна точка, помагат за формулиране на мнение. Метафората „четвърта власт" представя медиите като независими спрямо останалите три власти - съдебна, законодателна и изпълнителна. Изразът „четвърта власт" се налага във Франция през осемдесетте години на XVIII век, след процеса на Алфред Драйфус[*], който е обвинен, че е германски шпионин, осъден набързо и заточен. Тогава благодарение на журналистическо разследване платено от интелектуалци и общественици, се разкрива, че той е невинен. Целият тогавашен спектакъл е режисиран, защото Драйфус е бил евреин, а Емил Зола пише по този повод: „За щастие има една четвърта власт, която е в състояние да открива и коригира грешките, допуснати от трите секуларни власти...".

Целта на медиите дълго време е била да бъдат коректив на другите власти, да разкриват пред обществото нередностите извършвани от властта без да се страхуват от нея. С времето обаче, до голяма степен, медиите се превръщат в стока, своеобразен пазар, техният независим дух, който контролира нередностите, се превръща в покупко-продажба на информация или дезинформация. И така се появява зависимостта им и цензурата, която в най-общи линии представлява контрол върху словото и съдържанието, което може да бъде наложено не само от държавните институции.

Медиите са средство за оформяне на общественото мнение, те регулират и моделират човешката мисъл и я насочват. Медиите биват използвани за политически кампании, конфликти и др., чрез тях обществото се наслаждава на „панаира", от който има нужда за да се чувства значимо. За обикновения потребител медията е бойното поле на политически елит, от което той се чувства част, като го наблюдава. Медиите, чрез техните особена сила и широки възможности, могат да оказват влияние за да определят силата, обхвата, посоката и интензитета на обществено-политическите и стопанските процеси, протичащи в отделните страни. Перифразирайки Буров[*]: „Банка, политик и муха се убиват с вестник".

---

[*] *Alfred Dreyfus (фр.) е единственият френски офицер от еврейски произход, достигнал до служба в Генералния щаб на френската армия. Обвинен в шпионаж в полза на Германската империя и осъден през декември 1894 г. на доживотна каторга във Френска Гвиана. Делото „Драйфус" е едно от най-противоречивите и поляризиращи съдебни дела в съвременната история на Франция и завършва с пълната реабилитация на обвинения.*

[*] *Атанас Буров (30.01.1875 – 15.05.1954) е известен български финансист, филантроп, дипломат и политик, министър на търговията, промишлеността и труда (1913, 1919 – 1920) и на външните работи и изповеданията (1926 – 1931). Считан е за една от най-влиятелните фигури в българския политически живот през първата половина на XX век, а заради политическите си речи и въвеждането на модерни за времето си европейски практики на българска почва е наричан „идеолог на българската буржоазия".*

Стигаме до властта на обществото. Във всяко общество се формират групи, които по един или друг начин създават център на власт, който излъчва своето действие в различни посоки като: религия, икономика, култура, местни обичаи, спорт, дори мода. Обществото е истинско „стълпотворение от сили", съсредоточено в организирана единица, и позволява хармоничното развитие на различните слоеве в него, което води до интеграция на политическата власт. Генерално властта се ражда като необходимост да се осигури съжителството на хората, следователно, ако няма ред и власт, възможността за съвместно живеене и взаимодействие в обществото се компрометира.

„Публичната власт", понятие, което обикновено се използва в множествено число като „публични правомощия", означава съвкупност от държавни органи и институции. Тук обаче става дума за възможност на публични (на обществото) организации и други различни обединения да влияят на действащата власт (власти), предимно с демократични средства и техния инструментариум. Това са политическите партии, групите за натиск, лобизма, обществените организации и движения, и техни производни.

Под понятието „групи за натиск" най-често се разбира предимно доброволни обединения, приспособени или специално създадени от гражданите за изразяване и защита на техни властно значими интереси в отношенията с държавата и другите политически институции. Най-съществения различие между групите за натиск и политическите партии е в характера на целите. Ако главният стремеж на партиите е завоюването на властта за осъществяване на партийната програма, групите за натиск целят оказване на влияние върху политиката. Партията включва хора с разнообразни интереси и трябва да формулира политически позиции, които имат общ характер, а участващите в групите за натиск преследват специфични интереси и концентрират вниманието си преди всичко върху един или няколко проблема. Днес под групи за натиск (групи по интереси, заинтересувани групи) се има предвид целият арсенал от групи и организации с определена степен на политическа активност, като се започне от синдикатите с голяма членска маса и се стигне до локалните граждански акции от по няколко души. Заинтересувани групи могат да съществуват както в центровете на властта, така и извън тях, да се формират на политическа и извънполитическа основа, да бъдат локални, регионални, национални и транснационални. Могат да бъдат също по-тесни землячески, кланови, етнически или други подгрупи във властовите структури. Борбата между тях за контрол над ресурсите или статусните привилегии обикновено се води задкулисно и негласно, опирайки се преди всичко на лични връзки и ключови фигури. Резултатът, най-общо, е определено преразпределяне на влиянието, на административно-длъжностните позиции.

В страните с либерална демокрация основната функция на групите за натиск е артикулиране на интересите, тоест преобразуване на социалните емоции и очаквания, на чувствата за неудовлетвореност или солидарност на гражданите в определени политически искания, които се довеждат до знанието на вземащите политическите решения. Повдигайки много и разнородни искания, групите за натиск на пръв поглед усложняват, но всъщност оптимизират политическите процеси, защото дават възможност да се видят най-типичните проблеми, да се формулират приоритетите пред държавното управление и в разрешаването на социалните конфликти, да се адаптира управленската програма в съответствие с променящата се среда и оценките на общественото мнение.

В своите действия групите по интереси използват различни методи: подготовка на писма и лични обръщения към законодателите или към представителите на администрацията, организиране на съответна кампания в печата и другите средства за масово осведомяване, провеждане на демонстрации, маршове или някаква друга обществена акция. Широко разпространено средство за въздействие на групите за натиск върху държавните и политическите институции е т.нар. лобиране.

Всичките тези разновидности на властта, които я упражняват пряко или косвено, в по-малка или в по-голяма степен, имат своето влияние върху вземането на решения от властовите органи –

индивидуални (личностни) и групови (колективни) – по отношение на управлението на държава-та, във всички нейни нива и по отношение на всички упражнявани от нея функции.

References

1. Милина, В., „Политически аспекти на сигурността“, ВИ, София, 2003 г.
2. https://www.bg-pravo.com/2009/12/26_13.html, 07.02.2022 г.
3. http://www.bglegis.com/VLAST.html, 08.02.2022 г.
4. https://drugi.dokumentite.com/art/mediite-chetvyrta-vlast-1/83741, 08.02.2022 г.
5. https://wbg.waykun.com/articles/obshhestvena-vlast.html, 08.02.2022 г.
6. https://bg.wikipedia.org/wiki, 09.02.2022 г.
7. http://rechnik.info, 09.02.2022 г.

BASIS OF ANTI-CRISIS MANAGEMENT OF THE STATE ADMINISTRATION

Dimo V. Ginev

Assistant Professor in the Scientific Section "Strategic Research of Security and Defense" of Defence Advanced Research Institute, at the Rakovski National Defense college, d.ginev@rndc.bg

***Abstract**: The report tries to find an elegant answer to some of the academic searches related to the formulation of an acceptable phraseology regarding anti-crisis management. After which, on this basis, the main theoretical and conceptual positions, directly related to the implementation of quality management by the state administration in crises of different nature, are revealed.*

***Keywords**: Crises, public administration, anti-crisis management, bifurcation, reactive, proactive and follow-up actions.*

ОСНОВИ НА АНТИКРИЗИСНОТО УПРАВЛЕНИЕ НА ДЪРЖАВНАТА АДМИНИСТРАЦИЯ

Димо В. Гинев

Главен асистент в научна секция „Стратегически изследвания на сигурността и отбраната“, в Институт „Перспективни изследвания за отбраната“ на Военна академия „Г. С. Раковски“, гр. София, d.ginev@rndc.bg

***Анотация**: Докладът се опитва да намери елегантен отговор на част от академичните търсения, свързани с формулирането на приемливо словосъчетание по отношение управлението в условия на кризи. След това на тази база са разкрити основни теоретични и концептуални постановки, пряко свързани с осъществяването на качествено управление от страна на държавната администрация при кризи от различен характер.*

***Ключови думи**: Кризи, държавна администрация, антикризисно управление, бифуркация, реактивни, проактивни и последващи действия.*

Въведение

Въпросът за антикризисното управление е ключов за оцеляването, съществуването и/или развитието на всяка една държава, независимо от формата ѝ на управление, националната ѝ мощ или от съюзите и коалициите, в които участва. Ефективното противодействие на националните държави на всякакви външни или вътрешни, умишлени или случайни вредни влияния изискват изграждането, поддържането и развитието на адекватни способности за антикризисно управление в държавната администрация. В този контекст за страни като Република България е жизненоваж-

но да бъдат дефинирани основните теоретични постулати и конструкти, касаещи изграждането на способности в областта на антикризисното управление.

1. Държавната администрация в България и антикризисното управление

Понятието „*криза*" е изключително широко използвано в съвременния свят. Терминът присъства перманентно в речника на хората и медиите независимо дали се говори за ситуацията в Украйна, пандемията от коронавируса – COVID-19, изборите за редовно правителство, демографската, енергийната или икономическата ситуация в страната, качеството на образованието, отношенията с Република Северна Македония и т.н. В този ред на мисли голяма част от възникващите и развиващи се събития (случайни или не) с негативен характер, които касаят големи социални групи или образувания, засягат функционирането на част или на цялата държава, най-често се интерпретират с обобщеното понятие „кризи".

В различните клонове на науката кризите се представят и тълкуват по специфичен начин, който най-често се определя от сферата на обществения живот, която е засегната от съответните дестабилизиращи фактори, от причината за тяхното възникване, от нейните мащаби и деструктивност, от прогнозите за развитието, от честотата на проявлението ѝ и т.н. В този социален контекст, кризите се свързват най-вече с устойчивостта на конкретната социална система и възможността ѝ да реагира на проявилите се външни или вътрешни влияния (фактори/дразнения) и/или на конкретната промяна на условията, в резултат на което същата да продължи да съществува и функционира.

За рамките на една държава като Република България основните обстоятелства, от които зависят възможността за превенция, първоначалната реакция и/или последващото управление за неутрализиране или намаляване на последиците от дадена криза, е подготвеността на органите за управление и силите за реакция или така наречените подсистеми за управление и за реагиране. Де факто това са елементите на Националната система за управление при кризи. Същата, след отмяната на Закона за управление при кризи през 2009 г. в настоящият момент е дефинирана бледо в Закона за управление и функциониране на системата за защита на националната сигурност. В действителност в настоящия етап основната тежест при кризи се поема от Единната спасителна система, функционираща в съответствие със Закона за защита при бедствия. Анализирайки нейните елементи и части можем да кажем, че основна отговорност при различните видове инциденти, бедствия и кризисни ситуации има държавната администрация и подчинените им сили (екипи) за реагиране.

Споменавайки *държавна администрация* е важно да се уточни, че под това понятие следва да се разбират съответните органи на изпълнителната власт и подпомагащите ги служители при изпълнение на вменените им отговорности и задължения. Съгласно Закона за администрацията, органите на изпълнителната власт се делят на: централни и териториални. Централните органи на изпълнителната власт са: Министерският съвет, министър-председателят, заместник министър-председателите и министрите. Териториалните органи са: областните управители, кметовете на общини на райони и на кметства и кметските наместници. За органи на изпълнителната власт се считат и председателите на държавните агенции, държавните комисии, изпълнителните директори на изпълнителните агенции, ръководителите на държавни институции, създадени със закон или с постановление на Министерския съвет и др. [1] Тези служители и структури, които подпомагат органите на държавната власт според разпределението на дейностите, които извършват се наричат съответно обща и специализирана администрация. [2] За целта същите се организират в дирекции, чиито функции са разписани в съответните устройствени правилници.

Следователно при поява на индикации за зараждаща се криза или след материализирането на различни рискове в реални заплахи, отчитайки конкретните параметри на ситуацията, държавната администрация следва да предприеме антикризисни мерки по управление на териториално, а при по-крупни кризи и на централно ниво. В това число по превенция, противодействие и/или

ограничаване на последиците от кризата. Естествено запознатите с проблема вероятно ще се запитат защо в доклада е необходимо въвеждането на понятието „Антикризисно управление", вместо широко използваните и вече възприети в държавата понятия: „Управление при кризи", „Управление на кризи" и „Кризисен мениджмънт". Отговорът на този въпрос се корени в дългогодишното и почти безсмислено противопоставяне на тези три понятия.

В научните среди, които се възприема за меродавно „Управлението при кризи", се изхожда от факта, че като цяло кризите трудно могат да бъдат управлявани, тъй като изискват огромен ресурс, капацитет и всеобхватна субординация, с който нашата страна очевидно не разполага, за разлика например от САЩ и Китай. Следователно в такава реалност, според тях е логично да се управлява в условия на кризи. Другата научна група се противопоставя на тяхното мнение с аргумента, че самата архаична формулировка „Управление при кризи" изключва „проактивния" подход и превенцията. Според тези специалисти е необходимо да се управляват самите кризи и по възможност да не се допускат същите да се проявят, затова те се придържат към „Управлението на кризи". Реално в аргументите и на двете групи има смисъл и резон, ето защо най-вероятно третата група, опитвайки се да избяга от това не конструктивно противопоставяне въвежда англоезичния им аналог „Crisis management" или „Кризисен мениджмънт".

Съществува и още едно тълкуване на този въпрос – когато казваме „управление на криза" – то ние се фокусираме върху конкретна кризисна ситуация, а когато използваме словосъчетанието „управление при кризи" - говорим обобщено за различни кризисни ситуации. Ето защо за целите на този доклад, заобикаляйки всички тези противоречия, наслагвани с години в академичния живот на страната, ще използваме понятието „Антикризисно управление".

Под антикризисно управление ще разбираме прилагането на система от целенасочени управленски въздействия от държавната администрация, свързани с неутрализиране както на социални процеси, поведение и дейности на елементите на конкретната социална система, така и с дразнения и/или фактори, касаещи промяна във вътрешните и външни условия. В такъв случай неадекватната или несвоевременна реакция е в състояние да дестабилизира или изведе от устойчиво равновесно състояние конкретната система (държава) и тя да достигне т.нар. „точка на бифуркация".[1] При бифуркацията акцентът най-често се поставя върху необратимостта и непрогнозируемостта на последващите процеси. [3] В този ред на мисли може да се приеме, че антикризисното управление се базира на прогнозиране на опасността от криза (анализ на риска), предварително планиране и поддържане в готовност на силите, извършване на адекватен анализ на симптомите, признаците, рисковете и формите на проявление, вземане на управленски решения от държавната администрация и реализиране на мерки за извеждане на системата от кризата, намаляване на негативните последици от кризата и създаване на условия за стабилизиране и последващо развитие. [4] Предприемане на мерки за недопускане или поне за ограничаване на щетите от подобни ситуации в бъдеще.

В научната литература, когато се изследва съществуването на една социална система или организация, тя се свързва с два паралелно протичащи, но диалектично свързани процеса: на нейното „функциониране" и това на нейното „развитие". Функционирането, от една страна, касае поддържането на живота, запазването на базовите функции, които определят нейната цялост, сигурност, съществени характеристики и взаимоотношения или се основават на промени, базирани на регулаторни въздействия. Развитието, от друга страна, е свързано с преминаването в ново качествено състояние, при което се укрепва жизнената ѝ активност, на фона на постоянно променящата се среда. Последното включва комплекс от въздействия, които последователно променят или актуализират състоянието на системата и нейните характеристики. [5]

[1] Определен момент от времето и пространството касаещ развитието на дадена социална система, в който последиците от външни и/или вътрешни фактори водят до състояние на нестабилност, несигурност и повишен риск за съществуването ѝ. след преминаването на точката на бифуркация.

Функционирането и развитието на системите или организациите са тясно свързани помежду си и отразяват диалектическото единство на двата процеса, отчитайки възможността за възникване и необходимостта от разрешаване на кризи. Функционирането понякога пречи на развитието, защото отнема сили, ресурси и време, но в същото време е и негова „хранителна среда", която го стимулира. Развитието от друга страна също може да отнеме ресурс от съществени за функционирането процеси, но в край на сметка, реализацията му създава условия за последващо по-устойчиво функциониране на цялата система. [6]

Пряката връзка между функционирането и развитието на една система, най-често се свързва с появата на „криза". Навременното разкриване на признаци за поява на предстояща криза, правилното идентифициране на нейната природа, характеристики и причини, своевременната и коректна оценка и последващите реакции са в основата на „проактивното" или „реактивно" антикризисно управление и/или смекчаването на последиците и щетите за системата.

Антикризисното управление може да се сравни с механизма на „Хомеостазата" - свойството на една отворена система, особено на живите организми, да регулира вътрешната си среда така, че да поддържа стабилно, постоянно състояние, чрез многобройни корекции на динамичното равновесие, управлявани от взаимосвързани регулаторни механизми. [7] Тоест при възникване на криза, стремежът е да се запазят основните устойчиви характеристики на системата в определени граници и да не се допусне срив на базовите процеси и дейности, под влияние на външни или вътрешни влияния.

Изследвайки антикризисното управление, важен аспект е изясняването на философията и методиката на основните типове на управление, прилагани при сложни системи. Същите най-общо могат да се диференцират в две основни групи: силно и слабо централизирано управление. *Силно централизираното управление* е ориентирано към изпълнение на цели и задачи, които са предварително определени в каква последователност трябва да бъдат изпълнени или се заповядват в хода на кризисната реакция. В практиката последното е известно като командно-административен тип на управление (институционално) и се характеризира с реализиране на постоянно въздействие и контрол от висшестоящ орган. Подходящо е при сравнително ясна кризисна ситуация и/ или циклично случващи се събития.

Слабото централизирано управление се основава на делегиране на права и задължения на низшестоящите (подчинени) органи, при което им се оставя възможност за инициатива за действия и самостоятелно определяне на последователността за изпълнение на задачите, но в рамките на визията на ръководителя. При този мрежо-центричен метод на управление, отсъства постоянния контрол и въздействието от страна на по-старшия в йерархията орган, но не го изключва. В практиката и най-вече в армията същият се е наложил с името „мисийно" командване и управление, подходящо при неясна ситуационна картина, висока динамика и висока степен на несигурност на развиващите се процеси.

Обобщавайки всичко казано до тук може да се приеме за вярно, че процесът на антикризисно управление на държавната администрация е логическа последователност от предварително планирани, организирани и всестранно осигурени дейности, мероприятия и задачи, основани на набор от утвърдени принципи, предварително изготвени прогнози, допускания, анализ на риска, непрекъснат мониторинг на средата на сигурност, изготвени и синхронизирани разчети на наличните сили, средства и ресурси и проведена качествена подготовка на човешкия фактор от системата, гарантиращ тяхната готовност и наличие на базови способности, които са в състояние да бъдат използвани за реализиране на мероприятия и дейности насочени за превенция, неутрализиране (овладяване) и/или справяне с последиците от различни кризи.

Най-често осъществяването на това управление е свързано с „определяне на целите и задачите на управлението при конкретна криза; събиране на достатъчно информация за кризата; анализ и оценка на обстановката; подготовка и вземане на решения съобразно развитието на кризата; организиране, координиране и контролиране на действията и резултатите от тях по отношение на кризата; осъществяване на след кризисна програма…" [8]

Следователно антикризисното управление реализирано от държавната администрация би следвало да представлява особен микс между науката и изкуството, чиито продукт се основава на предприемането на низ от управленски въздействия, насочени от една страна за мобилизиране, а от друга - за оптимално разпределение на наличните ресурси, при поява на заплахи и/или при индикации за развитие на рискови фактори, които са в състояние да засегнат устойчивото функциониране на системата. Тези управленски въздействия най-често могат да се осъществяват под формата на конкретни проактивни, реактивни и пост-кризисни мерки, действия, реакции, отговори и/или операции.

Качествените *„проактивни" действия* се основават на: реалистични стратегически прогнози (обективен анализ на риска); извършване на качествено предварително планиране и подготовка на елементите на системата; поддържането на определени нива от резерви и запаси; възможността за осъществяване на изпреварващо оповестяване, способността за бърза и реалистична оценка на ситуацията; вземане на обосновани решения за своевременно, адекватно, гъвкаво и ситуативно използване на наличните инструменти и сили. Същите целят недопускане на системата да изпадне в състояние на криза, а ако това не е възможно, то поне значително редуциране както на изненадата, така и на остротата на проява на рисковите фактори.

„Реактивни" действия се предприемат при рязка промяна на динамиката на развитието на рисковите фактори и при поява на конкретни заплахи. Реакцията в случая се разпределя в две направления: незабавни, спешни, аварийно-спасителни и други приоритетни действия и последващи такива. При незабавните действия много важен аспект е приоритизирането на мерките, с цел концентрация на усилията чрез наличните сили, средства и ресурси, чрез които да бъдат минимизирани първоначалните (експоненциално развиващи се негативни процеси). Същите най-често се осъществяват от спешните служби за реагиране (медицински, полицейски, пожарникарски и т.н.) и аварийни екипи на ведомствено и териториално ниво. Тяхната реакция зависи от възможността за бързо оповестяване и/или активиране, готовността действие в динамична среда; от наличието на предварителни планове и стандартни процедури; възможността за координация и взаимодействие по между им.

Последващите действия се основават на осъществяването на непрекъснат мониторинг; на точността на прогнозите за развитието на кризата и оценката на последствията; качеството на работата на екипите подпомагащи ръководителите при вземане на управленски решения; наличието на предварително разработените планове и разчети; осигуряване на реалистична „ситуационна осведоменост"; актуализирането на съществуващите планове и/или разработване на адекватни алтернативи за реагиране; определяне на дефицитите; прилагане на съгласувани и синхронизирани мерки (провеждане на операции в отговор на ситуацията); извършване на преглед и корекция на предприетите действия, при необходимост и т.н.

Изследвайки кризите по отношение на дадена държава, виждаме, че същите могат да включват „система от дипломатически, икономически, политически, информационни, социални, военни, хуманитарни, специализирани полицейски и други дейности". [9] Могат да се реализират като интегрирани или съвместни операции между силите на специализираните служби, ведомствата, другите държавни институции на централната и териториална администрация, различни международни и неправителствени организации, доброволни формирования и т.н.

Ето защо антикризисното управление на държавната администрация изисква прилагането на: целенасоченост, рационалност, благоразумие, трезва оценка на текущата (или възникващата) ситуация и балансирани действия, съчетани с интегрирано и интелигентно използване на икономическите, финансовите, социалните, политическите, духовните, морални [10] и други устои на обществото. Процесът се базира на своевременната, изчерпателната и достоверна информация; възможност за бърз и споделен обмен на данни; наличието на силна политическа воля (в т.ч. компетентно ръководство, подкрепено от добри екипи от антикризисни съветници и/или мениджъри); поддържане на непрекъснат и открит диалог с обществото, за гарантиране на широка обществена подкрепа.

Последното е важно, тъй като обществото е не само обект на управление, но и активен участник (субект) в антикризисните действия. Същото притежава както творчески потенциал да предлага гъвкави и реалистични решения [10] , така и защото е носител на търпимостта, свързана с понасянето на бремето и несгодите, касаещи разрешаването на кризи. Резултатите от реактивните действия целят деескалацията на кризата и разширяване на възможностите за връщане на засегнатата социална система към състояние на стабилност [11] или преминаването ѝ в ново по-качествено състояние.

След установяването на сравнително устойчиво за функционирането на системата състояние, овладяването на основните заплахи или след отшумяването на ескалационните кризисни процеси следва предприемането на *пост-кризисни действия*. За да достигне до тази точка на стабилност, системата е изразходила множество сили, средства и ресурси, в резултат на което се нуждае от период за възстановяване на щетите и последиците. Дейностите тук могат да включват „широк спектър от национални и международни мерки за оказване на помощ и възстановяване на инфраструктурата, социалната система, отраслите на националното стопанство, финансовата стабилност, обществения ред, екологията, здравето и сигурността на гражданите и др.“ [12]

Следващата важна дейност е да продължат процесите за намаляване на „ескалацията“, да не се допусне появата на вторични или третични пулсации, свързани с възобновяване на кризисните процеси и нова дестабилизация на обстановката [13]. Логично е тези дългосрочни дейности да се облекат в „Планове за възстановяване“.

На последно място, но не и по-важност, е извършването на анализ на предварителната подготовка; на планирането; на предприетите действия от участниците по време на кризата; на оценка на тяхната ефикасност; на оценка работата на системата за управление; на разкриване на слабостите и трудностите; набелязване и предприемане „превантивни“ мерки целящи недопускането появата и/или намаляване на въздействието от подобни кризи в бъдеще. В състава на въоръжените сили този процес се нарича „Поуки от практиката“ (Lessons Learned).

Заключение

За да се реализира качествено, своевременно и целенасочено комплекса от тези проактивни, реактивни и пост-кризисни действия в рамките на една страна, е необходимо да бъде изградена Национална антикризисна система на концептуално, нормативно, организационно и техническо ниво. На концептуално ниво трябва да бъдат изяснени фундаменталните принципи и императиви на нейното функциониране. В последствие всички принципи на действие, задължения, отговорности и връзки между елементите на системата трябва да бъдат заложени в правно-регламентиращата база на страната. На тяхната основа трябва да бъдат изградени или трансформирани по функционален признак съответните организационни структури, като единни елементи на системата. Всички те трябва да бъдат свързани посредством технически (оперативно-съвместими една с друга) системи, на базата на които да се извършват всички разгледани управленски антикризисни процеси.

References

[1] Закон за администрацията, Обн. ДВ. бр.130 от 5 Ноември 1998г., посл. изм. ДВ. бр.21 от 13 Март 2020г., чл. 19

[2] Закон за администрацията, Обн. ДВ. бр.130 от 5 Ноември 1998г., посл. изм. ДВ. бр.21 от 13 Март 2020г., чл. 5

[3] Неделчев М., Как периодите поместват литературноисторическите сюжети (2002), Литературен вестник, брой 22, 05.06.2002г. източник: <http://www.slovo.bg/litvestnik/index.php?ar=92> посетен на 22.06.2022 в 09.20 ч.

[4] Охотский Е., Государственное антикризисное управление, източник: <https://studme.org/135023/menedzhment/krizisnoe_razvitie_antikrizisnoe_upravlenie> - посетен на 22.06.2022 в 09.22 ч.

[5] Э. М. Коротков (2014), Антикризисное управление, Юрайт, Москва, ISBN 978-5-9916-3026-9, стр. 18

[6] Э. М. Коротков (2014), Антикризисное управление, Юрайт, Москва, ISBN 978-5-9916-3026-9, стр. 37

[7] waybackmachine, Biology-Innovation, AS & A-Level Biologi Revision, Homeostasis, 15 august (2017), source: <https://web.archive.org/web/20170815140048/https://www.biology-innovation.co.uk/pages/human-biology/homeostasis/> - посетен на 23.08.2022 г. в 14:05 ч.

[8] Гоцев, Г., Управление при кризи, Авангард Прима (2021), София ISBN: 978-619-239-543-8, стр. 34-35

[9] Гоцев, Г., Управление при кризи, Авангард Прима (2021), София ISBN: 978-619-239-543-8, стр. 43

[10] Охотский Е., Государственное антикризисное управление, източник: <https://studme.org/135025/menedzhment/antikrizisnoe_upravlenie_osobennosti> - посетен на 01.07.2022 в 12.22 ч.

[11] Гоцев, Г., Управление при кризи, Авангард Прима (2021), София ISBN: 978-619-239-543-8, стр. 43

[12] Гоцев, Г., Управление при кризи, Авангард Прима (2021), София ISBN: 978-619-239-543-8, стр. 43-44

[13] Тактическа публикация на въоръжените сили на Република България ТП 5-1, Ръководство за планиране на операции част I – Стратегическо ниво (Издание А), МО (2019), София, стр. 72

COMPONENTS AND CAPABILITIES OF THE NATIONAL ANTI-CRISIS MANAGEMENT SYSTEM

Dimo V. Ginev

Assistant Professor in the Scientific Section "Strategic Research of Security and Defense" of Defence Advanced Research Institute, at the Rakovski National Defense college, d.ginev@rndc.bg

***Abstract**: The report attempts to conceptualize the architecture of a future National Anti-Crisis System. Its subsystems and components have been examined in detail and, based on the analysis, the main capabilities that ones should maintain in terms of prevention, neutralization and/or removal of consequences in various crisis situations have been deduced.*

***Keywords**: Crises, National Anti-Crisis System, capabilities, early warning, planning, forecasting, preparation, operations, response.*

КОМПОНЕНТИ И СПОСОБНОСТИ НА НАЦИОНАЛНАТА СИСТЕМА ЗА АНТИКРИЗИСНО УПРАВЛЕНИЕ

Димо В. Гинев

Главен асистент в научна секция „Стратегически изследвания на сигурността и отбраната", в Институт „Перспективни изследвания за отбраната" на Военна академия „Г. С. Раковски", гр. София, d.ginev@rndc.bg

***Анотация**: В доклада е направен опит да бъде концептуализирана архитектурата на една бъдеща Национална антикризисна система. Разгледани са детайлно нейните подсистеми и компоненти и на базата на анализа, са изведени основните способности, които същата би следвало да поддържа по отношение превенцията, неутрализирането и/или отстраняването на последици при различни кризисни ситуации.*

***Ключови думи**: Кризи, Национална антикризисна система, способности, ранно предупреждение, планиране, прогнозиране, подготовка, операции, реакция.*

Въведение

Въпросът за изграждането, поддържането и развитието на способности на държавата за антикризисно управление винаги е бил и ще бъде есенциален по отношение на оцеляването, съществуването и усъвършенстването на конкретната страна. Ефективното прогнозиране, противодействие и ограничаване на вредните последици на всевъзможни външни или вътрешни, умишлени или случайни рискове и заплахи, изисква наличието на многоаспектни и всеобхватни антикризисни способности, поддържане на органите на държавната администрация в готовност за взема-

не на своевременни, обосновани и адекватни решения и поддържане на силите за реагиране в готовност за действие. В контекста на все по-несигурната съвременна среда на сигурност е жизненоважно да бъдат дефинирани структурата и дефицитните способности на Националната антикризисна система, за да могат същите до започнат да се изграждат и развиват поетапно и системно.

Национална антикризисна система и способности

В нормативно-правния регламент на Република България понятието „Национална антикризисна система" не съществува, същевременно обаче е налице „Национална система за управление при кризи". След отмяната на Закона за управление при кризи и направения анализ от образувалия се през годините „вакуум", тази система е дефинирана в Закона за управление и функциониране на системата за защита на националната сигурност. Според него „Управлението при кризи е съществен елемент от дейностите по защита на националната сигурност. Управлението при кризи се осъществява от Министерския съвет чрез Националната система за управление при кризи" [1]. А „Националната система за управление при кризи включва национален, ведомствени и областни ситуационни центрове" [2].

Очевидно е, че тази непълна нормативна „кръпка" и наличието на Единна спасителна система, съгласно Закона за защита при бедствия, не отговарят адекватно на потребността на страната от единна и напълно функционална антикризисна система. Система, регламентирана с отделен закон, която да вменява права, задължения и отговорности на всички държавни и недържавни участници по отношение на кризите, която да обединява наличните „способности" за планиране, подготовка и реакция, която да регламентира управлението (планирането, организирането, ръководството, взаимодействието, мотивацията, контрола и т.н.) от най-високото държавно ниво до изпълнителите, която да се усъвършенства чрез изграждане на нови способности, в унисон със съвременните тенденции и да подържа готовност за реакция, независимо от вида на кризата.

Известен факт е, че всяка една система се състой от определен брой подсистеми, които си взаимодействат посредством различни структурни и функционални механизми, в резултат на което се изпълняват определени процеси, чрез които се реализират предмета и целта, за които са създадени или съществуват самите системи. Следователно за да се изгради антикризисна система на първо място трябва да се определят, кои са **подсистемите и елементите**, които я изграждат. В този ред на мисли условно може да приемем, че Националната антикризисна система може да се състои от: подсистема за мониторинг, предупреждение и оповестяване; подсистемата за предварително прогнозиране, планиране и подготовка; подсистема за кризисно планиране и последващо водене и контрол на операции; подсистема за реагиране включваща всички военни и невоенни сили за отговор и необходимата за целта инфраструктура и оборудване.

Подсистемата за мониторинг, предупреждение и оповестяване. На първо място, непрекъснатия мониторинг на тлеещите, зараждащите се или внезапно появяващите се рискове и заплахи може да се осъществява чрез набор от технически оперативни съоръжения (сензори, камери, спътници, дронове и т.н.) чрез обединяване действието на различни системи и техните прогностични данни и информация (в т.ч. Националния институт по метеорология и хидрология, Агенцията за поддържане и проучване на р. Дунав, Аварийния център на Агенция за ядрено регулиране, Геофизичния институт към БАН, Центърът за аерокосмическо наблюдение на МВР; Националният контратерористичен център към ДАНС; Национална система за спешни повиквания с Единния европейски номер 112 към МВР; Военния команден център към МО; Ситуационния център към МВнР; Националния оперативен център на ГД „ПЗБЗ", Интегрираната система „Синя граница" за наблюдение на нефтени разливи; Националния киберситуационен център на МЕУ; данните получавани от оперативните дежурни на всички останали министерства, ведомства и териториални структури; разузнавателни данни от ДАР и СВР и т.н.) Цялата съвкупна база от всички входящи данни на изброените системи трябва да се концентрира в единно информацион-

но място, свързано с набор от географски информационни системи и други програмни подложки, което да предоставя възможност за тяхната непрекъсната обработка и следене за промяна в състоянието на всеки важен параметър и за прогнозиране развитието. За целта е подходящо всичко това, заедно с подготвени оператори и длъжностни лица (човешки фактор) да бъдат позиционирани в мощен и ефикасен Национален ситуационен (кризисен) център.

Като цяло в държавата голяма част от тези системи съществуват и работят, но автономно и „на парче", следователно е необходимо тези оперативно-технически комплекси и техните продукти просто да бъдат свързани на едно място в ефикасна мрежа, с мощни компютърни системи, програми и подложки, които да подпомогнат изграждането на реална ситуационно осведоменост и възможност за адекватно и бързо прогнозиране.

На второ място тази подсистема трябва да е в състояние да обезпечи потребността за своевременно и адекватно ранно предупреждение и оповестяване. В настоящия момент за целта е изградена *Национална система за ранно предупреждение и оповестяване на органите на изпълнителната власт и населението при бедствия и за оповестяване при въздушна опасност*. Същата включва две подсистеми: система за ранно предупреждение и оповестяване на органите на изпълнителната власт и на съставните части на Единната спасителна система; система за ранно предупреждение и оповестяване на населението. Двете системи осигуряват информация и координация на национално, областно и общинско ниво, както и на кметствата и на отделните населени места чрез: национален контролен възел в националния оперативен център към Главна дирекция „Пожарна безопасност и защита на населението" и чрез алтернативни, регионални, общински и локални контролни възли. [3]

Системата за ранно предупреждение и оповестяване на органите на изпълнителната власт и на съставните части на единната спасителна система (ЕСС) е предназначена за индивидуално предупреждение и оповестяване в зависимост от: вида и мащабите на бедствията; нормативно определените правомощия на органите на изпълнителната власт на различните нива на управление; правомощията на длъжностните лица в администрациите на съответните органи на изпълнителната власт; специфичните функции или предмет на дейност на съставните части на ЕСС [3] За целта в държавните институции се поддържа оперативно дежурство, също така голяма част от ръководителите са включени в автоматичната телефонна система ДАКС, генерираща и кратки текстови съобщения.

Системата за ранно предупреждение и оповестяване на населението е предназначена за едновременното предупреждение или оповестяване на застрашени хора на определена територия за предстоящо или настъпило бедствие и за излъчване на указания за необходимите мерки и действия чрез акустични сигнали и гласова информация. Акустичните сигнали се подават чрез крайни акустични устройства - механични и електронни сирени. Гласовата информация се излъчва чрез крайни акустични устройства - електронни сирени, която се обновява при необходимост. [3] Основните проблеми тук са свързани с факта, че само в 10 областни града е изградена възмож-ността за предоставяне на гласова информация, а населението на останалите градове и села от страната може да разчитат единствено на акустичните сигнали. По този начин обаче последните не получават своевременна информация относно характеристиките на бедствието - произход, мащаби, прогнози за развитие и указания за поведение и действия.

При „въздушна опасност" оповестяването се извършва по подсистема „Сирени", системата за ранно предупреждение и оповестяване на населението, системата за ранно предупреждение и оповестяване на органите на изпълнителната власт и на съставните части на ЕСС, чрез Българското национално радио и Българската национална телевизия [3]. Ето защо е необходимо и двете подсистеми да бъдат модернизирани, така че да оповестяват не само при бедствия, а при всички видове опасни кризи. Логично е също така гласовите съобщения да станат достъпни за всички населени места в страната и за всички обекти от националната икономика. Не по-малко важно е да се обмисли и възможността за изпращането на кратки текстови съобщения от мобилните опе-

ратори за различни метеорологични и други заплахи на гражданите, които е възможно да бъдат засегнати от тях, с включени указания за действия и т.н.

Втората подсистема на Националната антикризисна система трябва да бъде ***подсистемата за предварително прогнозиране, планиране и подготовка***. Последната има изключително важно значение и нейните усилия трябва да бъдат насочени към анализ и оценка на рисковете фактори, наблюдавани и регистрирано непрекъснато от първата подсистема. На базата получените данни и чрез различни допускания, използването на софтуерни и други модели, в нея трябва да може да се извършва прогнозиране на рисковете и заплахите, приоритизиране и реализиране на адекватен анализ на риска. Като последният трябва да отчита вероятните мащаби, дистуктивност, честота на проявление и множество други параметри на зараждащата се или развиващата се криза.

На следващо място различни експертни групи на обектов, общински, областен и национален признак, обединявайки всички разработени продукти до тук трябва да се фокусират върху разработването на планиращи и координиращи документи като: стратегии, програми и предварителни планове. Предварителните планове трябва да включват конкретни мерки, дейности и стъпки, както и всички необходими разчети за тяхното осъществяване, като отговор на конкретни кризи, съобразявайки се с наличните материални, човешки, финансови и информационни ресурси сили и средства.

Същевременно всички тези предварителни планове и разчети е добре да бъдат въведени в единна общодостъпна база от данни и да бъдат проверени чрез извършване на различни тренировки (виртуални – компютърно подпомагани и реални). В съвременния свят се обръща все по-голямо значение на възможността за използване на компютърно моделиране и симулации на всички тези дейности, чрез възможностите на изкуствения интелект.

В настоящия момент в Република България предварителното планиране се извършва чрез разработването на множество планове на национално, областно, общинско ниво. Повече от ясно е, че фокусът е насочен основно към бедствията, в изпълнение на едноименния закон. В тази връзка е разработен „Национален план за защита при бедствия" занимаващ се с: наводнения, земетресения, радиоактивно замърсяване, промишлени аварии, свързани с отделяне на опасни вещества, биологично заразяване, свлачища, суша, заплаха от големи пожари, силни ветрове, обилни снеговалежи, снежни бури и заледяване, инциденти с плавателни съдове, авто-, ж.п.- и авиационни катастрофи, невзривени боеприпаси и др. Съществуват също така: „План за действие при временна закрила в Република България" - при повишаване на миграните потоци в страната, „Национален план за противодействие на тероризма", „Национален авариен план за борба с нефтени разливи в Черно море" и т.н. Основни недостатъци са че същите са разработвани от различни експертни групи, в различни времеви отрязъци, всеки един от тях е индивидуален, прилага различни подходи на управление и че същите не са напълно актуални по отношение на сили, средства и разчети. На тяхна основа са разработени и плановете на ведомствено, областно и общинско ниво.

Ето защо тази подсистема е необходимо да се заеме с актуализирането, дигитализирането и въвеждането им в общата база от данни на всички налични планове и да стартира разработването на нови такива, определени като дефицитни след извършването на качествен анализ на риска в държавата. Всичко това събрано на едно място (в основен и резервни сървъри и т.н.) е в състояние да улесни многократно предварителното планиране, предварителната подготовка на ръководители и участници, както и дейностите свързани с последващото кризисно планиране и предприемане на многократно по-бързи, адекватни и своевременни мерки при всички видове кризи.

Третата ***подсистема*** е тази ***за кризисно планиране и последващо водене и контрол на операции***. Важно е да се уточни, че всяка криза е индивидуална, уникална и със собствени отличителни характеристики, с възможност за множествени каскадни ефекти, материализира се в различни условия и при различни обстоятелства и т.н. Следователно допусканията направени по време на предварителното планиране не винаги придвижат всички параметри. Ето защо почти

винаги се налага на базата вече направените разчети и планове, да бъдат изготвени нови, или актуални планове, адекватни кризисната обстановка. Естествено предварителните планове силно облекчават кризисното планиране и предприемането на незабавни (спешни) мерки и/или операции. Последните се различават най-вече по отношение на последващите действия, касаещи отстраняването на последиците.

В това отношение незаменими помощници са различните компютърни системи, софтуерни подложки и приложения, базирани на изкуствения интелект. Но не бива да се забравя и факта, че човешкия фактор с неговия опит, рутина и най-вече креативно и нестандартно мислене са в състояния да генерират прости и много по-ефикасни решения.

Тази подсистема може да се разглежда и като *управляваща подсистема*. В действителност тя се състой от ръководните органи (централни и териториални), които вземат управленски решения, налагат управленски въздействия, планират и ръководят изпълнението на набелязаните мерки (изпълнението на операции), решават въпросите по взаимодействието с национални и международни органи, доброволни и неправителствени организации и т.н. В тази група влизат също така подпомагащите ги за целта структури и администрации и тези, които ги осигуряват всестранно, в т.ч. технически, софтуерно и др.

Де факто подсистемата се изгражда от една страна от *политическото ръководство* на държавата в лицето на Министерския съвет, Народно събрание, Президент, ръководителите на министерства, ведомства, институции и други организации, подпомагащите ги администрации (самите ведомства – МВР, МВнР, МО, МЗ, МИИ, МЕ, МРРБ, МОСВ, МЗГ., МТС, МЕУ, ДАНС, ДАДРВВЗ, ДАБ и т.н., териториалните органи за управление – областни управители и кметовете, с техните администрации.

От друга страна при кризи свързани с националната сигурност, разгледаните ръководители се подпомагат по различни въпроси от постоянно действащи политически органи наречени *съвети за сигурност*. Последните оказват помощ при планиране, организиране и координиране на усилията и ресурсите на съответните институции. Създават се на национално (Съвет за сигурност към МС, Консултативен съвет за национална сигурност към Президента), ведомствено, областно и общинско равнище, а функциите им са разписани в Закона за управление и функциониране на системата за защита на националната сигурност и правилниците на администрацията.

При конкретна криза, по предложение на съвета за сигурност и при решение на съответния ръководител като временен орган със специфична експертиза на национално, ведомствено, областно или общинско ниво може да се създаде *кризисен щаб*. Той се занимава с планирането, организирането, координирането и контрола на дейността на подчинените сили и средства. Така например Националният кризисен щаб (НКЩ) е временен орган на Министерския съвет за управление при кризи. Той организира, координира и контролира изпълнението на мерките, предприемани от правителството и централните органи на държавната власт, насочени към предотвратяване, ограничаване или разрешаване на конкретна криза, и оказва помощ на ведомствените и на териториалните органи в дейността им при кризисната ситуация. Министър-председателят може да ръководи лично НКЩ или, в зависимост от характера и параметрите на кризата, да възложи това на свой заместник или друг член на правителството. А резултатите от работата на Националния кризисен щаб се оформят като заповеди, решения, разпореждания и други документи [4].

Всяко министерство и агенция със заповед на съответния ръководител формира свой ведомствен кризисен щаб. Обикновено той е временен орган за управление, който е в основата на планирането, организирането, координирането и контролирането на действията на силите на ведомството при различни кризи. Щабът се ръководи от ръководителя на звеното по „ОМП" в институцията или от друг ръководен служител и включва служители от администрацията и структурите по различни направления на дейност, имащи съответните компетентност и подготовка. Областният (общинският) кризисен щаб се създава за координиране и контролиране на изпълнението на предприетите от съвета по сигурността антикризисни мерки в рамките на неговата административно-териториална компетентност, както и за оказване на помощ на подчинените звена,

на органите на държавната власт или на органите за местно самоуправление в дейността им при конкретни кризи. Кризисните щабове на областно и общинско равнище работят непрекъснато при възникване на кризисна ситуация до нейното предотвратяване, овладяване или разрешаване, а в определени случаи – и при ликвидиране на последствията от нея. [5]

Основните предизвикателства на държавата свързани с тази подсистема е необходимостта от унифициране на терминологията (например използват се думите оперативен, координационен, кризисен и друг щаб), разписването на ясни и еднотипни методологии и процедури за вземане на решения и планиране, дефиниране на подчинеността, взаимовръзките и взаимодействието на различните органи при кризи и т.н. Всичко това е логично да се обвърже в конкретен нормативен акт.

Четвъртата подсистема е ***подсистемата за реагиране***. В нея влизат всички военни и граждански сили и средства, които могат да бъдат използвани за превенция, разрешаване и/или минимизиране на последиците от кризи. В това число са силите на всички министерства и ведомства (като: МВР, МО, МЕ и т.н.), структури на администрациите на органите на изпълнителната власт, формирования на юридическите лица, екипи на центровете за спешна медицинска помощ, на други лечебни заведения или на здравни заведения, доброволни формирования по Закона за защита при бедствия. [6]

Анализът на регулярно и инцидентно случващите се в държавата кризисни ситуации показва, че на практика основната тежест при вътрешни кризи се поема от Министерството на вътрешните работи. Не случайно в структурата и организацията на същото е предвидено непрекъснато добиване на криминална и друга информация от всички сектори на обществения живот. Също така в него са позиционирани и основните сили (ГДЖСОБТ, ГДГП, ГДБОП и т.н.) осигуряващи поддържането на вътрешна сигурност и обществен ред дори при най-тежките социални сътресения като: масови безредици, бунтове и гражданска война.

Когато кризата е от военнополитически характер в или в близост до държавната граница, приоритет за нейното предотвратяване или овладяване има Министерството на отбраната (МО). При различни бедствия, при засилен мигрантски натиск на държавната граница, влошена пандемична обстановка и др. МО поддържа над 100 подготвени, оборудвани и екипирани формирования за оказване на гражданска помощ при бедствия.

Всички останали ведомства създават и поддържат в готовност сили и екипи за неутрализиране на кризи в областта, в която са отговорни. Така например Министерството на енергетиката поддържа аварийни екипи по отношение на прекъсването на преноса на ток, топлоенергия, нефт и газ. Министерството на околната среда и водите поддържа Националната автоматизирана система за непрекъснат контрол на радиационния гама–фон (BULRaMO), локални мониторингови станции регионални инспекции, специализирани и регионални лаборатории за контрол на качеството на атмосферния въздух и течащите повърхностни води. Министерството на земеделието - специализирана лаборатория и подстанция на системата за ранно оповестяване при радиационно окачествяване на поразени растителни суровини и храни, Централна лаборатория по ветеринарно-санитарна експертиза и екология; Централна лаборатория по карантина на растенията и Централна лаборатория за химически изследвания и контрол и др. Всички останали ведомства също поддържат сили, средства и екипи в областта им на компетенция.

Друг много важен елемент в тази подсистема са силите на Българския Червен кръст включващи: екип от спасители за работа при водни инциденти, екип от планински спасители за издирване на пострадали; екипи от професионални психолози, при бедствен стрес, имущества от първа необходимост за подпомагане на бедстващото население – за 5 000 човека и т.н.

За подпомагане на защитата при бедствия се ползват доброволци, организирани в доброволни формирования. Доброволните формирования се създават от кмета на общината по решение на общинския съвет. Редът за тяхното създаване и организиране на дейността им се определя с наредба на Министерския съвет. Отчета или регистъра на доброволните формирования в страната се води в Главна дирекция „Пожарна безопасност и защита на населението" – МВР. [7]

Добре би било всички сили, средства, техните възможности, дислокация и актуално състояние да са въведени в единната цифрова база данни, която е достъпна 24/7 от всеки един национален, ведомствен или териториален ситуационен център. По този начин всички разгледани подсистеми ще са в състояние да планират, организират и осъществяват действия, задачи или операции в отговор на всевъзможни кризи.

Последния компонент на Националната антикризисна система ***са необходимата за целта инфраструктура и оборудване***. Най-важните елементи в нея се явяват мрежата от национален, ведомствени и териториални ситуационни центрове и тяхното оборудване с комуникационно-информационни системи, подложки, софтуер и пълен набор от актуални бази данни, поддържането на оперативно дежурство и залагането на ефикасни процедури за непрекъсната работа, планиране, вземане на решения и осъществяване на контрол на силите за реагиране на терен. При кризи в ситуационните центрове ще работят съответните ръководители, подпомагащите ги съвети за сигурност и кризисните щабове.

На основата на взаимодействието между всички подсистеми и компоненти Националната антикризисна система трябва да поддържа определени способности и готовност за проактивни, реактивни и/или пост-кризисни реакции. В този контекст **основните способности**, които тази система трябва да изгражда, поддържа и развива са:

– извършване на непрекъснат мониторинг на средата на сигурност;
– улавяне и регистриране на динамиката и изменението в развитието на рисковите фактори, в реално време;
– подпомагане извършването на анализ на рисковете, тяхното приоритизиране и прогнозиране на развитието им;
– обезпечаване извършването на предварително планиране, основано на пакет от реалистични сценарии;
– поддържане в готовност на подготвени и добре екипирани професионални и доброволни формирования за действие в случаи на кризи [8] чрез регулярно обучение на персонала и осъществяване на пълноценна подготовка;
– осигуряване на възможност за незабавно оповестяване на компетентните органи, подпомагащия ги състав и силите за реагиране;
– реализиране на ранно предупреждение на застрашените групи от населението;
– предлагане на набор от превантивни и/или незабавни и последващи мерки за: предотвратяване разрастването на кризата, нейното овладяване или за ограничаване (ликвидиране на последиците);
– подпомагане кризисното планиране и вземането на управленски решения съобразно развитието на кризата;
– непрекъснато изобразяване или показване на кризисната ситуация чрез географски и други софтуерни и информационни приложения;
– предлагане на набор от инструменти за повишаване ефективността на организирането, координирането, взаимодействието и изпълнението на конкретните мероприятия или реакции между участниците на терен и ръководния състав;
– поддържане на непрекъсната комуникация в реално време (в т.ч. и висококачествен видео обмен) между всички участници в антикризисната система и предоставяне на възможност за осъществяване на контрол и корекция на предприетите управленски реакции;
– предоставяне на възможност за заявяване и планиране на международна помощ (от ЕС, НАТО или съседни страни);
– поддържане на способности за адекватна защита и/или евакуация на граждани, разсредоточаване на животни, материални и културни ценности, провеждане на аварийно-спасителни дейности, възстановяване работата на засегната критична инфраструктура и др.;
– подпомагане разработването на ефикасна след кризисна възстановителна програма;

– предоставяне на инструментариум за извършване функционален анализ, анализ на ефектите от кризата, оценка на ефективността на предприетите антикризисни мерки;

– планиране на мерки с оглед недопускане сходни кризи или за минимизиране на последиците и т.н.

Заключение

За осъществяването на качествени, своевременни и целенасочени проактивни, реактивни и пост-кризисни действия в рамките на една държава, е необходимо да бъде изградена напълно функционираща Национална антикризисна система. В структурно отношение същата може да включва: подсистема за мониторинг, предупреждение и оповестяване; подсистема за предварително прогнозиране, планиране и подготовка; подсистема за кризисно планиране, последващо водене и контрол на операции; подсистема за реагиране, включваща всички военни и невоенни сили за отговор и необходимата за целта инфраструктура и оборудване. На тази основа системата може да изгради, развие и поддържа широк набор от способности за работа преди, по-време и след кризисни ситуации.

References

[1] Закон за управление и функциониране на системата за защита на националната сигурност, В сила от 01.11.2015 г., Обн. ДВ. бр.61 от 11 Август 2015г., посл. доп. ДВ. бр.15 от 22 Февруари 2022г., чл.18

[2] Закон за управление и функциониране на системата за защита на националната сигурност, В сила от 01.11.2015 г., Обн. ДВ. бр.61 от 11 Август 2015г., посл. доп. ДВ. бр.15 от 22 Февруари 2022г., чл.17

[3] Наредба за условията и реда за функциониране на националната система за ранно предупреждение и оповестяване на органите на изпълнителната власт и населението при бедствия и за оповестяване при въздушна опасност, Приета с ПМС № 48 от 01.03.2012 г., посл. изм. доп. с Постановление № 265 от 2 август 2021 г. Обн. ДВ. бр.65 от 6 Август 2021г.

[4] Гоцев, Г., Управление при кризи (2021), Авангард Прима, София, ISBN: 978-619-239-543-8, стр. 103-104

[5] Гоцев, Г., Управление при кризи (2021), Авангард Прима, София, ISBN: 978-619-239-543-8, стр. 104-105

[6] Гоцев, Г., Управление при кризи (2021), Авангард Прима, София, ISBN: 978-619-239-543-8, стр. 108

[7] Гоцев, Г., Управление при кризи (2021), Авангард Прима, София, ISBN: 978-619-239-543-8, стр. 108

[8] Гоцев, Г., Управление при кризи (2021), Авангард Прима, София, ISBN: 978-619-239-543-8, стр. 95

MODERN CONCEPTS OF CONDUCTING A NAVAL LANDING OPERATION

Krasimir Kostadinov

GSM: +359887247435; e-mail: kraspk@abv.bg

***Abstract**: The report provides a historical overview of some typical amphibious operations carried out during the two world wars and sea landings carried out by the Bulgarian Army. The organization of actions, the tasks envisaged for execution and the forces involved in a naval landing operation are analyzed. As a result, conclusions were drawn, determining the conduct of a modern naval amphibious operation.*

***Keywords**: Maritime interdiction operations, Intelligence, Maritime security, NAVY, Surveillance.*

СЪВРЕМЕННИ СХВАЩАНИЯ ЗА ПРОВЕЖДАНЕ НА МОРСКА ДЕСАНТНА ОПЕРАЦИЯ

Красимир Костадинов

Провеждането на морски десантни операции датира от времената, когато човечеството е започнало да използва плавателни средства за военни цели. Още тогава е била осъзната и използвана възможността да се транспортират хора (войски, сили) през водни препятствия (морета, езера, реки), да се стоварят на територия, където да изпълнят определени задачи. С течение на времето и развитието на технологиите се променят както плавателните средства, така и начинът за тяхното използване за постигане на целите.

Една от най-мащабните морски десантни операции, позната на човечеството е десантът в Нормандия, позната още като операция „Овърлорд", осъществена през Втората световна война. Тя започва на 6 юни 1944 г., когато 5000 десантни кораба и плавателни средства, 289 ескортиращи кораба, 577 миночистачи и над 160000 войници преминават Ламанша и десантират на северното френско крайбрежие. В операцията участват 10 танкови дивизии и 11000 самолета. Тези цифри сами по себе си говорят за мащабите на военните действия. Самата операция продължава над два месеца, като броя на участващите войски достига 875000 човека. Само за една нощ, на 6 юни загубите на съюзниците възлизат на 10500 – убити, ранени, пленени или изчезнали войника.

Една от първите морски десантни операции за младата, все още българска армия е осъществена през Първата световна война в района на гр. Балчик. След включването на Румъния на страната на Съглашението през 1916 г. то тя се оказва противник на България и възниква необходимост да се осигури десния фланг на Трета българска армия, която действа в Добруджа. Целта на десанта е да се овладее морското крайбрежие на Балчик, Каварна и нос Калиакра и да се възпрепятстват евентуални удари от противника. На 5 септември в 1 часа и 30 минути торпедоносците „Смели", „Строги", Летящи", „Шумни" и „Храбри", заедно с три големи гребни лодки, които са буксирани, потеглят от гр. Варна. Около два часа по-късно те стоварват отряди в Балчик, Ка-

варна и н. Калиакра. Първоначалната численост на десанта е 235 човека. Операцията продължава през деня на 05 и об септември, като се прехвърлят още Портовата дружина на флота в състав от 466 човека и наблюдателна полурота с численост 44 души.

Друга морска десантна операция, проведена на по-късен етап е десантът на американски войски и окупиране на Гренада – държава от Карибския регион, чиято армия наброява около 1000 души. Операцията започва в 6 часа сутринта на 25 октомври 1983 година, като планът предвижда да се проведат внезапно и едновременно въздушен и морски десант и да се овладеят важни стратегически обекти. В операцията вземат участие сили на втори Американски флот, сухопътните и военновъздушните сили, като са сформирани - авионосна десантна група в състав от 12 кораба, начело със самолетоносача „Индипендънт". От ВВС участват 8 изтребителя F-15, самолети за радиоелектронна борба ЕС-130, 3 самолета за далечно радиолокационно откриване, около 60 транспортни самолета С-5А. Общата численост на десанта възлиза на 5000 души. Въпреки предварително планираните и проведени учения и голямото превъзходство в огнева мощ от страна на САЩ е нужно да се отбележи факта, че операцията протича силно дезорганизирано. Несъгласуваните действия, неправилните оценки и субективни действия създават хаос при провеждането, сравнително много жертви и загуба на техника (19 американски войници са загинали и 8 хеликоптера са унищожени).

Изложените факти от провеждането на някои характерни десантни морски операции през двете световни войни и по-новата история недвусмислено показват, че осъществяването на такова военно мероприятие е свързано с участие на разнородни сили, изисква детайлна организация, план на провеждане и точно изпълнение на поставените задачи. Напрежението на силите е огромно, загубите са големи и успеха не е гарантиран от превъзходството в определена област.

Като форма на военни действия морската десантна операция представлява провеждането на синхронизирани бойни действия, включващи формирования от видовете и родове сили. Бойните действия за стоварване на морски десант са съвкупност от съгласувани по цел, място и време и провеждани по единен замисъл и план бойни действия на съединенията и частите на флота и сухопътните войски, подкрепяни от военновъздушните сили за стоварване на морски десант на територия, отбранявана от противника и за изпълнение на поставените им задачи на брега.

В съюзните публикации, както и в доктрината за морски операции НП-3.1 тези действия са определени като амфибийни бойни действия. „Амфибийните бойни действия включват синхронизирани бойни действия на всички видове кораби, подводници, авиация и формирования на въоръжените сили, водещи своето начало от морето. Основна цел е стоварването на брега на войски , сили и средства или тактически групи".

Съставът на морския десант се определя, като се изхожда от поставената бойна задача, обстановката в района на стоварването и продължителността на самостоятелните действия на десанта на брега.

В зависимост от целите на десантните действия и състава на участващите сили десантите се подразделят на:

- оперативно-стратегически - стоварва се групировка, включваща съединения и части от различните видове въоръжени сили;
- оперативни - стоварват се няколко оперативно-тактическо формирования (механизирани бригади и бригада морска пехота);

- оперативно-тактически - стоварва се едно усилено оперативно-тактическо формирование;
- тактически - механизирана (танкова) бригада, бригада морска пехота или усилен механизиран батальон;
- със специално назначение - стоварва се войсково подразделение до рота за изпълнение на диверсионни и разузнавателни задачи.

Морските десанти се стоварват за постигане на определени цели, които могат да бъдат:

- овладяване на проливни зони, важни райони на крайбрежието и острови, военноморски бази и други брегови обекти на противника, важни за достигане на желаното крайно състояние;
- съдействие и подпомагане на войските, действащи на приморското направление.

За стоварването на морски десант се привличат съединения и части на сухопътните войски, ВВС и ПВО и всички родове сили на ВМС. За всеки район за стоварване се формират сили за стоварване, които са предназначени за осигуряване прехода на десанта по море, стоварването и поддържане действията на брега. За командир на силите за стоварване се назначава един от командирите на съединения на флота. Той отговаря за товаренето на десанта, прехода му по море, стоварването на десанта в назначения район, провеждането на огневото осигуряване на развръщането на силите за стоварване, огневата подготовка, огневата поддръжка на стоварването и огневото съпровождане на действията на десанта на брега, за отбраната и защитата на десанта при прехода по море, за подвоза на материални средства и за евакуацията на ранените и болните.

За провеждане на десантна операция се формират различни по състав и задачи групи, които имат за цел да осигурят десантиращите сили в различни направления. Силите за стоварване включват: десантни отряди, отряд кораби за огнева поддръжка, ударни, поисково-ударни групи, осигуряващи групи, група кораби за охрана на водния район, база на стоварването, демонстративни и лъжливи групи от кораби.

Десантните отряди (ДЕСО) са предназначени за превоз на войските от десанта и стоварването им в назначените райони и включват десантни кораби, транспорти, сили за охранение и осигуряване. За командир на ДЕСО, включващ десантни кораби се назначава, като правило се назначава командира на съединението десантни кораби. За командир на ДЕСО, включващ транспортни кораби - командира на силите за охранение на този десантен отряд.

Отрядът кораби за огнева поддръжка (ОКОП) е предназначен за решаване на задачите по огнево осигуряване на развръщането на силите за стоварване, огневата подготовка, огневата поддръжка на стоварването и огневото съпровождане на действията на десанта на брега и включва ракетно-артилерийски (патрулни) кораби и катери. На прехода по море корабите от ОКОП могат да се използват за отбрана на предните десантни отряди. За командир на ОКОП се назначава командира на съединението ракетно-артилерийски (патрулни) кораби.

Корабните ударни групи (КУГ) са предназначени за отбрана на десантните отряди на прехода по море и в района на стоварването и включват ракетно-артилерийски кораби и катери.

Корабните поисково-ударни групи (КПУГ) са предназначени за поиск и унищожаване на подводниците на противника в района за формиране на ДЕСО, на прехода по море и в района за стоварване и включват в състава си патрулни кораби.

Осигуряващите групи се създават в зависимост от замисъла за действия, обстановката на прехода по море и в района за стоварване.

Миночистачните групи (МЧГ) са предназначени за осигуряване безопасността на корабите от мини в района за формиране на ДЕСО, на прехода по море и в района за стоварване и включват миночистачните кораби от различни подкласи.

Групите за разграждане са предназначени за прокарване на проходи в ПДЗ във водата и на брега в пунктовете за стоварване. Състоят се от подразделения сапьори и леководолази, заделени от инженерните части на ВМС и десанта, а също така от кораби и катери, оборудвани със средства за разминиране.

Групите за разузнаване и наблюдение са предназначени за своевременно откриване на въздушния и надводния противник, оповестяване за него силите за стоварване и даване по целеуказване на ударните сили и включват кораби и летателни апарати, както и брегови РЛС.

Групите за радиолокационен дозор се състоят от кораби и летателни апарати за радиолокационен дозор с пунктове за управление и навеждане на изтребителната авиация и са предназначени за своевременно откриване на въздушния противник и насочване към него на изтребителната авиация.

Групите за радиоелектронна борба (РЕБ) включват надводни кораби и самолети (вертолети), оборудвани със средства за РЕБ, а също така и подразделения и части за РЕБ на ВМС. Те са предназначени за подавяне на радиоелектронните средства за управление на силите и оръжието на противника.

Хидрографските групи се състоят от кораби и части на хидрографската служба на флота и са предназначени за осигуряване на товаренето, прехода по море и стоварването на десанта, а също така действията на ОКОП и тралните групи.

Маневрените поисково-спасителни отряди се състоят от кораби, предназначени за поисково-спасително осигуряване на десанта при прехода му по море и в района за стоварване.

Отрядите кораби за логистично осигуряване са предназначени за попълване на запасите от материални средства и за техническо осигуряване на силите за стоварване при прехода по море и в района за стоварване.

Съединението (групата) кораби за охрана на водния район е предназначено за осигуряване на видовете отбрани[2] на десантните кораби в района на стоварването. В него се включват кораби, самолети и вертолети от състава на силите за охранение на десантните отряди и от други групи, които с пристигането си в района на стоварването се престрояват в предварително определения боен ред. За командир на охраната на водния район се назначава един от командирите на съединения патрулни или миночистачни кораби.

Лъжливите групи (отделни кораби) се включват в състава на ДЕСО с цел заблуждаване на противника относно неговия състав и за отвличане по тях атаките и оръжието му.

Демонстративните групи са предназначени за демонстриране стоварване на десант на лъжливо направление и затрудняване на противника в разкриването на главното направление на стоварването на десанта.

В зависимост от конкретната обстановка в района на прехода и стоварването на десанта от мащабите на десантните действия и наличните сили могат да се създават не всички, а само част от разгледаните групи или да се съвместят функциите на различните групи. Например при отсъствие на минна опасност не е необходимо да се създават миночистачни групи, а при скритно стоварване на неголеми подразделения могат да отсъстват ОКОП и други групи.

[2] Противовъздушна, противоподводна, противокорабна, противоминна и пр.

Морската десантна операция, разгледана като вид военни действия, притежава някои особености, които определят положителните и негативните ефекти от нейното провеждане.

На първо място провеждането на морски десант срещу добре подготвена, ешелонирана и организирана отбрана би довело до значителни загуби, които ще създаде деморализиращ ефект върху войските и отрицателно настроение на общественото мнение. Тези действия са характерни и са се използвали през първата и втората световни войни, но в днешно време, въпреки осигуряването на успех, не са приемливи.

От друга страна стоварването на десант на бряг, който не е оборудван и не се отбранява ангажира голям ресурс от осигуряващи сили и средства, който може да бъде използван в други направления и за решаване на други задачи.

Съвременните морски десантни операции могат да бъдат проведени в различни условия. Тези условия са определени от степента на подготовка на противника, оборудване на района в противодесантно отношение, използване на високоточни противокорабни ракетни комплекси с голяма ефективност. Тези условия, както и задачите, които са предвидени за изпълнение са определящи и за избора на сили, средства, както и за вида на десанта – морски или въздушен.

В днешно време предварителната подготовка и оборудване на десантно-опасните участъци в съчетание с използването на ефективни ракетни и артилерийски системи, както и възможността за ранно предупреждение за предстоящи морски десантни действия все повече изключват или минимизират възможността за провеждане на морска десантна операция от мащаба и вида на „Нормандия". Ефектът от използването на големи по мащаб и огневи потенциал сили не е съизмерим със загубите, които ще се получат и ефекта, който ще се предизвика в обществото. За да се избегнат тези негативни моменти и в същото време да се постигнат целите, все повече се използват десантни групи от сили за специални операции. Те се транспортират основно с въздушен транспорт до района за десантиране в тъмната част от денонощието или в условия на затруднена видимост. Основната цел на тези десанти е да се неутрализира съпротивата и се сведат до минимум отбранителните способности на противостоящите сили, да се овладеят важни обекти от системата за брегова отбрана, комуникации и критична инфраструктура. Успоредно с това се осигуряват райони за дебаркиране на десантни съдове, които да стоварят основната част от собствените сили.

В тази ситуация и при такава организация също съществува вероятност от нанасяне на удари по основните десантиращи сили, но те са по-скоро единични, от далекобойни системи и изтребително-бомбардировъчна авиация. В този случай е необходимо да се осигури надеждна противовъздушна и противоракетна отбрана. Разбира се, за да се гарантира успеха и да се сведат загубите до минимум е задължително осигуряването на всички видове охрани и отбрани.

От изложените факти и анализи могат да се направят следните изводи:

- десантната операция е сложна бойна дейност и изисква осъществяване и съгласуване на различни по характер съвместни действия от видовете и родовете сили;
- провеждането на десантна операция изисква ангажирането на значителен ресурс от сили и средства;
- в съвременни условия провеждане на мащабна морска десантна операция, включваща активни бойни действия е малко вероятно.

- в зависимост от целите и задачите, които се планират е удачно десантните действия да се провеждат от сили за специални операции, чрез използване на въздушен транспорт, които да осигурят район за стоварване на основните сили.

Военноморската история познава не един случай, в който морската десантна операция, като особено сложна съвместна операция на въоръжените сили при водене на бойни действия на Приморското направление, е заемала основното съдържание на въоръжения конфликт. При това неуспехът при организирането на противодесантната отбрана на крайбрежието най-често е водил до загуби за отбраняваната страна в оперативен или стратегически мащаб. Ето защо теоретичните основи на десантните действия заемат важно място в оперативно-тактическата подготовка на военноморските офицери. Чрез тях командния състав от ВМС получава необходимите знания за организиране и водене на широк кръг отбранителни и настъпателни бойни действия. Не на последно място тази теория в значителна степен осигурява и подготовката на силите за участие в небойна евакуационна операция на съединение от многонационални сили, като специфична форма за използване на ВМС в мирно време.

References*:*

1. КОЖУХАРОВ, А. (2007) *Морските десанти през двадесетия век*, Варна, издателство „СЛАВЕНА".
2. АТР-8(С), (2017) Doctrine for Amphibious Operations.
3. *Доктрина за морски операции*, НП-3.1, (2013).
4. ЙОРДАНОВ, Ж. *Взаимодействие между въоръжените сили и институциите при защита на сигурността в литоралната зона*, (2018) доклад на международна научна конференция в НВУ „В. Левски", факултет „А, ПВО и КИС" , Шумен, ISSN: 2367-7902.
5. ЧАЛЪКОВ, Р.,ИЛИЕВ, К. (2017) *„Съвместна огнева поддръжка" – фактор в съвременните операции,* сборник доклади от международна научна конференция, НВУ, Факултет „Артилерия, ПВО и КИС"*„с. 158-166,* Издателски комплекс на факултет „Артилерия, ПВО и КИС", Шумен, ISSN 2367-7902.
6. ЧАЛЪКОВ, Р.,МАРКОВ, Д. (2018) *Фактори влияещи на огневата поддръжка в операции*, International Scientific Conference Collectionofpapers, Shumen, Bulgaria.

PARTICIPATION OF NAVAL SURVEILLANCE AND COMMUNICATION (SAC) UNITS IN MARITIME INTERDICTION OPERATION

Zhivko St. Yordanov

GSM: +359887881809; & +359895456954; e-mail: sas_81@abv.bg

Abstract: The Naval surveillance and communication (SAC) units carry out a continuous duty of surveillance of national maritime spaces, thus participating in the full spectrum of maritime operations, including Maritime interdiction operations (MIO)

.

Keywords*: Maritime interdiction operations, Intelligence, Maritime security, NAVY, Surveillance;*

УЧАСТИЕ НА ФОРМИРОВАНИЯТА ЗА НАБЛЮДЕНИЕ И СВРЪЗКА (НиС) ОТ ВМС В ОПЕРАЦИЯ ПО КОНТРОЛ НА КОРАБОПЛАВАНЕТО

Капитан II ранг д-р Живко С. Йорданов

Формированията за наблюдение и свръзка от ВМС носят непрекъсната служба по наблюдение на националните морски пространства, поради което участват в целия спектър морски операции, в това число и операции по контрол на корабоплаването. Според Доктрината за морските операции (НП – 3.1), контрола на корабоплаването е определен като способност на ВМС за участие в мисиите на въоръжените сили[3]. Публикацията на НАТО АТР-71 определя контрола на корабоплаването като: операция по поиск, откриване, следене, разпитване, а когато е необходимо качване на борда на плавателния съд и извършване на проверка на документите, екипажа и товара[4]. За целите на настоящият доклад ще използвам определението дадено в АТР-71, тъй като определя в по-голяма степен съдържанието на операция по контрол на корабоплаването и изчерпателно изброява тактическите действия, които се извършват в подобна операция. Според АТР-71 контрола на корабоплаването включва следните тактически действия:

- разпитване на плавателния съд;
- отклоняване на кораби, които нарушват правилата за корабоплаване и/или не изпълняват указанията на органите по контрол на корабоплаването;
- изпращане на въоръжена група за качване на кораба с цел проверка на документите, екипажа и товара на кораба;
- събиране на доказателства за превозване на забранени стоки и предмети;

[3]МО*(2013) Доктрина за морските операции НП-3.1.Варна: стр. 15, т.35;*
[4] NATO *(2005)* ATP-7.1. *ALLIED MARITIME INTERDICTION OPERATIONS, 1-1, 102;*

- задържане на кораби и техните товари, които не изпълняват разпорежданията за извършване на проверка или превозват забранени стоки и продукти;

Операциите по контрол на корабоплаването са критично зависими от системата за наблюдение за събиране, обработка и разпространение на информация относно корабите в зоната на отговорност и тяхното движение, както и за подозрителни плавателни съдове или плавателни съдове без средства за опознаване, с подозрително (нехарактерно) движение и маневриране, или с които не може да се осъществи радиовръзка. За да бъде една операция по контрол на корабоплаването успешна е необходимо всички кораби в зоната за отговорност да бъдат открити и да бъдат определени техните елементи на движение (курс, скорост и т.н.). Формированията за наблюдение и свръзка от ВМС имат за задача да осигурят непрекъснато наблюдение на националните морски пространства, чрез което се изгражда единна опозната картина на морската обстановка(ОКМО) и да осигурят съответния командир провеждащ морска операция. Поради тази причина, формированията от бреговата система за наблюдение вземат участие в операциите провеждани в националните морски пространства в това число и операциите по контрол на корабоплаването като събират и обработват информация за надводната обстановка, която служи за вземане на решение от ръководителя на операцията за предприемане на съответни действия за проверка на плавателен съд и има за цел изпълнение на следните задачи:

- откриване на всички плавателни съдове и средства в зоната за отговорност;
- идентифициране на всички плавателни съдове и средства;
- установяване на плавателни съдове от интерес;
- проследяване на плавателни съдове от интерес;
- определяне на елементите на движение на целите и техните намерения;

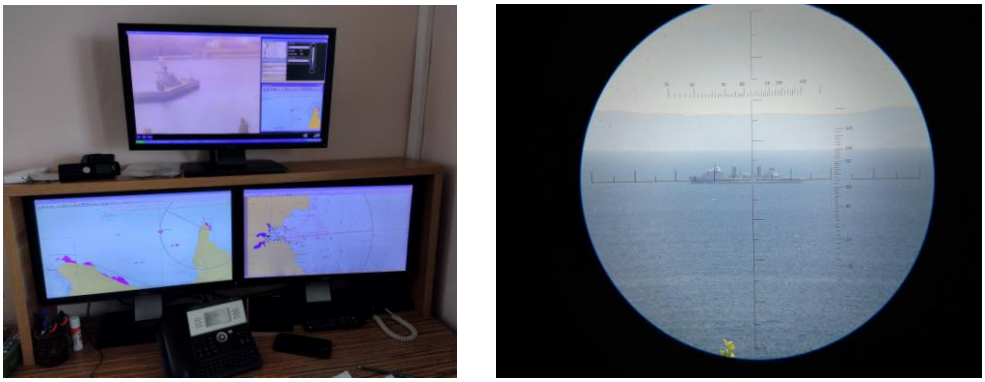
За изпълнение на тези задачи, формированията за наблюдение и свръзка следва да използват наличното въоръжение на поста като радиолокационни станции за наблюдение на морските пространства, средствата за визуално наблюдение (видеокемри за дневно и нощно виждане, оптически прибори за наблюдение, прибори за нощно виждане и др.) и средствата за свръзка с корабите на море, които се намират на поста. Наблюдението на заподозрян плавателен съд е от ключово значение за събиране и обработване на разузнавателна информация и информация за действията на плавателния съд в националните морски пространства както и за извършване на незаконни действия от кораба и екипажа като:

- пренасяне на забранени (ембаргови) стоки – бреговото наблюдение трябва да открие и идентифицира плавателния съд, да определи елементите на движение на целта, да установи пристанището на отплаване и пристанището определено като крайна точка на товара, името на корабособственика и да открие несъответствия между обявената информация и реалния статус на плавателния съд;
- трафик на оръжие и наркотици – формированията за наблюдение и свръзка могат да водят непрекъснато наблюдение на кораби от интерес и/или заподозряни, в превозването на забранени стоки и вещества като оръжие и наркотици;
- предотвратяване на екологична заплаха – откриване, следене и докладване на кораби, които замърсяват морските пространства или нарушават законодателството свързано с екологията и опазване на околната среда;
- наблюдение и откриване на малки лодки и рибарски кораби – откриване и установяване на рибарски кораби, които нарушават закона или извършват риболов в забранени райони;
- превозване на бежанци – формированията за наблюдение и свръзка могат да следят плавателни съдове, за които има разузнавателна информация, че превозват бежанци и да подпомагат силите за откриване на плавателния съд и предприемане на съответните действия за проверка, установяване и задържане на кораба и лицата, които превозва;

За участие в операции по контрол на корабоплаването и изпълнение на горепосочените задачи и описаните действия формированията за нблюдение и свръзка могат да изпълняват следните действия:

- поиск, откриване и опознаване на надводни цели;
- визуално откриване, опознаване и наблюдение на надводни цели;
- следене на кораби други плавателни съдове от интерес;
- разпитване на кораби и плавателни съдове от интерес;
- насочване на кораб към надводна цел за извършване на качване и проверка на документите, екипажа и товара на плавателния съд.

Поиск се нарича обзор на морското пространство в зоната за действие на радиолокационната станция с цел установяване на факта за наличието на плавателен съд или неговото отсъствие в тази зона. Откриване на цел означава, че радиолокационната станция е установила енергетичен контакт с плавателен съд намиращ се в зоната за действие на радиолокационната станция. За извършване на тези действия се използват наличните радиолокационни станции на поста. Освен с помощта на радиолокационните станции на поста, кораба от интерес може да бъде открит и наблюдаван визуално от поста за брегово наблюдение. Визуалното наблюдение, в операциите по контрол на корабоплаването има за задача визуално откриване и следене на целите от интерес. Визуалното наблюдение може да се води и с оптични и електронно-оптични прибори за наблюдение, видеокамери, инфрачервени сензори и прибори за нощно виждане.



***Снимка 1**. Работно място на РЛС и изглед през оптучески прибор ПАБ-2А;*

След като целта бъде открита от средствата на БПРТН тя се докладва в съответния оперативен център, след което се взема решение дали целта представлява интерес. В случай, че целта представлява интерес могат да бъдат предприети следните действия:

- **следене** на целта – следенето на целта се извършва чрез наличните РЛС и/или чрез средствата за визуално наблюдение с цел установяване на извършването на нерегламентирана дейност, нехарактерно движение на целта или отклоняване от обявения курс. За целта операторът на РЛС (вахтения наблюдател) води наблюдение на целта и докладва неините координати и елементи на движение в заповядания от оперативния център срок;
- **разпитване** на плавателен съд – при установяване на нехарактерно движение на плавателния съд или по заповед на ръководителя на операцията по контрол на корабоплаването дежурните от БПРТН могат да извършат разпитване на плавателния съд, което се извършва по два способа:

а) Проверка на информацията заложена в AIS – проверката на информацията заложена в информационната система на кораба, която се излъчва може да бъде проверена от оператора по всяко време по заповед от КП или при забелязване на нехарактрно движение на целта или други нехарактерни дейности. Като информация в AIS е заложена името на кораба, името на корабособственика, уникалния номер(IMO) на плавателния съд, пристанище на домуване, пристанища за товарене и пристанища за разтоварване, характер и тегло на товара, както и данни за курса и скоростта на кораба дата на пристигане в крайната точка и друга информация необходима за идентифициране на кораба и товара.

б) Установят на радиовръзка с плавателният съд от интерес – извършва се с цел установяване на причините за несъответствието между действията на плавателния съд и посочената за него информация. Първоначално връзка се установява на международния канал за търсене и спасяване при спазване на правилата за радиообмен и утвърдените процедури за установяване на връзка с невоенни кораби. След като се установи първоначална връзка с кораба от интерес се, запитва за неговото пристанище на отплаване и пристанището на пристигане, състав и съдържание на товара, състав на екипажа и други въпроси, касаещи дейностите на кораба и екипажа.

- **насочване** на военен (граничен)кораб към кораба от интерес – след като корабът от интерес бъде открит, проследен и бъдат определени неговите елементи на движение, при несъответствие на данните от AIS системата с данните от разпитването или движението на целта не съответства на обявения маршрут към пристанището за разтоварване е възможно да се извърши качване на борда на кораба и извършване на проверка на екипажа, документите и товара на плавателния съд. За това действия се изпраща кораб, който да установи контакт с кораба нарушител и да достави групата за проверка на кораба. При изпълнение на тази задача формированията за наблюдение и свръзка могат да изпълняват задача по насочване на военният (граничният) кораб към кораба цел на проверката. Това става след искане от страна на проверяващия кораб до командния пункт. След вземане на решение за извършване на подобна дейност командния пункт поставя задача за БПРТН(ПРЛС) за насочване на проверяващия кораб към кораба от интерес като указва честотите и канала (УКВ, КВ) за установяване на връзка. След установяване на връзка между кораба и съответнат пост за радиотехническо наблюдение последнят насочва военният(граничният) кораб по някой от следните способи:

а) директно насочване на военният(граничния) кораб към плавателният съд цел – при този способ от БПРТН(ПРЛС) определят и предават като данни за насочване пеленга и дистанцията от проверяващия кораб към кораба цел.

б) насочване от целеулазателна точка (ЦУТ) – при този способ като ориентир за насочване се определя брегови обект или друг неподвижен ориентир в зоната на радиолокационна видимост на РЛС и на БПРТН(ПРЛС) и на кораба изпратен за извършване на тактическите действия по проверка на подозрителния плавателен съд. В този случай екипажа на БПРТН(ПРЛС) подава данни за насочване като пеленг и дистанция спрямо този ориентир, който се приема за целеуказателна точка и от който се дават всички данни за местоположението на кораба за проверка и кораба от интерес.

Като извод може да се направи, че формированията за наблюдение и свръзка успешно изпълняват задачи в операции по контрол на корабоплаването в националните морски пространства на Република България като за целта изпълняват задачи по поиск, откриване и следене на надводни цели както и установяване на радиовръзка с невоенни кораби и осигуряване действията на военни (гранични) кораби за подхождане и извършване на проверка на съмнителни плавателни съдове и плавателни съдове от интерес.

References*:*

1. АНГЕЛОВ, Д. и колектив. (1995) *Радиоелектронно разузнаване*. София: Издателство на МО „Св. Георги Победоносец".
2. БОРИСЛАВОВ, Г. и колектив.(1978) *Радиолокационна техника.* София: ДИ „Техника".
3. ДИМИТРОВ, Г. (*1971*) *Основи на радиолокацията. София: ДВИ.*
4. ИЛИЕВ, И. (2019)*Техническо описание и експлоатация на „Брегова радиолокационна система за контрол на корабоплаването и охрана на морската граница – ЕКРАН"*. Варна: ВВМУ „Н. Й. Вапцаров", ISBN:978-954-899-186-5.

5. ЙОРДАНОВ, Н. (2003) *Проблеми на военноморското изкуство*. София: Военно издателство.
6. КОСТАДИНОВ, К. (2018) *Теоретични основи на оперативното използване на ВМС*, София: ВА «Г.С.Раковски», ISBN: 978-619-7478-12-9
7. МЕДНИКАРОВ, Б.(2008) *Защита на морския суверенитет*. Варна: ВВМУ „Н. Й. Вапцаров".
8. *МО: (*1993*)Тактика на ВМС.* Кн. III. София: ВИК „Св. Георги Победоносец".
9. *МО: (2013) Доктрина за морските операции НП-3.1.Варна:*
10. НИКОЛОВ, Н. (2004) *Моделиране преодоляването на ПВО от ударната авиация* – учебно пособие. София: ВА Г.С.Раковски, Катедра ВВС.
11. НИКОЛОВ, Н. (2004) *Тактика на авиационните удари по земни и морски обекти* – учебно пособие. София: ВА Г.С.Раковски, Катедра ВВС.
12. СТОЯНОВ, Н. (2017) *Автоматизирани информационни системи за боен мениджмънт*. Варна: Тера Балканика, ISBN 978-619-901-400-4.
13. СТОЯНОВ, Н. (2019) *Моделиране и симулация на бойните действия на Военноморските сили – минало, настояще и бъдеще*. Варна: Тера Балканика, ISBN 978-619-908-444-1.
14. СТОЯНОВ, Н. (2017) *Рискове и заплахи за сигурността на водната транспортно-преносна система*. Варна: Тера Балканика, ISBN 978-619-908-440-3.
15. СТАНЧЕВ, И. (2007) *Контратерористични рейдове*, София: ВИ, ISBN: 978-954-509-371-5.
16. СТАНЧЕВ, М. (2010) *Организация и тактика на защитата на обекти от МВР*, София, Акад. на МВР, ISBN:978-954-348-046-3
17. HUGHES, Wayne P., Jr. *Fleet Tactics and Coastal Combat (Second Edition).* Annapolis, MD: Naval Institute Press, 2000.
18. McMASTER*, Richard, BABER, Chris. Multi-agency operations: Cooperation during flooding. *Applied Ergonomics*, 2012.
19. NATO (2005): ATP-7.1. *ALLIED MARITIME INTERDICTION OPERATIONS*
20. O'KEEFE, Sean, KELSO, Frank B. II, MUNDY, C. E. Jr. From The Sea: Preparing the Naval Service for the 21st Century. *Navy and Marine Corps White Paper*, Sep 1992.

DEFENSE PLANNING MODEL

Ivo G. Radulov

Rakovski National Defence College, Defence Advanced Research Institute, 1504 Sofia, Bulgaria, 82 Evlogi i Hristo Georgievi Blvd, i.radulov@rndc.bg

***Abstract**: In this publication, the author focuses on the development of the Defense capability-based planning model.*

***Keywords**: Defense capability-based planning model, Strategic Defense Review; capability-based planning.*

МОДЕЛ ЗА ПЛАНИРАНЕ НА ОТБРАНАТА

Иво Г. Радулов

Военна академия „Г. С. Раковски", Институт перспективни изследвания за отбраната, научна секция „Стратегически изследвания на сигурността и отбраната", гр. София, i.radulov@rndc.bg

***Анотация:** Реализацията на планираното ниво на ефективност на решенията в сферата на отбраната, а от там и изграждането на необходимите отбранителни способности, в значителна степен зависи и се определя от качественото планиране на отбраната и изпълнението на трансформацията на въоръжените сили. Тази особеност е от изключителна актуалност в условията на неопределеност на бъдещата среда за сигурност. Запазването и развитието на отбранителните способности в отговор на заплахите и ангажиментите към националната и световна сигурност, в условия на силни ограничения на разполагаемите ресурси налага търсене на адекватни методи за повишаване на ефективността на процеса за планиране на отбраната.*

В настоящата публикация авторът акцентира върху развитието на модела за планиране на отбраната, базирано на способности.

***Ключови думи:** Планиране, базирано на способности.*

Увод

Всички държави в НАТО имат утвърдени процеси, процедури и методи за планиране на отбраната. С помощта на тези средства участниците в този процес определят необходимите способности на въоръжените си сили така, че същите да могат да изпълняват (към момента и/или в дългосрочен план) определените стандарти. Доказано от практиката, е че когато става въпрос за реално придобиване и развитие на отбранителни способности, необходимите средства за това винаги са недостатъчни. Резултатът е дефицит от способности. Тези дефицити имат различни форми и измерения, най-често са под формата на недостиг на въоръжение и техника, бойна подготовка, логистично осигуряване и комуникации, несъвместими и/или уязвими комуникационни и ин-

формационни технологии, системи за командване и управление и т. н. Не са изключение и други негативни примери за дефицити, в следствие от разходването на бюджета за закупуване на активи и услуги, които не допринасят за развитието на реално необходимите за въоръжените сили (ВС) способности. Резултатът от всичко това са небоеспособни формирования и структури, които не са в състояние да изпълняват мисиите и задачите си.

1. Модели за планиране на отбраната

Традиционно за планиране на отбраната и въоръжените сили в страните членки на алианса се използват следните няколко подхода, известни в литературата като:

- Целеви подход (или планиране „отгоре-надолу" (Top-Down);
- Планиране „отдолу-нагоре" (Bottom-Up);
- Планиране на основата на сценарии;
- Планиране на основата на заплахи;
- Планиране на основата на мисии;
- Хеджинг (Hedging) подход, основан на редуциране или пълно контролиране на риска;
- Технологичен подход;
- Финансов (или „бюджетен") подход.

Всеки от тези подходи притежава характерни особености, със съответните силни и слаби страни.

Процесът на планиране на отбраната, базирано на способности, е разновидност на част от изброените по-горе подходи. Той е основен инструмент за планиране, отразяващ динамиката на съвременната среда на сигурност. Целта на този процес е да защити и утвърди националните интереси чрез изграждане, поддържане и използване на адекватни на средата на сигурност отбранителни способности.

2. Анализ на съществуващия (As-Is) модел за планиране на отбраната в БА

Процесът на планиране на отбраната, базирано на способности, се използва в МО и БА още от 2012 г., когато за пръв път е разработено и методическо ръководство за прилагането на този подход. Реалностите на средата наложи извършване на преглед на съществуващото “Ръководство за планиране на отбраната, базирано на способности”, от 2012. За целта са извършени следните задачи:

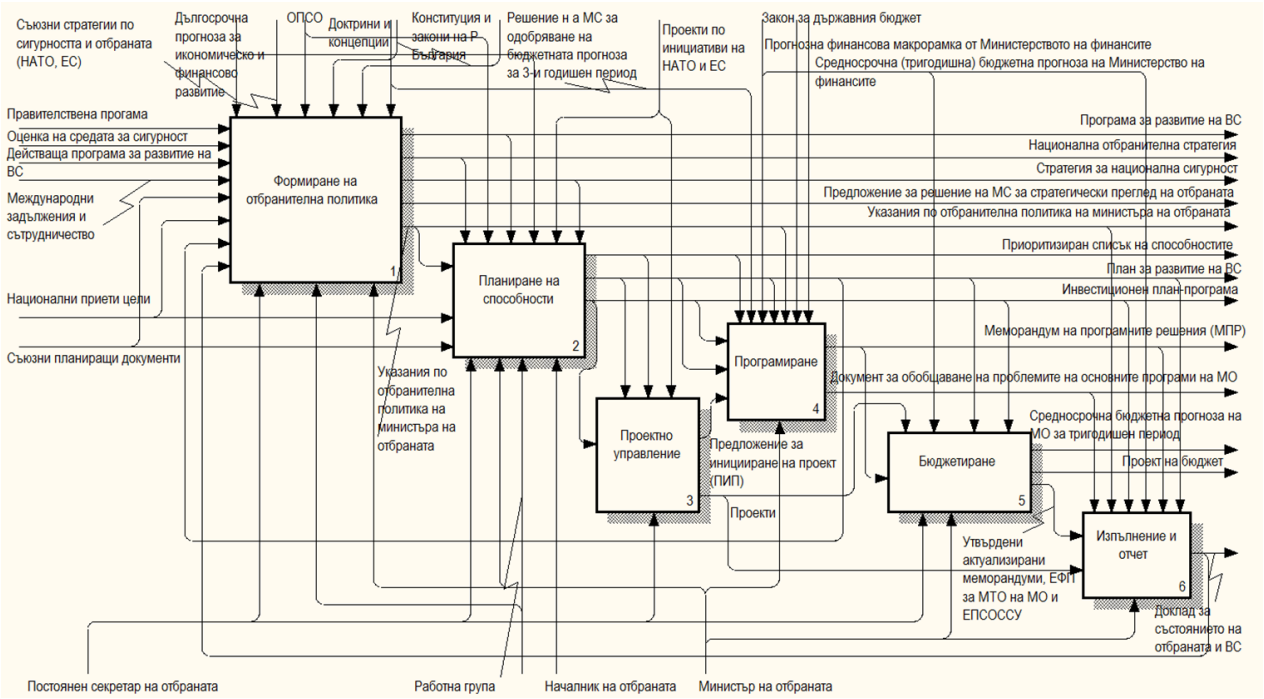
1. Подробно е изследван процесът за планиране, базирано на способности;
2. Избрани са стандартни средства за описания и обща работна среда, така че продуктите на модела да отразяват адекватно информационните потоци в организацията;
3. Извършен е реинженеринг на съществуващия модел на дейностите, така че новото състояние да: 1) съответства на нормативните и регламентиращи изисквания; 2) обхваща цялостния дизайн и динамика на системата и средата на функциониране; 3) съответства на стратегическите планове на организацията и 4) позволява непрекъсната промяна и трансформации.

В резултат на направения анализ на Ръководството за планиране от 2012 г., са констатирани редица неточности, в това число: липсата на регламентирани връзки между изпълнителите; липсата на отговорности на длъжностните лица; „паразитни“ дейности, които не дават „принадена стойност“ на процеса за планиране на отбраната. Не е описан етапа „Планиране“ на процеса, както и етапа „Управление на жизнения цикъл на отбранителните продукти“, не са визуализирани коректно дейностите на процеса, не са указани отговорностите на лицата, вземащи участие в процеса.

Основните изводи от анализа са, че моделът на дейностите от процеса за планиране е противоречив, непълен и не съответства на действащата в момента система за управление на отбраната. Тоест в този си вид той не може да се използва като методиката за провеждане на предстоящ преглед на отбраната.

За отстраняването на констатираните слабости моделът е преработен в усъвършенстван To-Be модел така, че същият да интегрира и отразява всички основни функционални и системни гледни точки на отбранителния мениджмънт [4].

Актуализираният To-Be модел е изобразен на фигура 15. Същият е изследван за непълнота и непротиворечивост с помощта на програмното средство ALL Fusion Process Modeler, Ver. 6.



Фигура 1. **To-Be модел за планиране на отбраната, базирано на способности**

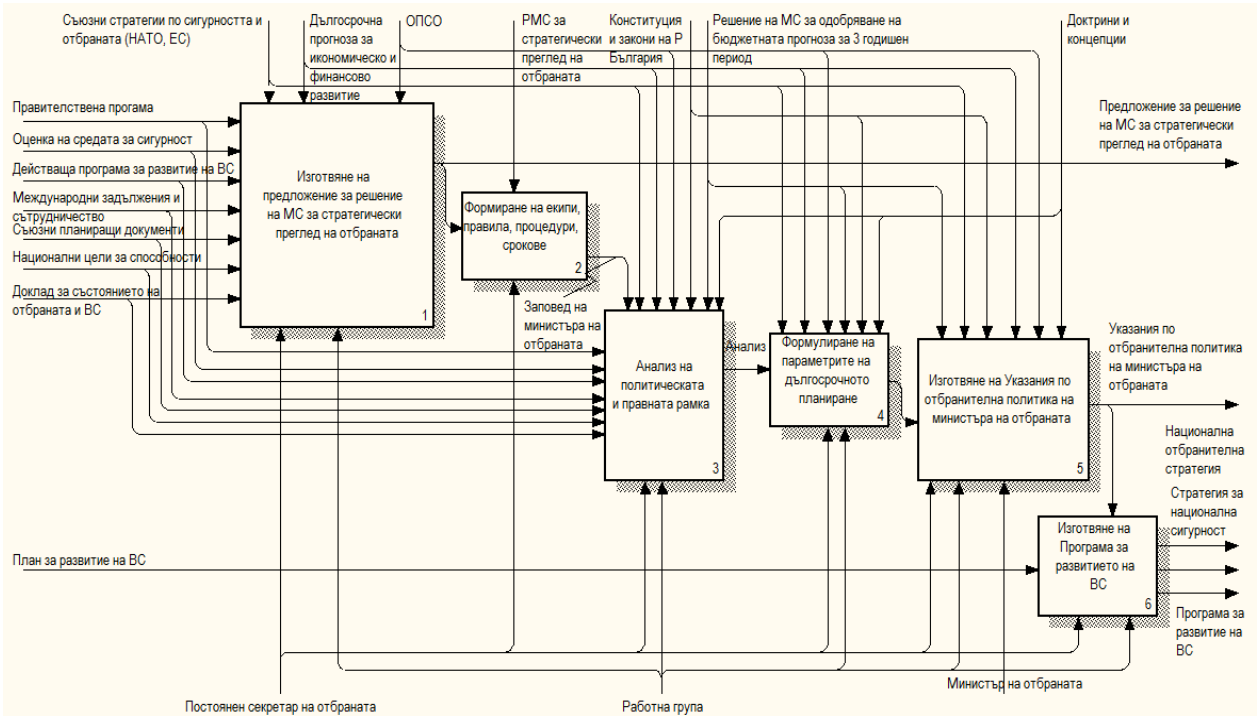
2.1. Формиране на отбранителна политика

Отбранителната политика е отправна точка за иницииране и провеждане на процеса по планиране на отбраната. Отбранителната политика е секторна политика на политиката за национална сигурност и представлява съвкупност от съгласувани цели и институционални и граждански действия за развитие, усъвършенстване, поддържане и използване на отбранителните способности за защита на националните интереси.

Основна задача на отбранителната политика е създаването на условия за оптимално използване на ВС, в контекста на политиката за национална сигурност, при отчитане на стратегическата среда на сигурност, ресурсните възможности на страната в средносрочен план и тяхното прогнозно развитие в по-дългосрочен план и участието на ВС в колективната отбрана на НАТО и Общата политика за сигурност и отбрана на ЕС [1]. Дейностите от този етап са изобразени на Фигура 2.

Основни изходни продукти от този етап са: 1) *Предложение за решение на МС за Стратегически преглед на отбраната;* 2) *Указания по отбранителна политика на министъра на отбраната*; 3) *Програма за развитие на Въоръжените сили*.

[5] Фигурите са изобразени с помощта на CASE (Computer-aided software engineering) средства по стандарта IDEF0 за представяне на модели на дейностите.



Фигура 2. **То-Ве модел за планиране на отбраната, базирано на способности - Етап „Формиране на отбранителна политика"**

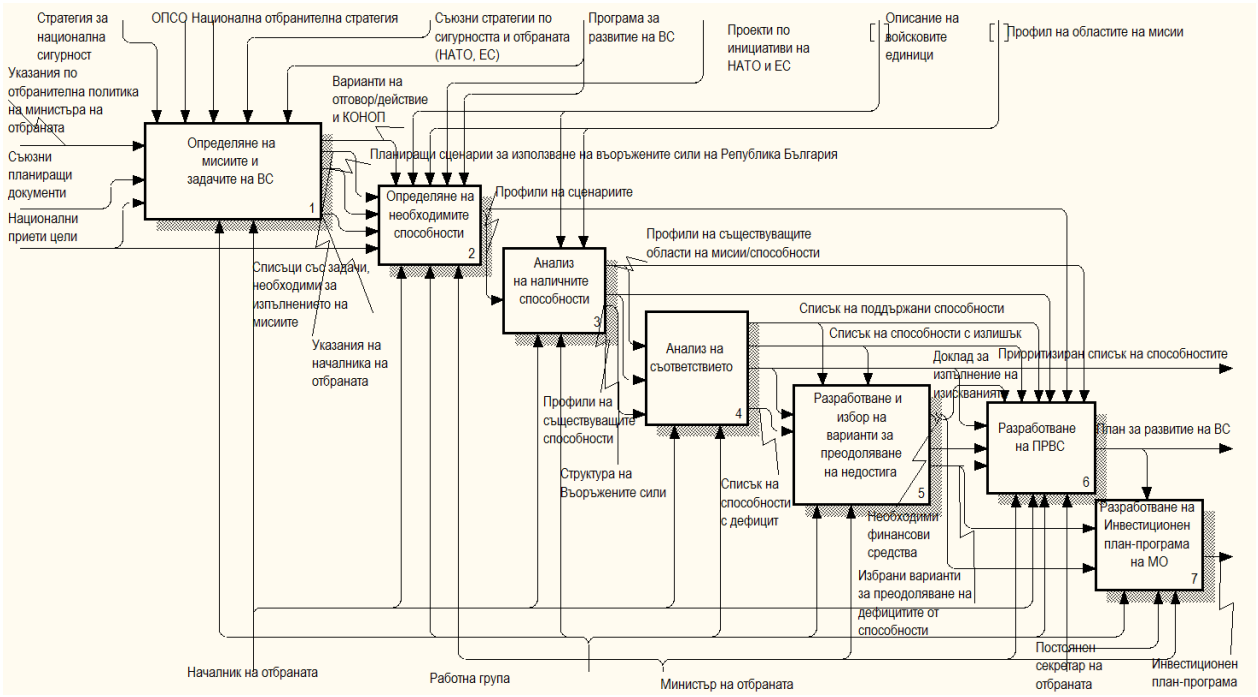
2.2. Планиране на способности

В етапа „Планиране на способности" промените в средата на сигурност и взетите политически решения се „преобразуват" в необходими способности за постигане на целите на отбраната [2]. Етапът включва следните дейности (Фигура 3):

- определяне на мисиите и задачите на въоръжените сили;
- определяне на необходимите способности;
- анализ на наличните способности;
- анализ на съответствието;
- разработване и избор на варианти за преодоляване на недостига от способности;
- разработване на План за развитие на въоръжените сили (ПРВС);
- разработване на Инвестиционен план-програма (ИПП) на МО.

Същността на този етап е определяне на отбранителните способности, които ще са необходими за следващите 10-15 години, и съставяне на план за тяхната поддръжка, развитие и изграждане.

Изходни продукти от етапа са: 1) План за развитие на ВС; 2) Инвестиционен план-програма на МО; 3) Приоритизиран списък на способностите.



Фигура 3. **То-Ве модел за планиране на отбраната, базирано на способности - Етап А.2. “Планиране на способности”**

2.3. „Проектно управление“

Дейностите по управлението и реализацията на проекта съгласно Методологията PRINCE2 са организирани в седем процеса, описани подробно в Ръководството за проектно управление в МО и структурите на пряко подчинение на министъра на отбраната и Българската армия (СППМО и БА).

В процеса „Подготовка за иницииране на проект“ се осигурява, обобщава и оформя първична информация с оглед вземане на решения за бъдещето на проектите. Процесът се осъществява във фаза „Предпроектна“, под ръководството на ръководителя на програма/организационна структура. Крайният резултат от процеса е Предложение за иницииране на проект (ПИП), което се внася за разглеждане в Борда за управление на портфолиото от проекти (П2Б). Предложението за иницииране на проект съдържа кратко изложение на проекта и служи за запознаване на П2Б с идеята за реализация на проекта [3]. Освен него се изготвят План за фаза „Иницииране“ и предложение за състав на Борд за управление на проекта (БУП) и ръководител на проекта (РП). При необходимост се разработва Работен план.

Процесът „Иницииране на проект” има за цел да създаде стабилна основа за ефективното изпълнение и контрол на проекта, чрез детайлно планиране на ресурси, време и етапи за реализация на проекта. Този процес протича във фаза „Иницииране на проект“ и основна отговорност за неговата реализация имат БУП и РП [3]. Крайният резултат на процеса е разработване на Документ за иницииране на проект (ДИП) и приложенията към него, които следва да съдържат пълната информация от организационен, финансов, технически и друг характер, необходима за реализацията на проекта. Освен ДИП се изготвя и План за етап (I-ви етап на проекта).

Процесът „Ръководство на проект“ описва отговорностите и дейностите на БУП за вземането на ключови решения и контрол на изпълнението на проекта от края на фаза „Предпроектна“ до приключването на проекта [3].

Процесът „Контролиране на етап на проект" описва дейностите на РП в ежедневната му работа по управление на проекта в рамките на всеки етап [3]. Изходни продукти от процеса са: 1) Отчети пред БУП; 2) Регистри риск, качество и проблемни въпроси и 3) Доклад за отклонение.

Процесът „Управление границите на етап" осигурява прозрачност като РП предоставя цялостна и систематизирана информация на БУП за развитието на проекта в текущия етап, актуалност на детайлната обосновка на проекта и риска По този начин БУП може да следи за напредъка на проекта и да одобри план за следващия етап от реализацията на проекта [3]. Изходни продукти от процеса са: 1) Доклад за приключване на етап; 2) Регистри риск, качество и проблемни въпроси и 3) Актуализиран план на проекта.

Процесът „Управление на доставката на продукт" осъществява комуникация и контрол на връзката между РП и ръководителя на работния екип, а в случаите когато не е назначен такъв на РП с членовете на работния екип [3]. Резултатите от процеса са продуктите на проекта и документите, свързани с управлението на качеството.

Процесът „Приключване на проект" включва комплекс от дейности, с които се потвърждава постигането на ползите от проекта, така както са заложени в ДИП. Процесът има за цел да удостовери, че потребителят е приел крайният/те продукт/и на проекта [3]. Изход на процеса е изготвен Доклад за приключване на проекта.

Провеждането на Стратегическите прегледи на отбраната основно се свързват с дейностите от етапите „Формиране на отбранителната политика" и „Планиране на способности".

2.4. Етап „Програмиране"

Етапът включва следните дейности (Фигура 4) [1]:

- планиране на ресурсите и разработване на Указания за програмиране на министъра на отбраната за шестгодишен период;
- разработване на Програмна структура на основните програми в МО;
- разработване на програмни меморандуми за шестгодишен период;
- провеждане на програмен преглед и вземане на решение относно разработените алтернативи на програмите;
- разработване на Меморандум на програмните решения (МПР) за шестгодишен период.

Същността на етапа е програмиране на отбранителните ресурси за изпълнение на Плана за развитие на ВС съгласно определените цели и приоритети и в съответствие с приетите национални закони, подзаконови актове, указания на МФ, планиращи документи за програмиране, бюджетиране, изразходване и отчитане на ресурсите.

Етапът се повтаря ежегодно, като се планират и програмират ресурсите за шест години.

Междинни документи от етапа са:

- *Указания за програмиране*. Указанията представляват основен планиращ документ, в който се конкретизират целите и приоритетите на отбраната по основни политики. Те съдържат основните направления за прилагане на отбранителната политика, като се търси баланс между задачите на ВС, числеността и разполагаемите ресурси, и дават практически насоки за изпълнение на ПРВС и ИПП чрез изпълнение на отбранителните програми. Указанията за програмиране са основа за подготовката на всички документи, свързани с изготвянето на Средносрочната (тригодишна) бюджетна прогноза на МО по политики, програми и по параграфи от Единната бюджетна класификация.

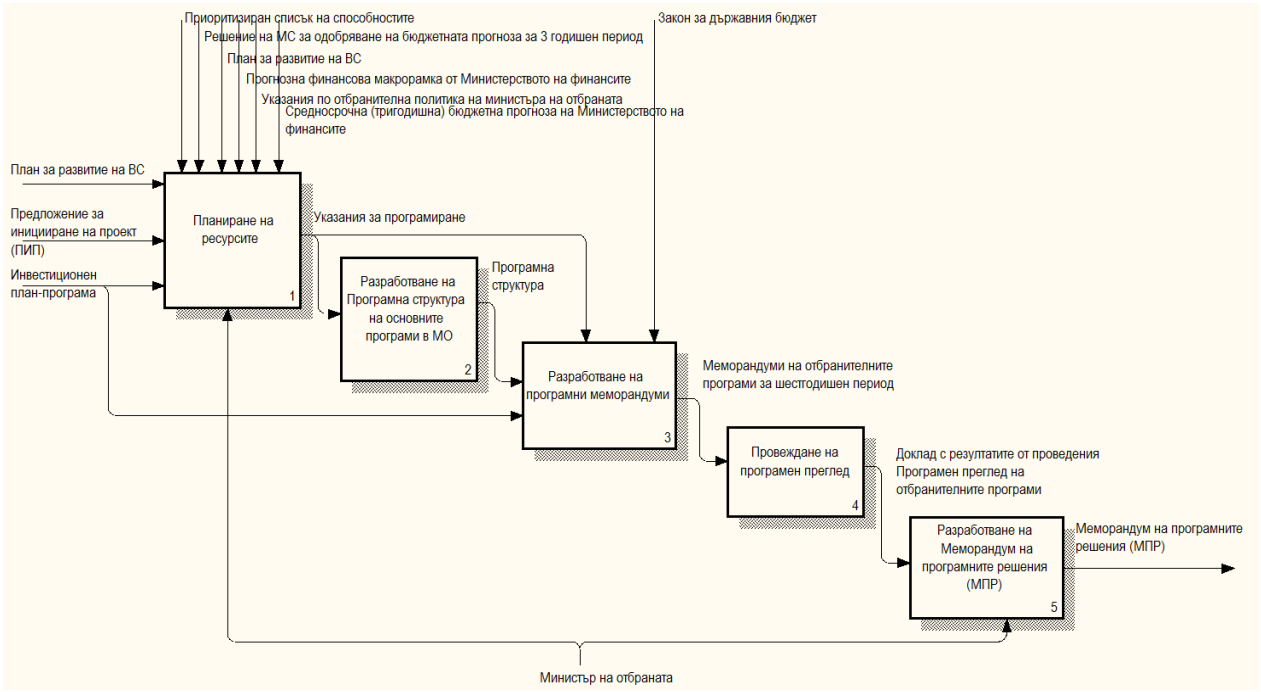
- ***Програмна структура.*** Програмната структура синхронизира планирането на ресурсите с развитието на необходимите способности за изпълнение на всяка мисия от утвърдените области на мисии. Всяка от основните програми (ОП) има структура от програми, подпрогра-

ми и програмни елементи, отразяваща целите и приоритетите на МО, структурите на пряко подчинение на министъра на отбраната и БА. При разработването на Програмната структура се използват утвърдените области на мисии от етап „Планиране на способности".

- ***Програмни меморандуми за шестгодишен период*.** Програмните меморандуми описват начина на разпределение на ресурсите за отбрана за всяка основна програма и програма за средносрочен период при отчитане на изискванията за ефективност и икономичност. Те съдържат стратегическите и оперативните цели на програмата, приоритетите й, програмния екип, отговорниците за изпълнението, планираните крайни резултати, както и разчетен ресурсен план за шестгодишен период. Във връзка с прилагането на планиране, базирано на способности, планираните крайни резултати в основните програми се обвързват с поддръжката, развитието и изграждането на необходимите способности съгласно *ПРВС* и *ИПП*.

- ***Доклад с резултатите от проведен Програмен преглед на отбранителните програми*.** Програмния преглед има за цел оценка на степента на съответствие на разработените програмни меморандуми по отношение на: 1) целите, приоритетите и ресурсните ограничения, регламентирани в *Указанията за програмиране на министъра на отбраната* за шестгодишен период; 2) сроковете и изискванията за изпълнение на цели за способности на НАТО; и 3) оценката на съответствие между разработените програмни меморандуми и постигането на приоритетните отбранителни способности на ВС.

Краен продукт от етапа е *Меморандумът на програмните решения (МПР)*. *Меморандумът на програмните решения* съдържа утвърдените от министъра на отбраната за изпълнение основни програми през следващия бюджетен и последващия средносрочен (шестгодишен) период, както и програмните цели, приоритети, крайни резултати и финансовите средства за тяхната реализация. *Меморандумът на програмните решения* се разработва в съответствие с приетите в процеса на програмен преглед програмни меморандуми на основните програми и програми и с взетите решения относно разпределението на ресурсите за отбрана. *Единният финансов план за материално-техническо осигуряване на МО* и *Единният поименен списък на обектите за строителство и строителни услуги на МО и БА* се изготвят и отчитат по програми съгласно приложенията на *Меморандума на програмните решения*. При необходимост *Меморандумът на програмните решения* се актуализира след утвърждаване на бюджета на МО след приемане на *Закона за държавния бюджет* за съответната бюджетна година и постановлението на МС за неговото изпълнение. *МПР* се актуализира в частта му за първата година от периода на програмиране (бюджетната година).



Фигура 1. **То-Ве модел за планиране на отбраната, базирано на способности - Основни дейности в етап „Програмиране”**

2.5. Етап „Бюджетиране“

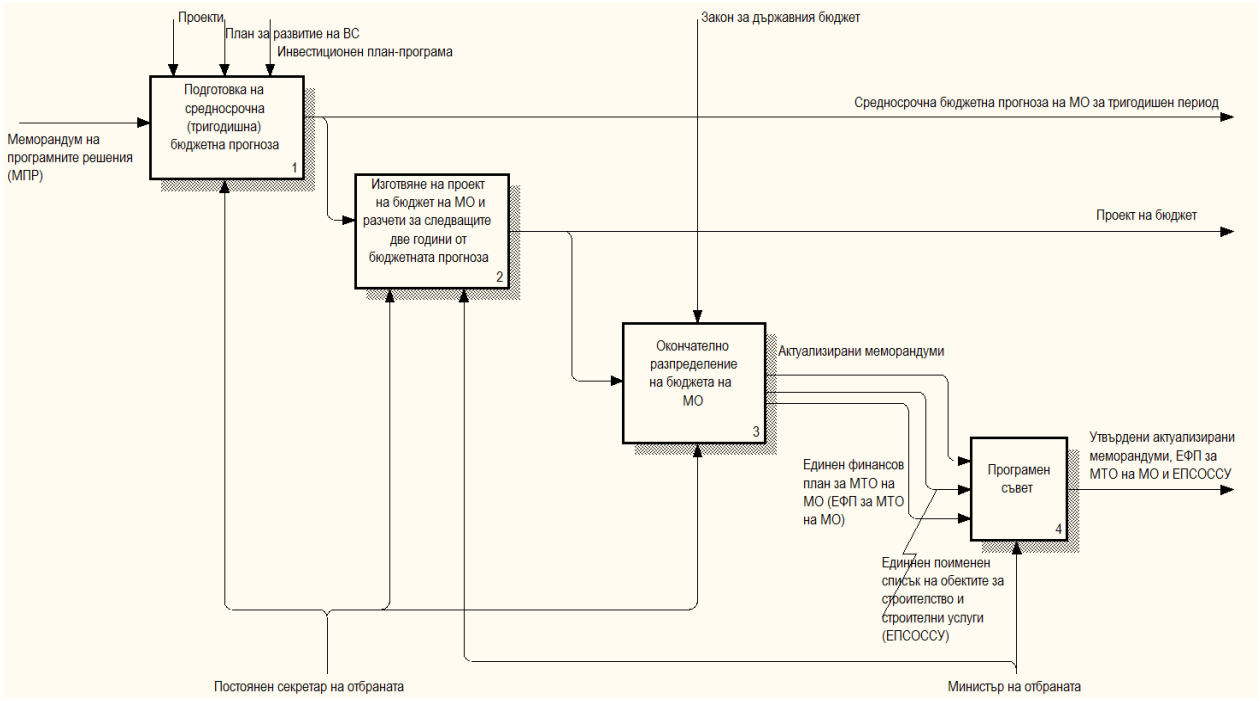
Същността на етапа е бюджетиране на отбранителните ресурси за изпълнение на *Плана за развитие на въоръжените сили* съгласно определените цели и приоритети и в съответствие с приетите национални закони, подзаконови актове, указания на МФ и планиращи документи за програмиране, бюджетиране, изразходване и отчитане на ресурсите [1].

Етапът се повтаря ежегодно, като се бюджетират ресурсите за една година с прогнози за последващите пет.

На този етап се цели такова разпределение на бюджета в проектите и окончателните бюджети на второстепенните разпоредители с бюджет, проектите на *Единния финансов план за МТО* и *Единния поименен списък на обектите за строителство и строителни услуги*, което да съответства на планирането от предходния етап (осигуряване на планираните дейности по изграждането и поддръжката на необходимите способности, с приоритет на изпълнението на целите за способности, определените приоритетни способности и приоритетните инвестиционни проекти) [1].

Етапът включва следните дейности (*Фигура 5*):

- подготовка на средносрочна (тригодишна) бюджетна прогноза;
- изготвяне на проект на бюджет на МО в програмен формат за съответната бюджетна година и разчети за следващите две години от бюджетната прогноза;
- окончателно разпределение на бюджета на МО по политики, основни програми и второстепенни разпоредители с бюджет (ВРБ);
- утвърждаване на *Единния финансов план за МТО* и *Единния поименен списък на обектите за строителство и строителни услуги*.



Фигура 2. **То-Ве модел за планиране на отбраната, базирано на способности - Основни дейности в етап „Бюджетиране“**

Крайни продукти от етапа са:

- Средносрочна (тригодишна) бюджетна прогноза. В сроковете, определени в решението на МС за бюджетната процедура, се разработва и представя в Министерството на финансите *средносрочна бюджетна прогноза за съответния тригодишен период* в съответствие с изискванията на МФ по предоставените унифицирани форми на документите. След извършване на оценка на тригодишните бюджетни прогнози от страна на Министерството на финансите и уведомяване на първостепенните разпоредители с бюджет за направените оценки се провеждат консултации за уточняване на конкретните стойности на финансовите средства за политиките и програмите. На основата на постигнатата договореност с Министерството на финансите се извършва актуализация на разходите по политики и програми по тригодишната бюджетна прогноза [1].

- Проект на бюджет на МО за съответната година и разчетите за следващите две години се изготвят в изпълнение на Указанията на МФ за бюджетната процедура и са структурирани по политики и основни програми. *Проектът на бюджет на МО* се разработва на база на одобрените от Министерския съвет средносрочна фискална рамка, основни допускания, макропоказатели, инструменти на политиките, разходни тавани и очаквани резултати по секторни политики и отбранителни програми за съответния тригодишен период. В срока, определен в решението на Министерския съвет, МО представя в Министерството на финансите проектобюджет за съответната година по политики и програми, както и разчети за разходи за следващите две години от бюджетната прогноза по секторни политики и отбранителни програми [1].

След приемането от Народното събрание на *Закона за държавния бюджет* за съответната година, както и на ПМС за неговото изпълнение, в едномесечен срок от публикуване на постановлението МО изготвя разпределение на бюджета по политики, програми, пълна единна бюджетна класификация, функции и дейности. Изготвят се годишни бюджети на основните програми и програми и второстепенните разпоредители с бюджет, в т.ч. по функции и дейности [1].

Изготвените документи за разпределението на бюджета на МО, доклада за резултатите от прегледа на актуализираните меморандуми на основните програми и програми за съответната

бюджетна година, *Единния финансов план за МТО на МО* и *Единния поименен списък на обектите за строителство и строителни услуги* се внасят за обсъждане в Програмния съвет и се утвърждават от министъра на отбраната [1].

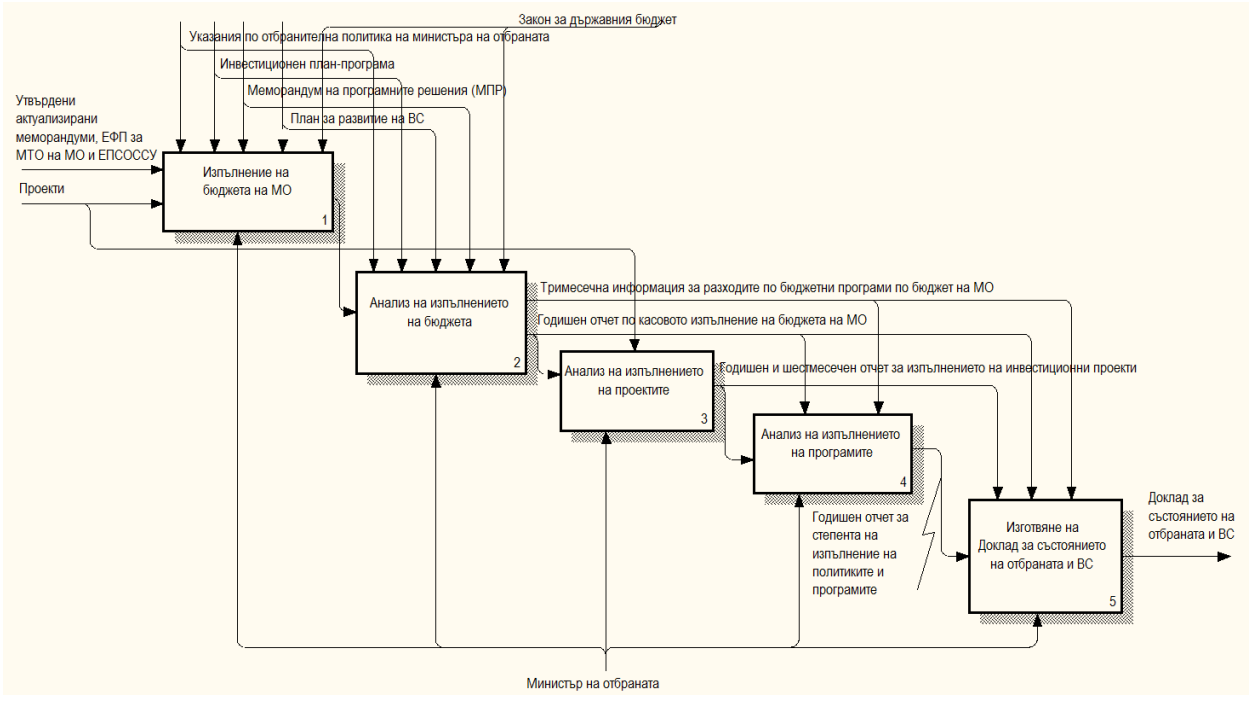
2.6. Етап „Изпълнение и отчет"

По време на етап „Изпълнение и отчет" се извършва изпълнение и отчитане на необходимите дейности за постигането на планираните цели и задачи (*Фигура 6*).

Етапът включва:

- изпълнение на дейности, свързани с планираните цели и задачи, в т.ч. изпълнение на бюджета в рамките на текущата година, управление на аквизационните процеси, жизнения цикъл на отбранителните продукти, включително управление на договорите, управление и изпълнение на проектите, научно-изследователска и развойна дейност, управление на риска, финансов контрол и одит, регламентирани с отделни указания или ръководства, утвърждавани/подписвани от ПСО или министъра на отбраната [1];

- отчет на резултатите от изпълнените дейности и реализирането на планираните цели и задачи, в т.ч. организация на процеса по разработване на отчета за постигнатите планирани цели, *Указания за отчет за степента на изпълнение на политиките и отбранителните програми*, *Отчет за степента на изпълнение на политиките и отбранителните програми на МО, структурите на пряко подчинение и БА*, включително изразходваните ресурси по програми, *Доклад за състоянието на отбраната и въоръжените сили* и др. [1].



Фигура 3. **То-Ве модел за планиране на отбраната, базирано на способности - Основни дейности в етап „Изпълнение и отчет"**

Изводи:

Описаният процес за планиране на отбраната, базирано на способности е представен подробно в *„Ръководство за планиране на отбраната, базирано на способности“* от 2019 г., като непрекъснат и цикличен, последователност от описаните по-горе етапи: „Формиране на отбранителната политика“; „Планиране на способности“; „Програмиране“; „Бюджетиране“; „Изпълнение и отчет“. В рамките на изпълнението се реализира и процесът „Проектно управление“.

Проведения през 2020 г. Стратегическият преглед на отбраната, на практика валидира като работещ инструмент с практическа насоченост, представения в настоящата статия, актуализиран модел за планиране на отбраната, базирано на способности. Всички дейности от прегледа са осъществени по описания модел, при който националните стратегически цели се превръщат във военни цели, възможни операции и задачи, а те от своя страна в сили и средства, необходими за изпълнението на тези задачи в операциите.

Представеният модел за планиране, базирано на способностите е инвариантен и конструктивен, което го прави приложими и при автоматизация на процесите.

References

1. „Концепция за дългосрочно планиране на отбраната“, утвърдена със заповед на министъра на отбраната № ОХ - 313/15.04.2021 г.

2. „Ръководство за планиране на отбраната, базирано на способности“, въведено за изпълнение в МО, СППМО и БА със заповед на министъра на отбраната № ОХ-323/29.03.2019 г.

3. “Ръководството за проектно управление в МО и структурите на пряко подчинение на министъра на отбраната и Българската армия”, обявена със заповед на министъра на отбраната № ОХ-947/09.12.2016 г.

4. З. Здравков, А. Атипова, Съвместен и алтернативен анализ - способности за научен напредък в съвременната среда за сигурност, Годишна научна конференция "110 години традиции, качество, престиж", Военна академия "Г. С. Раковски", 12-13 април 2022, ISBN 978-619-7478-88-4

COMPARATIVE ANALYSIS OF THE REMOTELY PILOTED AIRCRAFT SYSTEMS USED IN THE RUSSIA-UKRAINE WAR

Ivaylo Zh. Bozov

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

Abstract*: The last decades have shown the constantly changing nature of armed conflicts, and the introduction of new ways of conducting combat operations. This led to the widespread use of UAVs for reconnaissance and airstrikes. The war between Russia and Ukraine is no exception, and the diversity of different models UAV, used in this war is impressive. The aim of this report is to make a brief comparative analysis of the UAVs used by Russia and Ukraine.*

Key words: *Russia, Ukraine, UAVs, target acquisition.*

Introduction

Recent decades have shown the ever-changing nature of armed conflicts, which has presented armed forces with new challenges. In many of the developed countries, the introduction of new technologies, constant modernization of armaments and the related introduction of new methods of conducting combat operations are observed.

Military conflicts have brought to the fore the use of remotely piloted aircraft systems (RPAS) for reconnaissance, target asquisition or direct strike. The war between Russia and Ukraine is no exception, and according to some of the leading experts in this field (Samuel Bendet , David Hambling) , this war is characterized by a wide variety of unmanned aerial vehicles (UAV) used by both warring parties. Ranging from rotary-wing (copter -type), fixed-wing (combat, reconnaissance) and loitering munitions (kamikaze), the arsenal employed is truly impressive.

1. Fixed-wing RPAS

This type of UAV represents the largest percentage of aircraft in use. A large number of RPAS manufacturers are focusing on the production of such models, as they have many advantages, some of which are - greater flight distance, greater flight ceiling, the ability to quickly assemble and perform tasks (for the models of the mini and micro class) and many others, the disadvantage being the way of take-off and landing. The variety of models produced is really huge, as well as the tasks they perform.

This report will examine a large number of wartime UAV, mainly of Class I and Class II, as well as combat UAV (UCAV).

UCAV

UCAVs are not distinguished by great variety, but the models used showed that this is one of the weapons of the future. They were widely used by Ukraine, especially in the initial stage of the war, hitting mainly armored vehicles. The standout in these early months was the Turkish Bayraktar-TB2, but as the hostilities progressed, Russian forces were able to perfect their air defense system and began

shooting down these UCAVs. This led Ukraine to limit their use, due to their high cost, and focus on the use of the smaller UCAV Punisher - of its own production. On the other hand, Russia relies to a lesser extent on its strike aircraft, and the strikes carried out by them are rather episodic. Their typical representative of this class is the UCAV Orion, while the Forpost is primarily a reconnaissance drone, but Russia has adapted it to carry modified 60-pound Kornet anti-tank missiles or 50-pound KAB-20 laser-guided bombs.

Some characteristics of the mentioned models are shown in Table 1.

Model	Weight, kg	Wingspan, m	Flight time, h	Flight ceiling, m	Flight distance, km	Speed, km/h	Engine	Armament	Manufacturer
Used by Russia									
Orion	1000	16.3	24	7500	250	120-200	DVG	KAV-20, KAV-50	Russia
Forpost	350	8.55	20	6100	-	200	DVG	Cornet ; KAV -20	Russia
Used by Ukraine									
Bayraktar-TB2	650	12	24	8200	150	130	DVG	MAM-C, MAM-L	Turkey
Punisher		2.25	1.5	400	50	198	Electric	UB-75HE; MACE	Ukraine

Table 1 : UCAV used in the war.

Reconnaissance UAV

The variety of RPAS used in the war, mainly of the I "Mini" class, is impressive. The different tasks they perform and the ability to carry a payload are the reason for their diverse equipment with different cameras (day, night, thermal imaging, infrared, etc.) and sensors (for measuring weather conditions, radiation, chemical pollution, etc.). All this helps, in addition to reconnaissance of the battlefield and capturing targets, UAVs can also be used to adjust artillery fire. Some models are even equipped with pointers for laser guidance of ammunition. The characteristics of the main models used by both sides in the conflict are shown in Table 2.

While Ukraine relies more heavily on UCAVs, Russia has turned to using UAVs to acquire targets and adjust artillery fire. The most striking representative is the Russian Orlan-10, and it is not by chance that it is called "the workhorse of the fleet of unmanned aircraft of Russia". Unlike many unmanned aircraft that are controlled remotely by operators, the Orlan-10 can be controlled directly by Russian artillery formations as part of an automated fire control system. The Orlan-30, in turn, is equipped with an improved navigation system and a precision laser targeting system that allows artillery formations to hit targets with 152mm Krasnopol shells. Almost all Russian models listed in Table 2, in addition to reconnaissance tasks, can also perform tasks of adjusting artillery fire.

The A-1S Furia, UJ-22 and RQ-20 Puma used by Ukraine are also used to correct artillery fire, for example the A-1S Furia's communications are integrated with the Ukrainian automated fire control system of artillery. The Leleka-100 is the most common military small drone in the Ukrainian army, which is used to provide aerial reconnaissance of Russian targets. The German Vektor is a new generation UAV with vertical take-off and landing and the possibility of replacing the wings with rotary ones.

Model	Weight, kg	Wingspan, m	Flight time, h	Flight ceiling, m	Flight distance , km	Speed, km/h	Engine	Manufacturer
Used by Russia								
Zala -421-16E5	29.5	5	20	3600	150	65-110	DVG	Russia
Garnet -4	30	3.2	6	3500	70	140	Electric	Russia
Orlan -10	16	3.1	16	5000	120	245	DVG	Russia
Orlan -30	27	-	5	4500	300	170	DVG	Russia
Zastava	5.5	2.2	1.3	2200	10	120	Electric	Russia
Tachyon	25	2	2	4000	40	120	Electric	Russia
Used by Ukraine								
Leleka-100	5.5	2	2.5	1500	45	180	Electric	Ukraine
A-1S Furia		2	3	2500		120	Electric	Ukraine
UJ-22	-	-	7	6000	100	160	DVG	Ukraine
Quantix	2.27	1	0.75	-	20	72	Electric	USA
RQ-20 Puma	6.3	2.8	2	3200	20	75	Electric	USA
Spectator	2.5	3	2	3000	50	120	Electric	Ukraine
Vector	7.4	2.8	2	-	25	90	Electric	Germany
WB FlyEye	11	3.6	2.5	3500	-	120	Electric	Poland

Table 2: Fixed-wing reconnaissance drones in use in the war .

The following conclusions can be drawn from the analysis and table 2;

- As with UCAV, Russia relies entirely on systems of its own production, and not a small part of them are with internal combustion engines (ICE). The Zastava and Forpost UAVs are models where Russia licensed the design and modified it;
- Russia relies exclusively on reconnaissance UAVs as a means of adjusting artillery fire;
- Ukraine uses both its own systems and systems of foreign manufacturers, all of which except the UJ-22 have electric motors;
- While the Russian intelligence DUL are heavier and have a larger perimeter of action, those of Ukraine are lighter and operate at shorter distances. This can be explained by the tactical tasks that the advancing and defending troops perform.

Multy-rotor RPAS

Rotary-wing UAVs (quadro, hexa, octo), also called VTOL (vertical take-off and landing), allow these aircraft to take off and land vertically and circle to provide constant target observation. Other advantages are small size and low noise levels. These UAVs tend to move slower than fixed-wing ones and have a shorter flight time, so formations use them for closer-range missions. The characteristics of some of them are shown in Table 3.

Model	Weight, kg	Wingspan, m	Flight time, min	Payload, kg	Flight distance , km	Flight ceiling, m	Speed, km/h	Armament	Manufacturer
Used by Russia									
KBLA-IVT	300	4.57	60	-	-	-	-	-	Russia
Used by Ukraine									
R18	-	1.82	40	5	4	300	-	RKG-1600	Ukraine
Autel Evo II	-	0.4	-	-	-	-	72	Vog-17	China
Mavic Mini	0.250	0.2	30	-	4	-	45	-	China
TEAC Golden eagle	-	0.5	30	-	3	-	80	-	USA
Skydio X2	-	0.6	35	-	6	-	40	-	USA

Table 3: Reconnaissance DULS with fixed wings used _ in the war .

As can be seen from Table 3, Russia does not rely on this type of UAV, mainly due to the short range and small mass of the payload. On the other hand, Ukraine again relies on everything that would help in the course of hostilities, not only aircraft produced for military purposes, but also amateur ones. Here again, the desire of the Ukrainian forces to hit targets from the air, mostly armored ones, is noticeable. An impressive R18 octocopter capable of carrying several kilograms of payload - up to 5 kg of free-falling ammunition. As such, RKG-3 or RKG-1600 cumulative anti-tank grenades are used.

Russian forces use the KBLA-IVT primarily as a mobile target for reconnaissance and detection of Ukraine's air defense system.

Loitering munition - "kamikaze" .

This type of UAV carries an explosive warhead on one-way attack missions. Unlike conventional weapons, the operator does not need to identify the target before firing. Once the drone is in the air, a pilot on the ground search enemy targets using on-board cameras. When the operator locks on the target, the loitering munition slams into it, detonating its warhead. The characteristics of some of those used in the war are shown in Table 3.

Model	Weight, kg	Wingspan, m	Flight distance , km	Flight time, min	Speed, km/h	Manufacturer
Used by Russia						
Zala KYB	3	1.21	-	30	130	Russia
Used by Ukraine						
Switchblade 300	2.5	1.20	10	15	160	USA
Switchblade 600	22.7	1.80	40	40	185	USA
Phoenix Ghost	-	-	-	360	-	USA
Warmate	5.7	1.6	30	50	150	Poland

Table 3: Barrage ammunition used _ in the war .

From the review of the sources providing information on the kamikaze-type UAV used and summarized in Table 3, it can be seen that Ukraine also has an advantage here. The arsenal at its disposal is entirely foreign-made, as the Switchblade 600 and Warmate are capable of delivering accurate hits to the long-range artillery of the Russian forces, and the Warmate has the ability to return when it does not detect a target and be used for follow-up strikes.

Russian forces rely on the Zala KYB as a means of engaging armored and lightly armored enemy vehicles, although they also possess the Zala Lancet , and for the latter there is no information that they have been used so far.

Conclusion

1. Both warring countries have a large arsenal of anti-aircraft missiles, with Russia relying entirely on systems of its own production, while Ukraine also uses systems developed by other countries. This fact and the various tasks performed by UAVs lead to an increase in the combat capabilities of the Ukrainian forces. The disadvantage is that operator training is required for each RPAS and there is a shortage of spare parts.

2. While Ukraine relies on all kinds of UAVs to strike armor-wounds, lightly armored targets and various installations, Russia has mainly focused on using Class I "Mini" anti-aircraft missiles to perform reconnaissance and target acquisition tasks and adjusting artillery fire. These systems are a difficult target for the means of air defense, due to their small size, and their price is lower. In this way, a lower cost of incurred losses in reconnaissance assets is achieved.

3. UCAVs are a powerful weapon, without danger to human life. The experience of military operations since the beginning of the war shows that they are highly effective in meeting an unprepared or weak air defense system. When a sustained and advanced air defense system is in place, UCAVs lose

much of their effectiveness because they are an easy target and their cost is much higher. In such cases, flying munitions - "kamikaze" are the most reliable means of hitting enemy targets.

References

1. Katsev I., (2019). Analysis of the opportunities for employment unmanned aerial vehicles class mini in artillery formations. International Scientific Conference — Defense Technologies DefTech 2019, Shumen, Bulgaria, pp 116-123, ISSN 2367-7902.
2. David Hambling. (23.06.2022). Every Single Drone Fighting In Russia's War Against Ukraine. Retrieved from https://www.popularmechanics.com/military/a40298287/drone-fighting-ukraine-war-russia/ .
3. David Hambling. (22.05.2022). How Drones Are Making Ukrainian Artillery Lethally Accurate. Retrieved from https://www.forbes.com/sites/davidhambling/2022/05/12/drones-give-ukrainian-artillery-lethal-accuracy/?sh=16e14ec4424b.
4. Hannah Fuchs. (04.05.2022). Ukraine: How drones are changing the way of war. Retrieved from https://www.dw.com/en/ukraine-how-drones-are-changing-the-way-of-war/a-61681013 .
5. Sébastien Roblin. (30.06.2022). Russia's War in Ukraine. Retrieved from https://insideunmannedsystems.com/russias-war-in-ukraine/ .
6. Igor Kosov. (26.07.2022). A Game of Drones: Ukraine builds up UAV fleet. Retrieved from https://kyivindependent.com/national/a-game-of-drones-ukraine-builds-up-uav-fleet .
7. Analysis of the opportunities for employment unmanned aerial vehicles class mini in artillery formations
8. https://aerorozvidka.xyz/uk/
9. https://tealdrones.com/suas-golden-eagle/
10. https://www.skydio.com/skydio-x2
11. https://www.avinc.com/tms/switchblade
12. https://www.wbgroup.pl/en/produkt/warmate-loitering-munitions/

REMOTELY PILOTED AIRCRAFT SYSTEMS (RPAS) IN SERVICE TO ARTILLERY FORMATIONS

Ivaylo Zh. Bozov

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

***Abstract**: The dynamically changing security environment, defined by the constantly changing nature of armed conflicts, characterized by the introduction of new technologies and the related introduction of new ways of conducting combat operations, present the armed forces with new challenges. The need to implement new methods of target acquisition and adjusting fire necessitates the use of unmanned aerial vehicles (UAVs) in artillery formations. The aim of this report is to present the possible methods of target acquisition and correcting the fire of artillery formations using RPAS.*

***Keywords:** RPAS, UAVs, fire support, artillery, target acquisition.*

Introduction

The experience of wars and armed conflicts of the last decades convincingly testifies to the objective need for air reconnaissance, in the interest of fire support (artillery, aviation, naval artillery).

One of the ways to increase the effectiveness of fire support is establishment an effective intelligence system and coordinating it with the combat forces and means.

The most promising means of reconnaissance at the moment are RPAS, allowing to quickly and with high accuracy obtain intelligence data for targets at a great depth in the location of the opposing forces. RPAS have become one of the types of weapons that received a strong launch in development during armed conflicts in recent years. At the moment, one of the most important tasks assigned to these systems is support of artillery formations during the execution of firing tasks as a means of target acquisition and adjusting the fire. The war between Russia and Ukraine fully confirms this, where battles are leaded mainly by artillery formations directed by RPAS. Studying the experience of the armed forces of developed economic countries is important from the point of view of developing methods for adjusting the fire at typical targets using such aircrafts.

An increasing number of manufactured UAVs (depending on the class and level of equipment) are capable of performing tasks related to artillery reconnaissance and artillery fire adjustment.

1. Tasks performed by RPAS in the interest of artillery

The preparation of data for artillery fire is carried out in several ways, the main of which are full preparation of shooting data, adjusting of fire and transferring fire from a shooted point. While full preparation and transfer of fire from a shooted point shooting can also be conducted at unobservable targets, adjusting of fire is necessary the target to be observable. When are finding the data necessary to hit the target (by differend methods), the next step is fire for effect. It is assessed whether the bursts hit the target and what is the degree of damages, and if is necessary, the fire is corrected.

Artillery fire correction means measuring the range and deviations of the burst (group of bursts) from the target by reconnaissance means and transforming them into corrections for the firing position. To determine the corrections, it is necessary to determine the distance and direction from the firing position (FP) to the target (the center of a group target) and to the burst(the center of the group of

bursts). The correction is the difference between the distance and direction from the FP to the target and to the burst.

Reconnaissance means used in artillery to determine topographical data to the target and to measure burst deviations from the target are:

- Radar stations;
- Sound reconnaissance points;
- Optical means from ground points (forward observer - FO)
- Air reconnaissance assets.

Air reconnaissance in the interests of artillery is characterized by certain advantages over others:

- Observation in great depth of opposing forces;
- Obtain a real, accurate and clear image of the target and bursts, in real time or with minimal delay;
- Some of the unobservable targets become observable, then the order of striking the targets is changed;

One of the ways to adjust artillery fire is with the help of a helicopter. The specifics and order of firing are described in " Правила за стрелба и управление на огъня на земната артилерия " - 98.

Although many advantages, the use of a helicopter to support artillery fire is carried out for target acquisition and support the artillery fire, mainly from territory occupied by our troops on a large strip. That fact does not allow high accuracy in determining coordinates of the targets. Due to the above reasons related to the safety of the crew and limited flight resources, the pilot-corrector cannot always correct the fire and assess the degree of defeat. Determining the real state of the target after fire for effect is also not always possible, due to the large distance to it. In addition, another disadvantages of using a helicopter as a means of artillery reconnaissance, is complex organization of subordination of the helicopter crew to the artillery commander.

All this necessitates the need to look for other ways of conducting reconnaissance and serving the artillery fire. RPAS is a very good and successful alternative. It is particularly effective in intersections, which are characterized by many spaces unobservable by forward observers.

The capabilities of RPAS to service artillery fire significantly depend on the type and characteristics of the aircraft and the formation in whose interest they are used.

Modern RPAS must take into account the specifics of the combat use of artillery (mortar) formations to ensure the following tasks:

- conducting reconnaissance (additional reconnaissance) of enemy objects (targets) in real or with minimal delay, with the necessary accuracy in determining coordinates (grid, polar) and height above sea level;
- determination of shooting weather conditions and their consideration when calculating shooting data by compiling a "Meteorological" sheet;
- serving the firing of artillery (mortar) formations;
- analysis of damage attack;
- reconnaissance of routes and areas for firing positions;
- indicate of targets - when using high-precision ammunition.

These systems must maintain compatibility with the automated artillery fire control system (if available).

Class I UAVs - "small" and "mini" according to NATO standards [6] and "Концепция за въздушно наблюдение и разузнаване с БЛС в РБ"[7] are the most suitable for performing such type of tasks.

Depending on the scale of the military operation, the rank of formations and the assigned mission, three groups of tasks should be considered:

[6]Joint Doctrine Note 2/11 - The UK approach to Unmanned Aircraft Systems, 2011;
[7]Concept for aerial surveillance and reconnaissance with unmanned aerial systems by the Armed Forces of the Republic of Bulgaria, Ministry of Defense, 2012.

1. Target acquisition and servicing the firing in the interest of formations with the rank of battalion - **battalion artillery** for direct support (mainly mortar batteries). These formations mainly use RPAS of the "mini" category with a smaller range, with fixed wings or multi-rotor ("copter" type). The characteristics of these aircraft meet the requirements for reconnaissance in the close tactical area and the area of responsibility of formations of battalion rank;
2. Target acquisition and servicing the firing of **artillery formations for direct support** (battery, division) with the aim of hitting artillery batteries, command center and observation posts, mobile and stationary fire, etc. along the entire depth in the area of responsibility of the joint military formation. For the performance of these tasks, class I RPAS - "mini" and "small" are mainly used. They are characterized by a greater range of action and a greater period of time to stay in the air;
3. Target acquisition and servicing the firing of **artillery formations for general support** (division) in order to hit certain important targets (highly accurate weapon, counter-battery combat, command center, vehicle columns, air defense systems, etc.). Class I - "small" RPAS are used for the performance of such tasks, and a large part of the aircraft are also equipped with means for targeting high-precision munitions.

2. Organization of the interaction for acquiring and damaging targets.

The commander of the artillery formation (division commander) organizes the interaction with the assigned RPAS through the tactical operations center of the division.

When organizing the interaction, the chief of staff does the following:

- organize communication with the RPAS commander;
- informs the RPAS commander about the coordinates and callsigns of the batteries and the division;
- determines the method and order of firing (correction of fire in the course of firing to hit) and notifies the RPAS commander about it;
- designates (coordinates) the area for reconnaissance by UAV (where reconnaissance, target acquisition and service artillery fire will be conducted).
- establishes control signals;
- determines the time of readiness of the RPAS to serve the firing.

The division (battery) commander receives intelligence and target acquisition data from the RPAS commander or through the division's TOC, and these data must include:

- number and nature of the target;
- coordinates and absolute height of the target, the number and coordinates of individual targets part of a group target (if necessary);
- dimensions of the target - front and depth;
- target behavior and degree of protection of soldiers and equipments;
- a digital image of the target (if the necessary means are available to make such a connection);
- target detection time and confidence level.

The equipment of a large part of UAVs used in the interest of artillery allows to determine the grid coordinates of the target and bursts, deviations of the bursts from the target in meters, as well as polar coordinates to the target (burst) relative to the position of the UAV. With the help of RPAS, it is expedient to shoot at targets whose coordinates are determined by the same aircraft. If coordinates are determined by other means, they are refined when the target is detected by UAV (reconnaissance, detection of the target). In this way, errors from the preparation of data for shooting of the various detection means is avoided. To determine the corrections, the coordinates of the target, determined with the help of the aircraft serving the shooting, are used.

When the division (battery) is ready to fire, the RPAS commander is notified of the number of shots, which have to be observed and the time of flight of the rounds. Fire is permitted at the indicated

rate after the RPAS commander's report of readiness to locate the bursts, and he is ordered to locate them.

To simplify aiming (correction of fire) with the help of RPAS, it is recommended to use grid coordinates of the target (bursts). Determination of corrections is done by calculation, automatized fire control systems - AFCS, computers or "Прибор за управление на огъня - ПУО".

Shooting with the help of RPAS is associated with difficulties in detecting and identifying the bursts of the service formation due to the large field of view provided by the aircraft. Conducting shell fire with a high-explosive detonator in place increases the reliability of detection and assessment bursts because the hole is better observed by the UAV's operator. Therefore, to increase the reliability for detecting bursts, it is advisable to conduct the firing with the installation of the high-explosive detonator. In the presence of fuze at the firing position, it is advisable the first shot with a fuze from the battery's main gun.

Conclusion

RPAS are capable to perform a large number of tasks - reconnaissance, combat missions, serving of artillery fire and many others. The latter are subdivided into: surveillance, additional reconnaissance, target acquisition, firing support, targeting of high-precision ammunition and assessment of the degree of damages.

The use of RPAS enables reconnaissance and target acquisition in the so-called "invisible fields" (unobservable areas). In addition, targets that are unobservable for forward observers can be observed with RPAS, which objectively leads to a change in the order of shooting these targets and reducing the expenditure of ammunition required to damage the target;

The difference between a helicopter and a RPAS to detect and ensure effective engagement of ground targets is that, in addition to the risk of losing expensive equipment, in firing service there will always be a risk of losing the crew on board. In addition, the crew's work under combat stress is more prone to error than the work of a RPAS operator, who may be miles away from the enemy forces;

The experience of recent conflicts and wars convincingly shows that RPAS are mandatory tools of military formations. Reconnaissance, surveillance and target acquisition with such systems would inevitably increase the effectiveness of artillery fire.

References

1. Марков Д.К., Чалъков Р.Б., (2018). Поразяване на цели и коригиране на огъня на дивизионите за непосредствена огнева поддръжка с АСУОАД „Вулкан - С" ПИКИС с помощта на безпилотни летателни апарати. *Годишник - Предизвикателства пред обучението и подготовката в контекста на политиката за сигурност и отбрана на Европейския съюз"*. Военна академия „Г. С. Раковски", ISSN 1312-2991, стр 133-141;
2. Кацев И.Г., (2019). Метод за класификация и приоритизиране на целите, поразявани от артилерията. *International Scientific Conference — Defense Technologies DefTech 2019*. Shumen, Bulgaria, ISSN 2367-7902, стр. 235- 241
3. Калиной А.И., (2016). Применение комплексов воздушной разведки для обслуживания стрельбы артиллерии. *Перспективы развития и применения комплексов с беспилотными летательными аппаратами*. Коломна, УДК 681.51, стр. 101-107;
4. Правила стрельбы и управления огнем артиллерии (ПСиУО-2011), Москва, 2011

CONTEMPORARY EDUCATIONAL TECHNIQUES: GAMIFICATION

Ivelin G. Katsev

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

***Abstract**: Motivation can become a problem for learners, especially when they do not find the purpose of a learning activity or it is not clear and understandable. Gamification is a recent concept, primarily from the web and gaming development industry that can make learning activities more active and participatory, gamification can also provide solution to trainee's motivation problems.*

***Keywords**: Education, Gamification, Game Thinking.*

Introduction

Education is an active process and as with all active processes, requires motivation both to initiate and prolong it. For younger learners, the motivation to acquire knowledge may often not be present, while for senior learners it may be present, or opposite and this is particularly so for cases when an element of self-direction and autonomy is required. Since learning is a process in which knowledge and skills are accumulated, it follows that there could be great benefits from incorporating game concepts into education.

Games and their technologies are increasingly transcending the traditional boundaries of the software environment, as evidenced by an increase in the creation of serious and comprehensive games in industry and research. In recent years the tendency to accelerate influence of the software sphere, more precisely entry of computer (video) games into industry, business and education has led to the identification of the term "Gamification".

Gamification can be characterized as the use of game elements and game thinking in non-game environments to increase the student's employment and motivation in the relevant field. It originates from the computer game industry and when it is used in a business environment, this process can be defined as integrating game dynamics into a website, business service, online community, content portal, or marketing campaign to initiate participation and increase user engagement.

At a fundamental level gaming techniques tap into and influence people's natural desires for competition, achievement, recognition, and self-expression.

The main components of gamification are:

- Elements of computer (video) games, not entire games – these elements must be aimed at acquiring specific knowledge or skills;
- "Game thinking" - a proven innovation system based on techniques acquired while playing games, on figure 1 are shown main elements that form the game thinking.
- Building knowledge and skills through gamification applicable outside the game environment;

Figure 1. Elements that form the game thinking

- Increasing the employment and motivation of trainees in a predetermined direction.

The concept of gamification and its techniques in non-game environments are proving to be innovative and accelerate emerging learning practices. Although still in its infancy, the dynamics and techniques of gamification have been found to be successfully implemented in some areas of industry and business. Examples of this are:

- America's army - an official game of the US army, developed for recruitment. The game works primarily as a marketing tool, promoting the US military and thereby increasing the number of recruits;
- M&M's Eye-Spy Pretzel - in 2013, the M&M company introduced its game M&M's Eye-Spy Pretzel, as part of its marketing campaign, this game is a classic example of gamification;
- NikeFuel - The NIKE Company releases a game that allows the NIKE+ community to compete with each other. NikeFuel aims to increase the sports activity of users, create the possibility to share the results of sports activities and promote the sports brand.

It should be noted that games like streamed of twitch or other streaming platforms do not apply to gamification. It is related to the use of game elements outside of games. The entire computer game does not belong to gamification.

Aside from complete computer games, there are several other terms that can easily be confused with gamification. Serious Games and Playful Design do have something to do with gamification, but they are actually something else:

- Serious games are fully constructed games that are goal-oriented, with clear rules, tasks and restrictions to achieve a given goal. Examples of serious games are simulators for pilots, medical professionals and others.
- Playful Design has no specific goals, rules, or meaningful choices that make it a serious game or gamification.

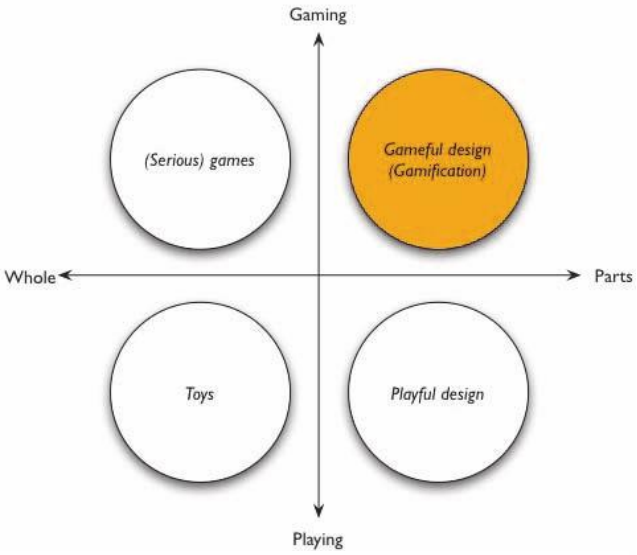


Figure 2. Differences between serious games, playful design and gamification

Most common differences between serious games, playful design and gamification are presented on figure 2. Gamification is on the right side of the spectrum. It doesn't offer a complete gaming experience, but some game elements are used. Although there is sometimes confusion between Gamification and Playful Design, there is a clear difference: Gamification sets a clear and specific goal for its users, has rules and restrictions that make it like a game. There is a challenge to achieve the goals that are set. For achieving the goals, tasks, exams and others, there are some components that can be added into gamification:

- Points - which the learner can earn after mastering certain knowledge;
- Prizes - for which the learner can use his points;
- Badges - type of awards that the learner receives after successfully passing an exam;
- Rankings – tables in which to note the progress of each learner.

Those components can play a vital role in motivation the students/trainees to proceed with the education that is mostly explained by implementing Maslow's popular behavioral model - Hierarchy of Needs into gamification education, which identifies that humans have a number of needs that we strive to fulfill in our lives and gamification can be used to promote and achieve the first three levels. According to Dan Pink's "The Surprising Truth About What Motivates Us" (Pink, 2011), the hierarchy of needs correlates with the basic principles of gamification and explains that deficit of needs in the model are met through long-term interaction with the gamification method, where people can achieve a higher level of social

status, cohesion and reputation. The reason gamification is so successful is because of the rewards provided on top of Maslow's model of self-actualization. By playing the same 'game', social cohesion is created and through the use of rewards and feedback, self-esteem and a sense of achievement are encouraged [7].

The Hierarchy of Needs from Abraham Maslow presented in his 1943 paper "A Theory of Human Motivation" in the journal Psychological Review is presented on figure 3.The Dan Pink's representation of Maslow's hierarchy of needs and its application in gamification is presented on figure 4.

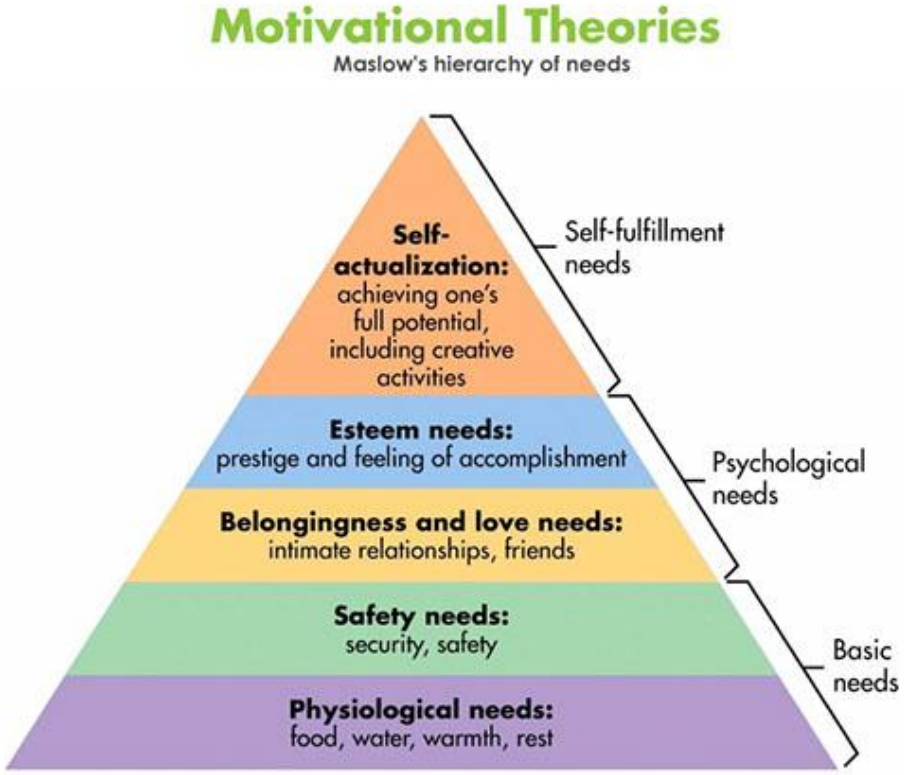


Figure 3. Maslow's hierarchy of needs.

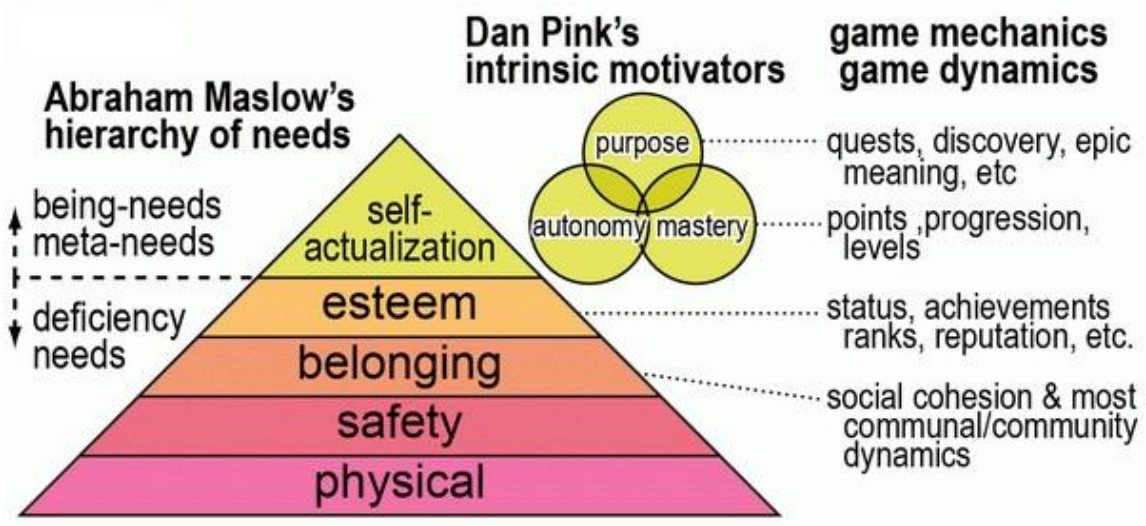


Figure 4. Dan Pink's representation of Maslow's hierarchy of needs and its application in gamification.

The benefits of implementing gamification in the learning process can be:

- Providing higher levels of motivation;
- Providing higher levels of productivity;
- Increasing the sense of shared goals;
- Increasing the continuity of repetitive, less exciting tasks;
- Greater individual and team achievements;
- Ensuring a timely understanding of the team's productivity;
- Gathering data that can assist managers/commanders in understanding the skill base of the team;
- Stronger commitment to an organization/mission/task;
- Greater transparency;
- Clearer accountability;
- Increased levels of staff retention;
- Immediate and ongoing feedback.

In addition to the advantages, some risks (disadvantages), hidden by gamification should be noted:

- Alienation of some trainees/students from the organization/mission/task;
- The system may not work for all areas and levels of teams/students/trainees;
- When there are winners, there are losers – it needs to be think about what effect will this have on them (losers);
- Some learners may react negatively to this type of training;
- Applying gamification to any aspect of learning can lead to a lack of focus and prevent interest in other more engaging phases or stages;
- Points and badges may become less exclusive over time, leading to a lack of interest in gamification;
- Education can be mindless if learning through gamification is not well thought out and not aligned to the desired level;
- Healthy competition can turn into destructive competition, creating divisions and preventing students/trainees cohesion;
- Cheating in gamification can lead to demotivation and dissatisfaction;
- Gamification can alienate older team members/learners who are unsure and unfamiliar with the terminology (this can apply equally to any team member/learner regardless of age).

In addition to what has been presented so far, gamification can also be used for training people with disabilities and anomalies, but due to their specific needs, in addition to gamification, they also need specific devices. People with disabilities and anomalies that have complex communication needs are around us and we often can't communicate effectively with them without any previous basic preparation. Augmented and alternative communication technology can be use as a an instrument to replace natural human speech or writing, as a way to communicate to educators, speech-language pathologists, physical therapists, occupational therapists and other medical specialist

Conclusion

The use of gamification in online and in-person learning increases the attractiveness of the learning material, highlights learning elements that may be more challenging to learn, and makes learning material (knowledge acquirement) an object of interest. Clearly defining the different stages in the game situations and the necessary steps to move to the next "level" helps to keep the interest of the learners.

Some statistics show that the use of gamification as a training method in some organizations may decline over time, this may be due to a number of factors including planning and implementation. If levels of difficulty or challenge are not increased, learners become bored and stop engaging and interacting with the gamification learning system. It is also an important element for educators to analyze the generated data and adapt the learning system or else there is an increment risk of learning failure.

With most gamification programs, the focus is on the final goal, not the journey to reach it. Gamers find that the most rewarding objective is devising a strategy to achieve mission's completion; to stop the opposing team or avoid the traps, not just to keep the badges/awards. Therefore, in order for gamification to continue its journey from the gaming industry to the halls or classrooms of educational institutions, it is necessary to carefully consider its purpose, as well as create a background plot on the path of learners to the ultimate goal.

The technologies of e-learning and gamification contribute significantly to the realization of the concept of lifelong learning. This development should make the educational process more effective, to provide more attractive ways for learning the material, which in turn will achieve a more sustainable personality development and knowledge acquirement by the learners.

References

1. Чонков, С., Цветанов, К., Перспективи на е-обучението и игровобазираното обучение като средства за повишаване на езиковата култура, *Научна конференция „Иновационни ИКТ в научните изследвания и обучението: математика, информатика и информационни технологии",*стр. 173-188, 2019.
2. Boer, P., Introduction to Gamification, 2013.
3. Bostwick, Ch., White paper on Gamification in app development. Previous implementations, possibile future implementations; small start to a broad topic and big future, University of Maryland University College, 2018.
DOI: 10.13140/RG.2.2.32434.09920
4. Deterding, S., et al, Gamification: Using Game Design Elements in Non-Gaming Contexts, International Conference on Human Factors in Computing Systems, Vancouver (Canada), 2011.
5. Dimitrova, D., Nedelchev, M., Digital technology as a part of habilitation and rehabilitation services for people with disabilities.
6. Glover, I., Play As You Learn: Gamification as a technique for motivating learners, World Conference on Educational Multimedia, Hypermedia and Telecommunications, Chesapeake, pp. 1999-2008, 2013.
7. Introduction to Gamification, Association for Project Management (APM), 2014, Paperback ISBN: 978-1-903494-51-6, EPUB ISBN: 978-1-903494-52-3
8. Pink, D., Drive: The surprising truth about what motivates us. book, Riverhead Books, 2011.
9. Smith, P., Serious Games 101. Report, S&I organization, STO-EN-MSG-115.
10. Tóth, Á., Tóvölgyi, S., The introduction of gamification: A review paper about the applied gamification in the smartphone applications, 7th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), 2016, ISBN:978-1-5090-2646-3.
DOI: 10.1109/CogInfoCom.2016.7804551
11. Uysal, H., Aydemir, S., Genç, E., Maslow's hierarchy of needs in 21st century: the examination of vocational differences, Researches on Science and Art in 21st Century Turkey, vol 1, ch 23, pp 211-227, 2017.
12. Walther, B., Playing and Gaming Reflections and Classifications,Game Studies the international journal of computer game research, vol 3, issue 1, 2003
http://www.gamestudies.org/0301/walther/
13. Wood, L. C., Reiners, T., Gamification, Encyclopedia of Information Science and Technology, ed 3, pp 3039-3047, 2015.
DOI: 10.4018/978-1-4666-5888-2.

ANALISYS OF ARTILLERY FIRE'S EFFECTIVENESS AGAINST UNITARY TARGETS: COMPARING CONTEMPORARY CONVENTIONAL PROJECTILES VERSUS PRECISION GUIDED PROJECTILES

Ivelin G. Katsev

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

***Abstract**: Artillery's effectiveness heavily depends on how accurate and powerful will be weapon delivery, which is mostly correlate to artillery projectiles' effect on the targets, on circular errors and lethal areas. Comparing contemporary conventional projectiles versus precision guided projectiles provides vital information for artillery commanders.*

***Keywords**: Damage probability, unitary target, contemporary conventional projectiles, precision guided projectiles.*

Introduction

In contemporary military conflicts the warring parties widely use artillery formations to fulfill their military missions or operational goals. Artillery is and proves to be the major combat element of the land component for engaging various enemy targets in combat. The main combat usage of artillery formations is fire support. Fire support is the main battle functions and represents firepower enforcement by using the fire of artillery weapon systems to support maneuver formations, last acquires great importance for the success of the operation. The prime employment of the artillery is to minimize the combat potential of the enemy group and to limit its capabilities in battle. As an essential tool of the land component involved in fire support, artillery plays a vital role in achieving and retaining fire superiority in operation.

The success of operation depends heavily on the effectiveness of fire support, which in turn depends on the effectiveness of the forces involved in the fire support. A significant part of the effective use of artillery formations lies in the effectiveness of the fire impact on the enemy's targets. Artillery formations conduct fire tasks against different enemy targets and objects. Targets and objects in the opposing force in operations can be generally divided into unitary and area targets. To fulfill the purpose of this study, we will focus on the unitary targets and an evaluation method of the artillery's effectiveness against unitary targets while using precision (guided) projectiles compared to contemporary conventional projectile.

The efficiency of artillery fire against unitary target depends mainly on the probability that the target will be damaged or destroyed. This probability changes as a result of the deviation in the distance and direction of the mean point of impact from the target center (aiming point). Deviations in distance and direction are caused by a number of random errors associated with the specificity of the work of the artillery formations in the preparation of fire data, such as miscalculation of latitude and longitude of fire position, distance to target, wind effect and uncertainties in target's location. Random errors are typically divided into two groups. First ones are the repetitive errors. They are repeatable for all shots and these errors are associated with inaccuracies in the targeting due to errors in the calculation of the fire position,

observation post and target locations, errors in aiming the weapon systems, errors in determining the meteorological and ballistic conditions, and others. The second type of random errors are the non-repetitive errors, which refers to ballistic projectile errors caused by variations in the shape of the ammunition, the angle of projectile discharge, the amount of gunpowder used in the shells and others.

The Factors that influence the effectiveness of artillery fire can be summarized as:

- characteristics, type, dimensions and resilience of the targets;
- mobility of targets;
- accuracy in determining artillery firing data;
- characteristic of technical dispersion and reliability of weapon systems;
- projectiles' lethal area;
- amount of artillery systems;
- expenditure of projectiles;
- method of weapon delivery;
- accuracy of correction in unadjusted fire;
- countermeasures by the opponent.

These factors are increasing its influence in urban environment. The urban combat is characterized by a complex and multi-dimensional operational environment, the limited visibility in observation and adjusting fire and the inability to fully assess the efficiency of artillery fire result in difficulties for artillery units achieve high efficiency [1].

In addition to those factors, the effectiveness of fire support is also influenced by the reach of fire; it is characterized as the ability that own formations can affect a given target at a certain distance and firing direction.

1. Theoretical aspects

There are some elements of artillery's effectiveness calculation that needs to be determined:

- The mathematical model for effectiveness calculation;
- The types of targets that will be reviewed;
- The type and characteristics of the projectiles.

1.1. Mathematical model for assessing effectiveness of artillery.

The model for assessing the efficiency of damage from fire systems is based on determination of a precision function and a damage function.

The accuracy function depends on the repetitive errors in the fire data preparation. These errors can be represented by a range error probable and deflection error probable as a quantum of random errors. Those random errors are normally distributed and independent from each other.

$$(1)\ E_x = \sum_{i=1}^{n} E_{x_i}$$

$$(2)\ E_y = \sum_{i=1}^{n} E_{y_i}$$

where E_{x_i} and E_{y_i} - random error of i-th element, i - elements involved in the fire data preparation, E_x and E_y – repetitive errors in range and defection direction.

Errors due to ballistic dispersion occur for each round fired from weapon systems and may be denoted by E_{d_x} for random dispersion error in range and E_{d_y} random dispersion error in deflection.

In order to determine the efficiency of artillery fire from closed fire positions against unitary observable ground targets, standard deviation of errors is used and according to the normal distribution law, the standard deviation is calculated by following formulas:

$$(3)\ \sigma_{mpi_x} = \frac{E_x}{0.6745}$$

$$(4)\ \sigma_{mpi_y} = \frac{E_y}{0.6745}$$

$$(5)\ \sigma_{d_x} = \frac{E_{d_x}}{0.6745}$$

$$(6)\ \sigma_{d_y} = \frac{E_{d_y}}{0.6745}$$

$$(7)\ \sigma_x = \sqrt{\sigma_{mpi_x}{}^2 + \sigma_{d_x}{}^2}$$

$$(8)\ \sigma_y = \sqrt{\sigma_{mpi_y}{}^2 + \sigma_{d_y}{}^2}$$

where σ_{mpi_x} and σ_{mpi_y} – standard deviations or repetitive errors in preparation of fire data, σ_{d_x} and σ_{d_y} – standard deviations or non-repetitive errors due to ballistic dispersion, σ_x and σ_y – standard deviations of the sum of standard deviations of errors due to normal distribution law.

The damage function determination depends on the power of the weapon systems, the artillery shells and type of the target. The damage function of a fragmentation projectile is represented by the Carleton damage function. To determine the power of the weapon systems and the impact of the projectiles on the target, we calculate the lethal area of the target from a single round by:

Carleton damage function is used for calculating fragmentation lethal area of an artillery shell with basic data considered for projectile mass, caliber and amount of shrapnel. The damage function also consider impact angle and output data is effective weapon area:

$$(9)\ a = 1 - 0.8 * cos\,\theta$$

$$(10)\ S_r = \sqrt{AL * a}$$

$$(11)\ S_d = \frac{S_r}{a}$$

where a - impact angle coefficient, θ - impact angle, AL - target lethal area, S_r - effective weapon length, S_d - effective weapon width.

In some cases, unitary targets require a hit by single shot to be destroyed, that demands the single sortie probability of damage to be determined. This probability is calculated by using the cumulative function of the normal distribution by the formulas:

$$(12)\ P_x = 2 * \ normcdf\ \frac{S_r}{2}, 0, \sigma_x\ - 0.5$$

$$(13)\ P_y = 2 * \ normcdf\ \frac{S_d}{2}, 0, \sigma_y\ - 0.5$$

$$(14)\ P_{hit} = P_x * P_y$$

where P_x - probability of damage in range direction, P_y- probability of damage in deflection direction, P_{hit} - single sortie probability of damage.

The probability of damage due to the number of shots, fired from weapon systems is determined by the formula:

$$(15)\ P_{=1}^{k} = 1 - \ 1 - P_{hit}\ ^{n}$$

where $P_{=1}^{k}$ - the probability of damage after firing the n shots, n - number of shots fired.

Some targets require more than one hit to be damaged; such targets must be struck by a certain number of shots to be destroyed, so we have to determine the probability of the target being hit by the minimum number of rounds necessary for its destruction. For this purpose we use the cumulative function of binomial distribution:

$$(16)\ P_{\geq 1}^{k} = 1 - binocdf\ u - 1, n, P_{hit}$$

where $P_{\geq 1}^{k}$ - probability of damage, u - number of hits required for target destruction.

1.2. Unitary targets.

Objects and objectives in the composition of the opposing force in the area of operation, in addition to their basic division into individual and group, are separated into:

- Armored and non-armored;
- Concealed and unconcealed placement;
- With high and low mobility.

Unitary target which will be calculated the efficiency of damage from artillery systems are presented in table 1 with their possessed characteristics and lethal areas.

Table 1. Unitary targets to be attacked by artillery formations during fire support in contemporary operations.

№	Name of the unitary target	Characteristics of targets			
		protection	placement	mobility	Lethal area, m^2
1.	Radio location station (Radar)	non-armored	unconcealed	low	1100
2.	Armored combat vehicle	armored	unconcealed	high	70
3.	Tactical operation center (TOC)	non-armored	concealed (disguised/ camouflaged)	low	530
4.	Towed artillery howitzer/mortar team	non-armored	concealed (disguised/ camouflaged)	low	510
5.	Forward observer post	non-armored	concealed (disguised/ camouflaged)	low	260
6.	Military land transport vehicle	non-armored	unconcealed	high	360

Table 1 shows most common unitary targets, with their characteristics, that will be affected by artillery fire during fire support of maneuvered formations in contemporary operations.

1.3. Artillery projectiles

Artillery munitions are major factor influencing artillery fire and carry a great deal of weight in determining its effectiveness. Lethal area dimensions, and dispersion, and range of projectile are the most important factors that affect the effectiveness of firepower.

Conventional artillery ammunitions are characterized by high dispersion and a relatively short maximum flight distance, while retaining good lethal area.

Overview of example of contemporary conventional artillery ammunition is M795. It is 155mm artillery projectile that can be fired from all NATO standard 155mm /L52 guns and has maximum range of 22.5km, lethal area of around ~1000м^2 and circular error probable (CEP) of 50metres.

Precision (guided) projectiles are the bread and butter of contemporary artillery systems. They can be characterized with extremely high precision, longer range and good lethal area.

Overview of example of precision (guided) artillery projectile is M982A1 – Excalibur.

The Excalibur (XM982, M982 and M982A1) is a 155 mm, Global Positioning System (GPS)-guided, extended range artillery projectile in use as the Army's next-generation cannon artillery precision munitions. It provides improved fire support to the maneuver force commander, increases lethality and reduces collateral damage. The target, platform location and GPS-specific data are entered into the projectile's mission computer through an Enhanced Portable Inductive Artillery Fuze Setter. The Excalibur projectile uses a jam-resistant internal GPS receiver to update the inertial navigation system, providing precision in-flight guidance and dramatically improving accuracy to less than two meters miss distance regardless of range. The Excalibur projectile has three fuze options (point-detonation, point-detonation delay and height-of-burst) and is employable in all weather conditions and terrains. The Excalibur's capabilities allow for first-round effects-on-target while simultaneously minimizing collateral damage and the number of rounds required to engage targets [3]. It is also characterized with CEP of 4 meters.

2. Analysis of artillery fire's effectiveness against unitary targets while using precision projectiles

Assessing the efficiency of artillery fire while using contemporary conventional projectiles and precision (guided) projectiles, and analysis of artillery fire's effectiveness against unitary targets while using precision projectiles will be completed in following tables.

Table 2. Efficiency of artillery fire against unitary targets, when using contemporary conventional projectiles versus using precision (guided) projectiles.

№	Name of the unitary target	degree of destruction	Number of artillery projectiles	
			M795	M982 – Excalibur
1.	Radio location station (Radar)	30%	6	1-2
2.	Armored combat vehicle	10%	56	1-2
3.	Tactical operation center (TOC)	30%	12	1
4.	Towed artillery howitzer/mortar team	30%	12	1
5.	Forward observer post	20%	10	1-2
6.	Military land transport vehicle	30%	14	1-2

Table 2 reveals the differences in round fired upon unitary targets during fire support of maneuvered formations in contemporary operations.

Conclusions from table 2

- When artillery formation attack with adjusted fire radio location stations (radar) with contemporary conventional projectiles such as M795 artillery ammunition, for achieving the accepted, in NATO's STANAG agreements, degree of destruction. On the other hand when artillery formation use precision (guided) projectiles such as M982 – Excalibur, most of the time there will be no need for second round to be fired due to increased accuracy (low circular error probable).
- When artillery attack armored combat vehicle with conventional projectiles, due to low lethal area of the unitary target and vast CEP, the rounds fired are increasing significantly even with lower degree of destruction. Opposite to that using M982 – Excalibur with its increased precision (quiet low CEP) will be needed not more than two rounds for destroying the armored combat vehicle.
- When employ artillery units to destroy tactical operation center (TOC) and towed artillery howitzer/mortar teams, which are not in fortifications, to achieve desirable degree of destruction twelve rounds are needed. When using M982 – Excalibur there is no need to conduct more than one shot for each target because both of them are not armored, with huge lethal area and all elements of the target are close to each other.
- With regards to last two targets in the table 2 things are similar to the previous unitary targets, while precision (guided) projectiles would need no more than two rounds to complete the fire task.

3. Conclusion

In contemporary conflicts, the percentage of unitary targets compared to group/area targets is significantly lower, but nevertheless they represent a serious threat to allied forces and must be defeated accordingly. Those targets can be dealt with successfully while using contemporary conventional munitions, but to achieve destruction on them large amount of projectiles needs to be fired. Employing whole artillery battery for firing those projectiles will hasten the shooting, but will expose all artillery systems in the battery to opposing forces. On the other hand using a platoon will both hasten weapon delivery

and not exposing all artillery systems to opposing forces, but still half of the artillery systems in the battery are revealed.

To solve the survivability problems and to achieve greater effectiveness of artillery it's appropriate for precision (guided) projectiles to be using for unitary targets. When this type of projectiles are used one artillery system only can be employed to conduct quick and clean (precise) fire task with one or two rounds fired. Precision (guided) projectiles such as M982 – Excalibur, Vulcano 155, 2K25 Krasnopol and others, are modern solutions for artillery formations to accomplish higher efficiency and effectiveness in the dynamic and difficult to predict operational environment in contemporary conflicts.

References

1. Бозов., И., Характеристики влияещи на бойните действия в град и отражението им върху огневата поддръжка от артилерията, Годишна университетска научна конференция НВУ „В. Левски" 2020, част 1, стр. 117-124. ISSN 1312-6148.

2. Чанев, Ст., Фактори оказващи влияние на оперативните способности на групировка за противовъздушна отбрана, Годишник на НВУ „Васил Левски": част II. с. 91-97. ISSN 1312-6148.

3. Brady, M., Goethals, P., Comparative analysis of contemporary 155 mm artillery projectiles, Journal of defense analytics and logistics, Vol. 3, No. 2, 2019, pp. 171-192.

DOI 10.1108/JDAL-05-2019-0011

4. Excalibur Precision 155 mm Projectiles

Assets on: https://asc.army.mil/web/portfolio-item/ammo-excalibur-xm982-m982-and-m982a1-precision-guided-extended-range-projectile/

5. Robinson, J., Berefelt, F., On Guidance and Control for Guided Artillery Projectiles, Part 1: General Considerations. Technical report, 2011, p. 29, ISSN-1650-1942.

6. 155MM M795 HE, High explosive artillery projectile.

7. Assets on: https://www.gd-ots.com/wp-content/uploads/2021/02/155mm-M795-HE-ArtilleryProjectile-202007-1.pdf

ORIGIN AND DEVELOPMENT OF PSYCHOLOGICAL OPERATIONS FROM ANCIENT TIMES TO THE PRESENT DAYS

Veliko P. Petrov

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

Abstract*: A report for the purpose and for the benefit of the reader with the knowledge and development of psychological operations from antiquity to the present day. Psychologically, operations were probably carried out even in ancient times and included the "face in the face" communication, with some one person experiencing it through gestures, thoughts, actions or actions (or in combination with tyah) and influencing another person. From time immemorial, psychological operations have been the preferred strategy for wars, which are more and more important when successfully planned and carried out in modern military operations. Because of the control over the mislit, psychic states, the effect on the horata and the formirano, improved and paseno kato secret weapons from the priests, dzharzhavnitsy and military commanders on Babylon, Egypt, China, Ancient Georgia and Rome.*

We can only define "psychological operations" thanks to the most powerful "weapons" for comprehending on setting military and political goals of the century on information technology, thanks to this through manipulation on the enemy, creating an opportunity for a forest victory without water for military operations.

"Psychological operations" sa planirani operations for podnasyan on selectirana information is alien to the audience with the goal of influencing the top of it, which uses various non-violence methods (inspire fear, szdavane panic, mass psychosis, special sympathy and other methods for destroying the mental balance). Review the psychological characteristics of the target audience (culturally, national consciousness, social discipline, traditions in the family and social life, morality, religion, etc.) and psychologically base the mechanisms that influence the behavior of this, which is the result of persuasion (due to the use of logic, fear, desires and other mental factors), instead of physical coercion, psychological operations are a prerequisite for determining emotions, blasphemy or behavior at the top alienate governments, organizations, groups and individuals.

Key words: *psychological operations*

ВЪЗНИКВАНЕ И РАЗВИТИЕ НА ПСИХОЛОГИЧЕСКИТЕ ОПЕРАЦИИ ОТ ДРЕВНОСТТА ДО НАШИ ДНИ

Велико П. Петров

Терминът „психологически операции", известен още и като: MISO, PsyOps, Political warfare, "Hearts and Minds" и пропаганда се използва за описание на действия, които имат за цел да породят планирани реакции в други хора, използвайки основно психологични методи.

Психологическите операции са провеждани още в дълбока древност. Вероятно те са включвали общуване „лице в лице", при което един човек се е опитвал чрез жестове, думи, викове или

действия (или в комбинация от тях) да повлияе на друг човек. От древни времена пълководци и военачалници знаят стойността на понижаването на морала на противниците си. Войниците в римските легиони използват тактика на шок и страхопочитание, за да тероризират враговете си, като тропат с мечовете на щитовете в ритмичен модел.

Известно е да са правени опити още в древността за психологическо въздействие върху противника с цел дезинформация, сплашване и деморализация. Целенасоченото психологическо въздействие на човек върху човек с цел промяна на поведението на друг се използвало от възникването на първите контакти между хората. Една от библейските легенди разказва как Гедеон, водейки война с многобройните си противници, често е прибягвал до военни трикове, дезинформация и сплашване на неприятелите. Веднъж е успял толкова да сплаши противника, че той, след като е загубил контрол над действията си е насочил своите удари срещу войските си.

Изкуството за контролиране на мислите, психичните състояния, действията на хората е формирано, усъвършенствано и пазено като тайно оръжие от жреците, държавниците и военачалниците на Вавилон, Египет, Китай, Древна Гърция и Рим[1].

Основните принципи на психологическите операции са развити през втората половина на шести век преди новата ера от китайския военен стратег Сун Дзъ в знаменития трактат „Изкуството на войната"[2]. В тази много популярна и в наши дни книга той посочва, че предпочитаната стратегия при воденето на войни е манипулирането на противника по начин, който да създаде възможност за лесна победа без водене на военни действия. Според Сун Дзъ най-добрият начин да се постигне победа, е като се атакува стратегията на противника, след което усилията да се насочат към неговите съюзници, а след това да се атакуват войските му, като щурмуването на неговите укрепени градове е най-лошият избран начин за постигане на победа.

Може би един от най-ранните примери за военни психологически операции се приписва на Александър Велики. Във всеки завладян регион той е оставял войници, чрез които е поддържал контрола над завладяната територия. Въпреки това, дойде момент, когато Александър осъзна, че е разпръснал твърде много армията си и сега е в опасност да загуби от голяма противникова военна сила. Единствената възможност на Александър беше да отстъпи и да се прегрупира с армиите, които беше оставил. Въпреки това той знаеше, че ако го направи, това със сигурност ще провокира противника да го преследва и много вероятно да го победи. Александър Велики осъзнава, че единственият шанс за победа ще бъде способността да сплаши врага, така че враговете да се страхуват да преследват отстъпващата му армия. Александър инструктира своите оръжейници да изковат много огромни брони и шлемове, които да пасват на гигантски воини с височина от 2,2 до 2,4 метра. Бронята беше доста смачкана, нарязана с мечове, за да изглежда реалистична, и произволно разпръсната из лагера. Същата нощ армията на Александър започва да се изтегля. На следващия ден изоставената огромна броня беше намерена от врага, който влезе в бившия лагер. Огромните доспехи, съчетани с историите, които врагът чува от пътниците за жестокостта на армията на Александър, предизвикват достатъчно съмнения и страх, че е решено да не се преследват македонските войски, за да не се сблъскат с жестоките гиганти, които със сигурност биха загубили[3].

В древен Египет се е вярвало, че котките улавят отражението на залязващото слънце в очите си и го пазят до сутринта. Това направи незаконно убиването на котки, с изключение на ритуалните жертвоприношения, извършвани от свещеници. През 525 пр.н.е. персийските и египетските войски водят ожесточена битка за град Пелусиум. Жителите на Пелузиум почитали котките като богове. Техният враг знаеше за тази вяра и се възползва от нея. Персите разположиха силите си в селата и градовете в околността, като заловиха колкото се може повече котки. Когато египтяните

[1] Лукин Е.В., Психологические основы информационной войны, центр стратегических оценок и прогнозов, http://csef.ru/ru/oborona-i-bezopasnost/265/psihologicheskie-osnovy-informaczionnoj-vojny-3725, стр. 2

2 Суан Дзъ,(2005) "Изкуството на войната":Древни китайски трактати,Труд.

[3] История возникновения информационных войн и их трансформация в современных условиях, https://onkto.ru/blog/psychology/istoriya-informatsionnykh-vojn, стр. 1

нападнали персите, персите пуснали стотици паникьосани котки на бойното поле, с което се постигна объркване сред египетските редици. Тогава персийските войски напреднаха и всеки от персийските войници държеше котка. Египетските войници не посмяха да влязат в битка с врага или да стрелят по тях, страхувайки се, че това може да застраши живота на котките. Персите бързо разпръсват противника и отбраната на града. След превземането на града, персите са показали презрението си към египтяните, като са хвърляли котки в лицата им.

През 13 век след Христа лидерът на Монголската империя, Чингис хан, е бил широко известен с това, че води орди от диви конници. Монголите поддържат образа на жестоки варвари. Чингис хан широко използва доста модерни методи за психологически операции, дезинформация и оперативна сигурност, насочени към процеса на вземане на решения от неговите противници. „*Агенти на влияние*" били изпратени пред неговите армии, за да разпространяват слухове за изключителната жестокост и безбройността на воините в монголската армия. Хан също използва измама, за да създаде илюзията за значително числено превъзходство, като симулира огромни маси от войски в бързо и скрито прегрупиране. Когато монголските войни пътували, те влачили големи предмети зад конете си, за да създават прашни бури. Прашните бури създаваха впечатление за огромна настъпваща маса войски. Чингис хан също заповядва на войниците си да палят стотици допълнителни огньове през нощта, което също увеличава впечатлението за размера на армията[4]. Чингис хан заповядва на всеки войник да носи три горящи факли през нощта, така че броят на хората му да бъде видим за него[5]. Монголските воини изстрелвали стрели с малки дупки, от които стрелите свистели по време на полет. Свирещият звук успешно изплаши врага. Монголските армии също използват отрязани човешки глави по стените на вражеските села, за да плашат местните хора. Всички тези действия предизвикаха слабост и страх в духа на враговете на монголите.

По време на Американската революция британската армия носи цветни униформи в опит да сплаши по-скромно облечената пехота от Континенталната армия на Джордж Вашингтон. Яркочервеното се оказва катастрофална грешка, тъй като се формират ясни цели за деморализираните американски снайперисти.

Практически препоръки за психологическото разложение на противника са разработени от Суворов, Наполеон и други. Така например Наполеон е вярвал, че „четири вестника могат да причинят повече вреда, отколкото стохилядна армия". Затова в армията му винаги е имало полева печатница с капацитет до 10 хиляди листовки на ден.

Словосъчетанието „психологическа война' е употребено за първи път през 1920 г. от английския историк Дж. Ф. К. Фулър, който „пророкува", че чистата психологическа война би могла с времето да замени традиционната война. Историята на военното изкуство показва, че психологическите операции могат да бъдат особено успешни за намаляване интензивността и продължителността на бойните действия, а при определени случаи да ги направят и ненужни. От друга страна, психологическите операции се възползват от психичния стрес, в който изпада противникът по време на бойните действия.

Примери за използване на похвати от това, което днес наричаме психологически операции, могат да бъдат открити във всички периоди на историята, но едва през Първата световна война, и то в самия й край, можем да видим пропагандата като квалифициран инструмент, основан на научен подход и включващ обективни техники. Професор Казанджиев посочва, че „през Балканската и Междусъюзническата война това условие (пропагандата), като че съвсем не съществуваше. Тепърва в световната война то се превърна в истинско оръжие, с което воюващите народи уязвяваха взаимно морала на войските си на фронта и смущаваха народите си в тила". Почти всички страни, участващи във войната, използват форми на психологически операции. Много страни,

4 История возникновения информационных войн и их трансформация в современных условиях, https://onkto.ru/blog/psychology/istoriya-informatsionnykh-vojn, стр. 1
5 Linebarger, P. M. (2015). Psychological warfare. Pickle Partners Publishing.

включително и България, създават военни формирования, специализирани в пропагандна дейност. Основна задача на тези формирования е разпространението на позиви чрез артилерия, балони и самолети.

През това време британците и германците започват да разпространяват пропаганда на вътрешния и западния фронт в началото на войната. Британците имат няколко предимства в допълнение към превъзходните оръжия, които им помагат да спечелят битката за отношението на целия свят: те контролират голяма част от подводната кабелна система по това време и имат най-престижната новинарска система в света. Те също така имат опит в международната и междукултурна комуникация.

За разлика от репутацията на германските дипломатически служби, британците имат дипломатическа служба, която поддържа силни връзки с много нации по света.

Дейвид Лойд Джордж назначава Чарлз Мастерман, член на парламента (МП), да оглави Агенция за пропаганда в Уелингтън Хаус през август 1914 г. Артър Конан Дойл, Форд Мадокс Форд, Г. К. Честъртън, Томас Харди, Ръдиард Киплинг и Х. Г. Уелс са сред литературните светила, наети за задачата. По време на войната са отпечатани над 1160 листовки, раздадени на неутрални страни и в крайна сметка на Германия. Доклад за предполагаемите германски безчинства от 1915 г., една от първите големи публикации, има огромно влияние върху общественото мнение по света. Брошурата описва подробно действителни зверства, извършени от германския Вермахт срещу белгийския народ[6].

През 1917 г. бюрото е погълнато от новия Департамент за информация и се разраства в телеграфни комуникации, радио, вестници, списания и филми[7]. Виконт Нортклиф става директор на Пропагандата във вражеските страни през 1918 г. Отделът е разделен между пропагандата на Х. Г. Уелс срещу Германия и Уикъм Стийд и пропагандата на Робърт Уилям Сетън на Уотсън срещу Австро-Унгарската империя; усилията на последния се съсредоточават върху липсата на етническото сближаване в Империята и подклаждат недоволствата на малцинства като хървати и словенци. Това има решаващо влияние върху окончателния срив на австро-унгарската армия в битката при Виторио Венето.

Над германските окопи са пуснати въздушни флаери от пощенски картички от военнопленници, очертаващи тяхното състрадателно състояние, известия за предаване и обща пропаганда срещу кайзера и германските генерали. До края на войната се разпръскват около 26 милиона листовки. Британците разработват безпилотни балони с листовки. Въпреки суровите наказания, поне една от всеки седем от тези брошури не е предадена от войниците на техните началници. Пленените твърдят, че са разочаровани от пропагандни листовки, изобразяващи германските сили като просто пушечно месо.

Британците започват да пускат по въздуха Le Courrier de l'Air, редовен вестник с листовки, за цивилни в окупираните от Германия Франция и Белгия през 1915 г. Френското правителство поема контрола над медиите в началото на войната, за да прикрие негативното отразяване. Те не започват да използват подобни стратегии за психологическа война до 1916 г., когато е създадена Maison de la Presse. Професор Тонелат и Жан-Жак Валц, елзаски художник с кодово име „Ханси", командват „Service de la Propagande aérienne" (Служба за въздушна пропаганда)[8]. Въпреки че пълната публикация на Четиринадесетте точки на президента Удроу Уилсън, която е значително редактирана в немските публикации, е предоставена чрез флаери във въздуха от французите, те са били склонни да разпространяват брошури само с изображения.

Според Джеймс Браун основните цели на психологическите (пропагандните) операции през

6 Ambrose, Stephen E. (1981). "Eisenhower, the Intelligence Community, and the D-Day Invasion". The Wisconsin Magazine of History. Vol. 64, no. 4. Wisconsin Historical Society. p. 269. ISSN 0043-6534.

7 Szunyogh, Béla (1955). Psychological warfare; an introduction to ideological propaganda and the techniques of psychological warfare. United States: William-Frederick Press. p. 13.

8 Rankin, Nicholas (1 October 2008). Churchill's Wizards: The British Genius for Deception, 1914–1945. Faber and Faber.

Първата световна война са[9]:

- да се мобилизира и насочи омраза срещу противника и да се подрине неговият боен дух;
- да се убеди собственото население в справедливостта на съюзническата кауза и да се повдигне и поддържа бойният дух;
- да се развива приятелство с неутралните държави и да се поддържа тяхната вяра, че съюзниците не само се борят за справедлива кауза, но и ще победят, ако получат тяхната активна подкрепа и сътрудничество;
- да се развива и заздравява приятелството със съюзните нации.

Влиянието на пропагандата през Първата световна война върху хода на бойните действия е предмет на многобройни изследвания. По това време радиото все още не се използва за масови комуникации. Използват се преди всичко бюлетини, позиви, вестници, постери, филми и публични речи. Изследователите са единодушни, че каквито и техники да са използвани и от двете страни, основната идея са „добрият съюзник" и „лошият враг" – черното и бялото. Това довежда не само до силна омраза към врага, но и до оневиняване на собствените брутални действия и до укрепване на духа и сплотеността на бойните единици.

Една от основните пропагандни теми на съюзниците са зверствата, жестокостите и варварщината на германците. Бомбардирането на катедралата в Лъовен (където може би е имало наблюдателни постове на съюзниците), нахлуването в неутрална Белгия (може би оправдано от тактическа гледна точка), потапянето на кораба „Луизитания" с 12 000 мъже, жени и деца на борда (даже и ако е превозвал оръжия за съюзниците) са сериозни грешки от психологическа гледна точка. Те се използват умело от съюзническата пропаганда и карат целия свят да гледа на германците като на варвари[10].

Адолф Хитлер е силно повлиян от британската тактика за психологическа война, използвана по време на Първата световна война, и той приписва поражението на Германия на ефекта от тази пропаганда върху войниците. През следващите десетилетия Хитлер е решен да използва масовата пропаганда, за да въздейства върху умовете на германския народ. Той успява да убеди много цивилни, че каузата му не е просто прищявка, а пътят към бъдещето, като нарича движението си Третият райх. Когато Хитлер идва на власт през 1933 г., Йозеф Гьобелс е избран за министър на пропагандата и той изобразява Хитлер като месианска фигура, която ще спаси Германия[11]. За допълнителен ефект Хитлер използва това с резониращите проекции на своите речи.

Всъщност не чувствителността на Германия към психологическите реакции на другите нации, включително неутралните, нанася по-големи вреди от тези, които са следствие на цялата съюзническа пропаганда. От друга страна, германската пропаганда като цяло е неефективна, защото офицерите, които я провеждат, не вярват в нейната значимост. Тя е в постоянна отбрана, изразходвайки по-голяма част от енергията си за опровергаване на вражеската пропаганда. С това германската пропаганда нарушава един от основните закони на пропагандата – посланието винаги трябва да бъде позитивно и никога негативно. В опитите си да коригират нечестната вражеска пропаганда, германците просто разпространяват оригиналните съюзнически послания, като по този начин те достигат и до тези, които не са чули за тях.

Хитлер в книгата си „Моята борба" също анализира пропагандната война по време на Първата световна война. Той пише: „Едва по време на Световната война стана напълно ясно какви огромни резултати може да даде правилно организираната пропаганда. Така например беше съвсем неправилно, че германската и австрийската пропаганда през цялото време се опитваха да представят противника в смешен образ в хумористичните листовки. Това беше неправилно, затова, защото при първата среща с реалния противник нашият войник получаваше съвършено друга

9 Карастоянов Георги, Психологически операции, ВИ София 2002 г., стр. 11
[10] Пак там, стр. 12
11 Ambrose, Stephen E. (1981). "Eisenhower, the Intelligence Community, and the D-Day Invasion". The Wisconsin Magazine of History. Vol. 64, no. 4. Wisconsin Historical Society. p. 269. ISSN 0043-6534.

представа за него от тази, която беше обрисувана в пресата. В резултат се нанасяше огромна вреда. Нашият войник се чувстваше излъган, престана да вярва и в останалия ни печат. Започна да му се струва, че печатът го мами за всичко. Разбира се, това по никакъв начин не можеше да укрепи волята за борба и да закали нашия войник. Напротив, войникът ни изпадаше в отчаяние. Военната пропаганда на англичаните и американците, напротив, беше от психологическа гледна точка напълно правилна. Англичаните и американците обрисуваха немците като варвари и хуни; с това подготвяха войника си за ужасите на войната... Пълното неразбиране на войнишката психология доведе дотам, че немската пропаганда се превърна в образец на това, което не трябва да се прави".

Психологическата война, предназначена както за чехословашкото население, така и за правителството, както и за чехословашките съюзници, е голям аспект от плана за нахлуване на Германия Fall Grün в Чехословакия. Той е толкова успешен, че Германия успява да превземе Чехословакия, без да се налага да води всеобхватна война, като понася само незначителни загуби в тайната война преди Мюнхенското споразумение[12].

Изпълнителното управление на политическата война е създадено от британците в началото на Втората световна война, за да генерира и разпространява пропаганда. С помощта на силни предаватели е могло да се правят излъчвания в цяла Европа. Сефтън Делмар организира успешна черна пропагандна кампания чрез редица радиостанции, предназначени да привлекат германските войници, както и да разпространяват новинарски материали, които накърняват морала им. Така британският премиер Уинстън Чърчил използва радиопрограми за разпространение на антигерманска пропаганда.

По време на Втората световна война британците широко използват измамата[13], създавайки множество нови техники и идеи в процеса. „A" Force, създаден през 1940 г. под командването на Дъдли Кларк, и Лондонската контролна секция (LCS), нает през 1942 г. под командването на Джон Беван, са основните протагонисти по това време. Много военни методи за измама са изобретени от Кларк. Неговите концепции за сливане на фалшиви бойни заповеди, визуална измама и двойни агенти помагат за дефинирането на съюзническата стратегия за измама през Втората световна война, спечелвайки му прозвището „най-големият британски измамник на Втората световна война"[14].

Много нови методи за психологическа война са разработени в навечерието на съюзническото нападение на Нормандия. Планът за операция „Бодигард" очертава обща стратегия за измама на германското висше командване относно действителната дата и местоположение на инвазията. Под надзора на Лондонската контролна секция (LCS), планирането започва през 1943 г. На конференцията в Техеран, известен като Плана Джаел, е представен на върховното командване на съюзниците. Операция Fortitude[15] е предназначена да убеди германците, че съюзниците са посилни от тях, използвайки фиктивни полеви армии, фалшиви операции за нахлуване и изтичане на информация относно бойния ред на съюзниците и подготовката за война.

В Ламанша са извършени сложни военноморски измами (операции *Glimmer, Taxable u Big Drum*). Малки кораби и самолети симулират нахлуващи флоти по бреговете на Пас де Кале, Кап д'Антифер и западния фланг на истинските нахлуващи сили.

За извършването на измамата са използвани двойни агенти, радиотрафик и визуална измама. До началото на войната британската антишпионска операция „*Double Cross*" постига голям успех и LCS успява да използва двойни агенти, за да получи фалшиви разузнавателни данни за намеренията на съюзническата инвазия. По време на Северноафриканската война фалшиви тан-

12 Rankin, Nicholas (1 October 2008). Churchill's Wizards: The British Genius for Deception, 1914–1945. Faber and Faber.
13 Adams, W. (2016, March 13). Anti-Venereal Disease Posters of World War 2. RelicRecord.
14 Ambrose, Stephen E. (1981). "Eisenhower, the Intelligence Community, and the D-Day Invasion". The Wisconsin Magazine of History. Vol. 64, no. 4. Wisconsin Historical Society. p. 269. ISSN 0043-6534.
15 Adams, W. (2016, March 13). Anti-Venereal Disease Posters of World War 2. RelicRecord.

кове и други военни активи като визуална измама са използвани[16].

Десантът в Нормандия е стратегически успех. В резултат на последвалата лъжа на Хитлер, подкрепленията от района на Кале са забавени за близо седем седмици.

Анализирайки от съвременна гледна точка целите на психологическите операции през Първата световна война, можем да посочим, че за всичките тези години до сега те не са се променили значително. От военна гледна точка при успешно планиране и провеждане на съвременните военни операции ролята на ПсО все повече нараства. Според схващанията на Китайската народноосвободителна армия ПсО са четвъртият вид бойни действия след сухоземни, морски и въздушни. Съвременните китайски военни теоретици перифразират Суан Дзъ, твърдейки, че е по-добре да атакуваш психиката на врага, отколкото неговите укрепени линии. Те определят основните задачи на ПсО така:

• да се повлияе на вражеските ръководители така, че те да се откажат от целите си и да изберат политика, която в крайна сметка не е изгодна за тях;

• да се внуши страх в умовете на вражеските военнослужещи, да се разруши техният психичен баланс и да се укрепи бойният дух на собствените войски;

• да се създава паника сред вражеското цивилно население чрез внушаване на страх и умора от войната и антивоенни настроения;

• да се спечелят симпатиите и подкрепата на неутрални държави и да се заздрави коалицията със съюзническите нации.

Като теоретично знание психологическите аспекти на убеждаването не са тайна за психолозите. Големият български психолог Спиридон Казанджиев, анализирайки пропагандата като „едно условие от извънредно голямо значение за психиката на бойците на фронта", посочва, че пропагандата „трябва да почива върху присъщи на човешката природа особености, като любопитство, сензация, слабост към слухове, потребност да се търсят в тежки моменти виновният, нуждата от авторитет, желание да се представим като добри и справедливи. От друга страна, пропагандата трябва да бъде съобразена с психологията на този, срещу когото се извършват с неговите културно ниво, народностно съзнание, обществена дисциплина, традиции в семейния и социалния живот, морал, религия и пр.

Най-сетне пропагандата трябва да се съобразява с конкретните условия, нужди и затруднения. Крайната цел, на пропагандата е да уязви морала на противника и преди всичко на войската му, за да разколебае неговите дух и дисциплина. За тази цел тя използва умело всички слабости и затруднения на противника, които правят внушенията и по-достоверни, и по-убедителни". С други думи, за да бъдат ефективни психологическите операции, трябва да се отчитат психологическите особености на целевата аудитория и основните психологически механизми, влияещи на поведението й.

По време на войната във Виетнам от САЩ се провежда мащабна кампания за психологическа война. Програма Феникс е предназначена да тероризира потенциални симпатизанти и пасивни поддръжници, както и да убива членове на Националния фронт за освобождение (NLF или Viet Cong) на Южен Виетнам. От друга страна, програмата Chiu Hoi на правителството на Южен Виетнам насърчава дезертиранията на NLF.

ЦРУ използва широко силите на Contra, за да дестабилизира сандинисткото правителство на Никарагуа. Излъчвайки незаконни телевизионни предавания, ЦРУ използва техники за психологическа война срещу панамците. Чрез TV Marti, разположено в Маями, Флорида, правителството на САЩ използва пропагандни предавания срещу кубинското правителство. Кубинското правителство, от друга страна, е ефективно в заглушаването на предаването на TV Marti.

САЩ разгръща кампанията за шок и страхопочитание във войната в Ирак, за да осакати психологически и да подкопае волята на иракската армия.

16 Ambrose, Stephen E. (1981). "Eisenhower, the Intelligence Community, and the D-Day Invasion". The Wisconsin Magazine of History. Vol. 64, no. 4. Wisconsin Historical Society. p. 269. ISSN 0043-6534.

Социалните медии направиха възможно разпространението на лъжи в голям мащаб в киберпространството. Анализатори откриват доказателства за подправени или измамни снимки, разпространявани от социалните медии по време на Гражданската война в Сирия и руската военна интервенция в Украйна през 2014 г. и 2022 г., вероятно с участието на държавата, според анализатори. Военни и правителствени служители са използвали психологически операции (PSYOPS) и информационна война в платформите на социалните медии, за да контролират чуждата пропаганда от страни като САЩ, Русия и Китай.

„Най-добре е собствената армия, батальон, рота или петчленен отряд да се поддържат непокътнати; да разбиеш вражеската армия, батальон, рота или отряд от пет души е просто второто най-добро", според известният китайски военен стратег Сун-Дзъ. Така че спечелването на сто битки не е върхът на съвършенството; върхът на съвършенството е покоряването на вражеската армия, без изобщо да се бие"[17]. Тези думи на един от най-блестящите военни стратези в историята и са актуални и днес.

В днешната военни действия все още е важно да се запазят човешките сили непокътнати, доколкото е възможно. Психологическата война и операции са изиграли основна роля в залавянето на вражески пленници и спечелването на сърцата и умовете, както на вражеските цивилни, така и на бойците през 20 век и в съвременни конфликти като Втората световна война, Корейския конфликт, Виетнамската война, Персийския залив, операция „Непреклонна свобода", операция „Свобода на Ирак" и различни мироопазващи мисии по света.

Понятието ПсО е с по-широко съдържание от психологическа война, защото включва и действия, които могат да бъдат насочени и към приятелски и неутрални аудитории, докато психологическата война е насочена само към враждебна целева аудитория. По същество дейностите, включени в понятието психологически операции, не са форма на сила, но са мултипликатор на силата, който използва ненасилствени средства много често в среда, пълна с насилие. Разчитайки на убеждението, вместо на физическото принуждение, психологическите операции използват логиката, страха, желанията и други психични фактори, за да предизвикат определени емоции, нагласи или поведение.

Някои психологически операции са добре известни, като например PSYOP, която принуди генерал Мануел Нориега да се предаде, като се пуска рок музика по високоговорителите. Ето защо думите на Сун-Дзъ от преди две хиляди години са валидни и днес: „Крайната победа е поражението на вражеската армия без битка"[18].

През последните десетилетия наред с ПсО в медийното пространство често се използват и понятия като „информационна кампания", „информационна война", „информационни операции" за разрешаване на военнополитическата криза с невоенни средства. Съгласно схващанията на западните армии информационните операции включват:

– борбата за превъзходство в управлението и контрола;

– операции по гражданско-военните отношения ;

– връзките с обществеността.

Борбата за превъзходство в управлението и контрола от своя страна включва:

- *Оперативна сигурност;*
- *Радиоелектронна борба;*
- *Въвеждане на противника в заблуждение;*
- *Физическо разрушаване на обекти и унищожаване на хора, т. е. огнево поразяване;*
- *Психологически операции.*

Една от най-съдържателните дефиниции е дадена в полевото ръководство „Психологически операции" на сухопътните войски на американската армия – ***планирана употреба на медии и действия за разпространяване на подбрана информация и индикатори сред чуждестранна***

17 Griffith, S. B. (1963). Sun Tzu: The art of war (Vol. 39). London: Oxford University Press.
18 Пак там

аудитория, която влияе на емоциите, мотивите и в крайна сметка на поведението на чуждестранни правителства, организации, групи хора и личности. Целта на психологическите операции е да предизвика нагласи и поведение, благоприятни за замисъла на планираните операции. Някои автори дори разглеждат термина убеждаващи комуникации като равнозначен на психологически операции. Въпреки че терминът психологически операции е сравнително нов, психическите въздействия са стари колкото и човешките конфликти.

ИЗВОДИ:

1. Психологически операции вероятно са се провеждали още в дълбока древност и са включвали общуване „лице в лице", при което един човек се е опитвал чрез жестове, думи, викове или действия (или в комбинация от тях) да повлияе на друг човек. От векове наред психологическите операции са предпочитаната стратегия при воденето на войни, чиято ролята все повече нараства при успешно планиране и провеждане на съвременните военни операции.

2. Като едно от най-мощните „оръжия" за постигане на поставени военни и политически цели във века на информационните технологии може да определим „психологическите операции", благодарение на които чрез манипулиране на противника се създава възможност за лесна победа без водене на военни действия.

3. „Психологическите операции" са планирани операции за поднасяне на селектирана информация към чуждестранна аудитория с цел влияние върху нея, като се използват различни ненасилствени методи (внушаване на страх, създаване на паника, масови психози, спечелване на симпатии и други методи за разрушаване на психичния баланс). Отчитайки психологическите особености на целевата аудитория (културно ниво, народностно съзнание, обществена дисциплина, традиции в семейния и социалния живот, морал, религия и пр.) и основните психологически механизми, влияещи на поведението й, като резултат от убеждението (използвайки логиката, страха, желанията и други психични фактори), вместо на физическото принуждение, психологическите операции предизвикат определени емоции, нагласи или поведение върху чуждите правителства, организации, групи и индивиди.

References

1. Шейнов В. П., Манипулирование сознанием, Минск: Харвест, 2010 г.
2. Митрев Димитър, „Информационни и психологически операции", УИ „Епископ Константин Преславски", Шумен, 2006 г.
3. Карастоянов Георги, Психологически операции, ВИ, София, 2002 г.
4. Петров Велико, учебник Стратегически комуникации, Издателство на НВУ „В. Левски", Велико Търново, 2021 г., с. 337, ISBN 978-619-7531-20-6
5. JP 3-53, Doctrine for Joint Psychological Operations
6. Почепцов Г., Психологические войны, „Рефлбук" „Ваклер", 2000 г.
7. История возникновения информационных войн и их трансформация в современных условиях, https://onkto.ru/blog/psychology/istoriya-informatsionnykh-vojn
8. Лукин Е. В., Психологические основы информационной войны, центр стратегических оценок и прогнозов, http://csef.ru/ru/oborona-i-bezopasnost/265/psihologicheskie-osnovy-informaczionnoj-vojny-3725
9. Суан Дзъ,(2005) "Изкуството на войната":Древни китайски трактати,Труд.
10. Linebarger, P. M. (2015). Psychological warfare. Pickle Partners Publishing.
11. Ambrose, Stephen E. (1981). "Eisenhower, the Intelligence Community, and the D-Day Invasion". The Wisconsin Magazine of History. Vol. 64, no. 4. Wisconsin Historical Society. p. 269. ISSN 0043-6534.

12. Szunyogh, Béla (1955). Psychological warfare; an introduction to ideological propaganda and the techniques of psychological warfare. United States: William-Frederick Press. p. 13.
13. Rankin, Nicholas (1 October 2008). Churchill's Wizards: The British Genius for Deception, 1914–1945. Faber and Faber.
14. Adams, W. (2016, March 13). Anti-Venereal Disease Posters of World War 2. RelicRecord.
15. Griffith, S. B. (1963). Sun Tzu: The art of war (Vol. 39). London: Oxford University Press

HISTORY AND REASONS FOR THE EMERGENCE OF THE PUBLIC DIPLOMACY

Veliko P. Petrov, Stancho G. Stanchev

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

Abstract*: The report aims to acquaint readers with the history and reasons for the emergence of public diplomacy. At the beginning, the historical development of diplomacy is traced. Diplomacy has an extremely long history. Beginnings of diplomacy can be seen even in the clan-communal system, when forms of negotiation are present. However, one can speak of the actual formation of diplomacy as a public institution only after the emergence of states.*

The emergence and development of public diplomacy is traced. The main difference between traditional diplomacy and public diplomacy is that traditional diplomacy is focused on the relationships between representatives of states and other international actors, while public diplomacy is aimed at the general public in foreign societies and more specific informal groups, organizations and individuals. The notion of public diplomacy is becoming a guiding understanding not only of American theory and practice, but also instructive of the foreign policy practices of other countries and international organizations around the world.

Public diplomacy has been formed due to certain factors, such as: globalization, advances in communication technology, and the increasing influence and participation of societies in the international affairs of states. Public diplomacy has its essential place for realizing the foreign policy priorities of individual countries both in their bilateral contacts and in the multilateral diplomatic communication that prevails in modern international relations. Public diplomacy is understood as a set of activities aimed at influencing a foreign audience, as well as its public opinion within the framework of its own state interests.

Public diplomacy is a government's process of communicating with foreign societies to achieve a better understanding of its national ideas and ideals, its institutions and culture, as well as its national goals, interests, and current policies. Public diplomacy is concerned with influencing public attitudes and seeks to represent the interests of a country through understanding, informing and influencing. This means clearly explaining the objectives, policies and activities of that country, promoting the understanding of these objectives through dialogue with citizens, communities, institutions and the media.

Key words: *public diplomacy, diplomacy*

ИСТОРИЯ И ПРИЧИНИ ЗА ПОЯВАТА НА ПУБЛИЧНАТА ДИПЛОМАЦИЯ

Велико П. Петров, Станчо Г. Станчев

Преди да се разгледа понятието „публична дипломация“ е необходимо да се дефинира самата дипломация като цяло. Има голям брой различни интерпретации на феномена „дипломация“. Някои от тях са дадени, например, в такива известни произведения като „Дипломация” на Г. Никълсън, в „Ръководство за дипломатическата практика” на Е. Сатоу и др. Много от тях се основават на тясната връзка на процеса на преговори с дипломацията. И така, Г. Никълсън, въз основа

на определението, дадено в Оксфордския речник, дава своето тълкуване на дипломацията „провеждането на международни отношения чрез преговори; методът, чрез който тези отношения управлявани и администрирани от посланици и пратеници; работата или изкуството на дипломат". Това определение впоследствие става основа за много изследователи в областта на дипломацията и теорията на преговорите. Би било погрешно да се свежда дипломацията само до водене на преговори. В такава ситуация извън сферата на дипломацията би било по-голямата част от консулската работа, както и например консултациите (те не включват приемане на съвместно решение, което е целта на преговорите) и редица други дейности. В резултат на което днес все по-често се използват по-широки дефиниции за дипломацията, в които преговорите играят преобладаваща роля.

Доста подробно определение е използвано в книгата на Дж. Беридж, английски изследовател, който разкрива дипломацията по следния начин: „дипломацията е провеждането на международни дела по-скоро чрез преговори, както и чрез други мирни средства (като събиране на информация, проявата на добра воля), включваща пряко или косвено преговори, отколкото чрез използване на сила, използване на пропаганда или прибягване до законодателство".

Съществуват много определения за дипломация, но ще посочим определението, дадено от В. Попов, че „*дипломацията е дейност по осъществяване на целите и задачите на външната политика на страната и по защита на правата и свободите на гражданите извън територията на страната с мирни средства чрез изграждане на доверие*". Външната политика и международните отношения на страната се реализират от органите на държавно управление, които биват подпомагани от професионални дипломати. В теорията се приема, че дипломацията е най-значимото мирно средство, което държавите използват, тъй като останалите (културни, икономически, религиозни, военни и др. средства) имат спомагателна, допълваща роля.

Дипломацията има изключително дълга история. Зачатъци на дипломация може да се видят още в родовообщинния строй, когато са налице форми на преговори. За същинско формиране на дипломацията като обществена институция обаче може да се говори само след появата на държавите.

С възникването на държавите дипломатическото изкуство приема по-съвършени форми. Например, Египет преди 3,5 хиляди години е подписал споразумение със съседната хетска държава за взаимно осигуряване на военна помощ срещу вътрешния враг. Някои от най-ранните записи са дипломатическите писма, писани между фараоните на осемнадесетата династия на Египет и владетелите на Ханаан по време на 14 век пр.н.е. Дипломатически дейности могат да се открият в периода на съществуване на древногръцките градове-държави (полиси). Там могат да се срещнат и посолства и преговори и дори международни конференции.

Гръцките градове-държави често изпращат посланици, които да преговарят за специфични проблеми, като война и мир или търговски връзки, но няма дипломатически представители, които да представят една страна на територията на друга. Въпреки това, някои от функциите на съвременните дипломатически представители са създадени именно в Древна Гърция. В Древния Рим, външнополитическите дела са ръководени от Сената, а след централизирането на държавната власт, ръководството се упражнява от императора.

В античните времена, и в Изтока, и в Гърция и в Рим, са използвани дипломатически средства като сключване на междудържавни договори, сключване на съюзи, обмен на дипломатически преписки.

Институцията посланик също възниква в дълбоката древност. В периода на съществуването на древногръцките градове-държави, конфликтите често се решават още преди да избухнат, с помощта на „посланици" – старейшини или вестоносци. Посланиците са избирани сред най-уважаваните граждани. Те съставят свое „посолство", членовете на което са равноправни. По-късно възниква обичая да бъде избиран ръководител – глава на мисията на посланика и която е първообраз на сегашните акредитиращи писма. От гръцката дума „диплома" произхожда днешната дума „дипломация".

Древна Индия, с нейните царства и династии, има дълга традиция в дипломацията. Древноиндийският политически и икономически трактат „Артхашастра" се приписва на Чанакя, който е главният съветник на Чандрагупта Мауря, основател на династията Мауря, управлявала през 3 век пр.н.е. „Артхашастра" е изцяло произведение на изкуството на царството. В него се използва теорията на дипломацията, както при ситуация на взаимно оспорване на царства, така и за създаване на съюзи от царя.

Произходът на раната модерна дипломация често се търси в страните от Северна Италия от Ранния Ренесанс, със създаването на първите посолства през 13-ти век. Милано играе водеща роля с установяването на постоянни посолства в други градове-държави в Северна Италия. Тоскана и Венеция също са центрове, в които дипломацията процъфтява от 14-ти век. Много от съвременните дипломатически практики започват точно на Апенинския полуостров, каквато например е предоставянето на акредитиви на посланиците до владетеля.

Посланиците и благородниците с малко опит в чужбина имат нужда да бъдат подпомагани от служители в посолството. Такива служители са изпращани на дългосрочни задачи и имат повече познания за страната-домакин. Персоналът на една средновековно посолство включва служители от всякакви професии, включително и някои, които са посветени на шпионаж. Същевременно в почти всички европейски държави са основани министерства, които да координират работата на посолствата и нивото на кадрите. Формата на тези външни министерства е далече от съвременната им форма, и много от тях имат и други вътрешни функции. Във Великобритания например има две министерства, чиято работа често се припокрива до 1872 г. Франция, която през осемдесетте години на 18 век има най-голямото външно министерство, тогава има само 70 постоянни служители.

Елементите на съвременната дипломация бавно се разширяват към Източна Европа и Русия. Цялата средновековна подредба на международните отношения е прекъсната от Френската революция и последващите години на войни. След революцията, дори и обикновени хора, издигнати от революционните армии, започват да поемат контрола върху дипломацията на френската държава. Премахнати са ранговете. Наполеон отказва да признае дипломатическия имунитет на няколко британски дипломати, обвинени в извършване на интриги срещу Франция.

Дипломатическите връзки получават своя разцвет през 18 и 19 век. На Виенския конгрес през 1815 г. представители на много европейски държави се договарят за дейността на дипломатическите представителства и старшинството на техните ръководители.

Понастоящем е в сила международен документ, който по-подробно и с отчитане на дипломатическата практика определя дипломатическите отношения. Документът е подписан през 1961 г. във Виена и се нарича *Виенска конвенция за дипломатическите отношения*.

Както и с почти всичко друго случващо се в човешката история, така и в случая с *публичната дипломация*, преди тя да се концептуализира и институционализира като самостоятелен клон на дипломацията, тя вече се е практикувала някъде без да се съзнава сегашния и статус, име и значение. Това може да се открие в историята на европейските политически, търговски и религиозни практики. Може да го срещнем като целенасочени действия по отношение на чуждестранна публика на античните градове-държави, особено на Атина в преследване на своите политически, икономически и военни интереси или на републиканския, а впоследствие и имперски Рим, при налагането на своята сила и изключителност сред обществата, обитаващи земите на неговото влияние.

Откриваме много изкусни и ефективни практики на християнските църкви и владетели по време на европейското Средновековие. Мисията на Светите братя Кирил и Методий в Моравия е брилянтна и тя е осъществила грандиозния проект на Византия за християнизиране и просвещаване на населението, включително чрез изобретяване на нова азбука. Известна е кампанията на Светия Престол, особено при Папа Григорий XV, който лично е инструктирал католическите свещеници, изпращани да служат в чуждестранни общества по целия свят, как да свеждат, разпространяват, осветляват и разясняват Светото писание. Не по-малко ефективни са били и методите на протестантските църкви за спечелване на сърцата на хората в полза на Христовата вяра в

Латинска Америка и Далечния Изток.

Голям е приноса на ренесансовите градове-републики – Венеция, Флоренция, Генуа и Милано – за работата им с поданиците на чужди владетели и при популяризиране на своите постижения в различни сфери (финанси, култура, политика и др.).

След изобретяването на печатницата от Гутенберг в XV век, венецианците дори са въвели систематично и регулярно разпространяване на брошури чрез своите дипломатически представителства сред чуждестранните публики. Да се въздейства върху многобройна чужда публика, без употреба на военна сила, с цел да се разпространи и защити кауза, интерес, вяра, образ, иновация или предимство, са практики, видими в цялата европейска история. Независимо дали са се провеждали интуитивно, или напълно премислено, навсякъде тези практики са били съпровождани от разбирането за полза и благо на тези, които са ги упражнявали.

Може би най-организираната и премислена публична политика в чужди страни, и с най-голямо разбиране за ползата от нея за държавния интерес, срещаме в европейската история при кардинал Ришельо, първи министър на френския крал Луи XIII. С постоянство, чрез убеждаване и инвестиране, Ришельо се наема да създаде националната идентичност на французите и да увековечи френската държавност[1].

С настъпването на информационната епоха традиционната дипломация е заменена от публичната, или, както още я наричат „публична дипломация". Първите опити да се даде научна дефиниция на понятието „публична дипломация" датират от края на 19 и началото на 20 век. Самият термин „публична дипломация" като синоним на думата „учтивост" е използван за първи път през 1856 г. в статия, публикувана във вестник „Таймс" за дейността на президента на САЩ Франклин Пиърс. През 1871 г. американският конгресмен Самуел Кокс използва термина за означаване на открита, честна дипломация. По това време целта на публичната дипломация е да впечатли чуждите граждани.

По време на Първата световна война „публична дипломация" означава нови методи на външна политика, по-популярният термин е „отворена дипломация", който определя публичния характер на международните отношения. Като цяло до края на Втората световна война терминът „публична дипломация" се използва в значенията на „гласност", „обществено сътрудничество" и „безпристрастност"[2].

Терминът „публична дипломация" (public diplomacy) е бил използван за първи път през 1965 година като означение на самостоятелна дисциплина от Едмънд Гълиан (Edmund Gullion), декан на Fletcher School of Law and Diplomacy при Tufts University. Когато впоследствие се е създавал Murrow Center of Public Diplomacy към същия университет, именно понятието на Едмънд Гълиан за публична дипломация е било положено като водещо. А то е включвало следното разбиране: *Публичната дипломация се занимава с влиянието на обществените нагласи върху формирането и осъществяването на външните политики на държавите*.

Първата научна дефиниция на термина „публична дипломация" е предложена от декана на Fletcher School of Law and Diplomacy към Tufts University, Едмънд Гълиан (Edmund Gullion): „публичната дипломация ... се занимава с влиянието на връзките с обществеността върху формирането и прилагането на външнополитическа дейност. Тази дейност обхваща тези аспекти на международните отношения, които са извън обхвата на традиционната дипломация: формирането от правителството на една страна на обществено мнение в друга страна; взаимодействието на частни групи и техните интереси в една страна със същите в друга; официални доклади за международните отношения и тяхното влияние върху политиката; комуникация между комуникиращите, както между дипломати и чуждестранни кореспонденти; процесът на междукултурна комуникация... Ос-

[1] Антъни Леви – Кардинал Ришельо, С. 2007;

2 Смирнов Никита, Публичная дипломатия: эволюция концепта в политической науке, 2015, https://cyberleninka.ru/article/n/publichnaya-diplomatiya-evolyutsiya-kontsepta-v-politicheskoy-nauke, стр. 79

новното в публичната дипломация е транснационалният поток от идеи и информация"[3].

Публичната дипломация започва да се изучава активно от други изследователи от онова време. През 1968 г. американският учен А. Хофман в книгата си „Международни комуникации и новата дипломация" твърди, че „революцията в средствата за масова комуникация породи нова дипломация, чиито методи все още не са напълно проучени"[4].

В следващите дефиниции на термина се поставя акцент върху постигане на определено влияние, като краен резултат от процеса на комуникация, върху „мнението на широката публика или на елита в друга държава с цел преориентирането на външната ѝ политика в нейна полза"[5]. В този смисъл комуникацията не е самоцел, а се води с ясно начертани цели и съответно с ясна стратегия за тяхното постигане.

На етапа на формиране на публичната дипломация (70-те и 80-те години на XX век) много учени изследваха въпроса как активно развиващите се области на кинематографията, медиите, музиката могат да бъдат използвани за влияние върху населението на чужди страни. Такова влияние се постига чрез „използване на политическа и икономическа власт за пропагандиране и популяризиране на ценностите и обичаите на чужда култура за сметка на местната култура"[6].

Американският политолог Джоузеф Най класифицира политиката на „меката сила" като публична дипломация. Разбирането за ролята на влиянието в процеса на постигане на желаните резултати при воденето на външна политика е залегнало в често използвания термин „*мека сила*", но също и власт (*soft power*), въведен от Джоузеф Най в началото на 21-ви век. През последното десетилетие този термин придоби голяма популярност и значение преди всичко заради стремежа да се намери противовес на идеята, че за постигане на външнополитически цели и упражняване на влияние на международната сцена са необходими военна и икономическа мощ. Джоузеф Най дефинира „меката сила" като „*способността да постигнете това, което искате, чрез привличане и убеждаване на другите да приемат вашите цели*"[7].

Основните характеристики на меката сила на дадена държава са нейните идеи, ценности, култура и институции, а публичната дипломация е прийомът за нейното приложение и разгръщане. Към нейния инструментариум принадлежат механизмите, които спомагат в процеса на привличане, определяне на дневния ред на международната общност или превръщането на дадена идея в повествование или визуален образ, който да резонира с общочовешките ценности. Така меката сила, упражнена чрез способите на публичната дипломация, се явява източник на легитимност и правдоподобност. Това са важни характеристика за поддържане на репутацията на всяка една държава, което от своя страна определя нейната способност да упражнява влияние на международната сцена, независимо от степента на нейната военна и икономическа сила. Именно този аспект на публичната дипломация ѝ придава огромно значение при воденето на външна политика.

Джоузеф Най пояснява, че страните имат по-голяма вероятност да постигнат влияние в ерата на информациите технологии, ако използват множество канали за комуникация, чрез които да оформят дебата по дадени въпроси; чиято култура и идеи са близки до преобладаващите глобални норми (а именно либерализъм, плурализъм и автономност); и чиято правдоподобност се подсилва от националните и международни ценности и политики[8].

Следователно, комуникация и влияние при воденето на публична дипломация са взаимно свързани. Комуникацията е съществена и за традиционната дипломация. Съществена разлика

3 What is Public Diplomacy? // United States Information Agency Alumni Association. Updated September 1, 2002. URL: http://pdaa.publicdiplomacy.org/?page_id=6

4 2 International Communication and the New Diplomacy / Ed. A.S. Hoffman. Bloomington: Indiana University Press, 1968.

5 Jarol B. Manheim, Strategic Public Diplomacy and American Foreign Policy: The Evolution of Influence", Oxford University Press, New York and Oxford, 1994

6 The Harper Dictionary of Modern Thought / eds. A. Bullock, O. Stallybrass. New York : Harper & Row, 1977

7 Joseph S. Nye Jr., Soft Power: The Means to Success in World Politics, New York: Public Affairs, 2004

8 Здравко Попов и авторски колектив, учебно пособие Публична дипломация и комуникационна политика в контекста на Европейския съюз, Дипломатически институт, София 2017 г., стр. 33.

обаче е, че при дипломацията отношенията между правителствата и техните представители са регулирани в рамките на широко приети международни правила и норми, установени с течение на времето. Комуникационните парадигми при публичната дипломация от своя страна са контекстуални и зависят от изпълнителя. Комуникацията в рамките на дипломацията се основава на принципа на реципрочността, докато публичната дипломация изисква от националните дипломатически представители да могат да работят и да действат в аморфни транснационални мрежи.

Освен това публичната дипломация позволява прилагането на широк спектър от механизми, техники и комуникационни методи, а техният успех или провал зависи от това дали е постигнато търсеното „привличане" и „убеждаване" в зависимост от нагласите и настройката на съответната аудитория, към която те са насочени. Резултатите от усилията в областта на публичната дипломация не могат да бъдат измерени лесно, а и не могат да бъдат съпоставени спрямо някакъв неоспорим бърз успех. Положителните последици са по-скоро създаването или трансформацията на дадени обществени нагласи в един по-дълъг период от време.

Публичната дипломация се изучава и анализира през призмата на две перспективи – *масова комуникация* и *създаване на мрежи от контакти и взаимоотношения*[9]. Парадигмата на масовата комуникация включва създаването и разпространението на информация с идеята тя да достигне до широката общественост посредством СМИ. В тази сфера публичната дипломация се позовава на опита в областта на журналистиката, комуникациите, както и на социалните науки по отношение на изследването на обществените нагласи и използването на СМИ. Силата и потенциалът на публичната дипломация обаче могат да бъдат най-добре обяснени през призмата на създаването на мрежи от контакти и взаимоотношения. Ако при масовата комуникация основният метод е монологът, то вторият подход е базиран на способността за водене на диалог и обмен на мнения и идеи, а не просто разпространяване на информация. Това обяснява необходимостта от създаване на взаимоотношения и сътрудничество, както и обединяване на мнения и усилия около конкретни въпроси или каузи.

ИЗВОДИ:

1. Основната разлика между традиционната дипломация и публичната дипломация е, че традиционната дипломация е фокусирана върху взаимоотношенията, осъществявани между представители на държави и други международни актьори, докато публичната дипломация е насочена към широката общественост в чуждестранни общества и по-специфични неформални групи, организации и индивиди.

2. Понятието за публична дипломация се превръща във водещо разбиране не само за американската теория и практика, но става инструктивно и за външнополитическите практики на други държави и за международните организации в света. Публичната дипломация се е формирала поради определени фактори, като: *глобализацията, напредъкът в областта на комуникационните технологии и нарастващото влияние и участие на обществата в международните дела на държавите*.

3. Публичната дипломация има своето съществено място за реализиране на външнополитическите приоритети на отделните държави както в двустранните им контакти, така и в многостранното дипломатическо общуване, което преобладава в съвременните международни отношения. Публичната дипломация се разбира като набор от дейности, насочени към въздействие върху чужда публика, както и върху нейното обществено мнение в рамките на собствените й държавни интереси.

4. Публичната дипломация е правителствен процес на комуникация с чуждестранните общества за постигане на едно по-добро разбиране на неговите национални идеи и идеали, на неговите институции и култура, както и на неговите национални цели, интереси и актуални политики.

9 R. S. Zaharna, The Soft Power Differential: Network Communication and Mass Communication in Public Diplomacy, The Hague Journal of Diplomacy, 2 (2007), pp. 213-228

Публичната дипломация се занимава с влиянието на публичните нагласи и се стреми да представи интересите на дадена страна чрез разбиране, информиране и въздействие. Това означава ясно обяснение на целите, политиките и дейностите на тази страна, благоприятствайки разбирането на тези цели чрез диалог с гражданите, общностите, институциите и медиите.

References

1. Попов Здравко и авторски колектив, учебно помагало Публична дипломация, Издателска къща „Св. Георги Победоносец“ ЕООД 2021 г, ISBN 978-619-7200-21-8

2. Петров Велико, учебник Стратегически комуникации, Издателство на НВУ „В. Левски“, Велико Търново, 2021 г., с. 337, ISBN 978-619-7531-20-6

3. Попов Здравко и авторски колектив, учебно пособие Публична дипломация и комуникационна политика в контекста на Европейския съюз, Дипломатически институт, София, 2017.

4. Мельникова Мария, Выпускная квалификационная работа „Публичная дипломатия как инструмент внешней политики в современных международных отношениях“, Екатеринбург 2018.

5. Антюхова Е. А. и авторский коллектив, Публичная дипломатия: Теория и практика: Научное издание / Под ред. М. М. Лебедевой, М.: Издательство „Аспект Пресс“, 2017 г, 272 с, ISBN 978–5–7567–0931–5

6. Леви Антъни – Кардинал Ришельо, С. 2007;

7. Смирнов Никита, Публичная дипломатия: эволюция концепта в политической науке, 2015, https://cyberleninka.ru/article/n/publichnaya-diplomatiya-evolyutsiya-kontsepta-v-politicheskoy-nauke

8. What is Public Diplomacy? // United States Information Agency Alumni Association. Updated September 1, 2002, http://pdaa.publicdiplomacy.org/?page_id=6

9. International Communication and the New Diplomacy / Ed. A.S. Hoffman. Bloomington: Indiana University Press, 1968.

10. Jarol B. Manheim, Strategic Public Diplomacy and American Foreign Policy: The Evolution of Influence”, Oxford University Press, New York and Oxford, 1994

11. The Harper Dictionary of Modern Thought / eds. A. Bullock, O. Stallybrass. New York : Harper & Row, 1977

12. Joseph S. Nye Jr., Soft Power: The Means to Success in World Politics, New York: Public Affairs, 2004

13. R. S. Zaharna, The Soft Power Differential: Network Communication and Mass Communication in Public Diplomacy, The Hague Journal of Diplomacy, 2 (2007), pp. 213-228

FOOD CRISES IN THE WORLD

Veliko P. Petrov, Kaloyan A. Iliev

Faculty of Artillery, Air Defense and Communication and Information Systems, National Military University, Shumen, Bulgaria, veliko_pp@abv.bg, kacho_78@abv.bg

Abstract*: Food crisis in the world from 2020 has been increased for us. Establish factors for food and storage of non-significant and under-protected food as a result of conflicts, economic disruptions and extreme meteorological phenomena or a combination of these factors. The war in the Ukraine dealt a blow to the food supply for millions of chorus. The consequences of the Tazi war will jump across the border to Ukraine and will see you in the holy land: all the country's zasegnati from swaying to value agricultural products, but the effect is very strong from the population to some developing countries, which veche se amirat in a significant state food nesigurnost and nedokhranvane. In the world plan, approximately 811 million souls are suffering from hunger, and in the regions for 2021, 193 million souls are dying in the situation of a food crisis in 53 countries or territories. Two billion people live in Asia, 799 million in Africa, 205 million in Latin America and the Caribbean, 88 million in North America and Europe and 5 .9 million in Oceania. It is also necessary to strengthen Sveta's network for combating food crises in work and for coping with it through multi-country and multi-sector interventions, citizens for sustainability and knowledge and for the interplay between humanitarian action, development and the world.*

Keywords: *food crisis, food sigurnost*

ПРОДОВОЛСТВЕНИТЕ КРИЗИ В СВЕТА

Велико П. Петров, Калоян А. Илиев

Сред глобалните проблеми на човешкото развитие повечето учени, експерти и анализатори изтъкват продоволствения проблем, който е актуален през целия минал век и началото на XXI век. Съвременният продоволствен проблем в развитието на човечеството е, че поради нерационалното и твърде интензивно използване на природните ресурси, повишеното търсене на животински продукти, увеличеното потребление на храна на глава от населението, както и други фактори, има постоянно нарастване на цените на храните, което допринася за появата на заплахи за продоволствената сигурност в развиващите се страни, включително за най-бедните групи от населението в развитите страни.

В момента в целия свят се наблюдава засилено обществено възприемане на проблемите като бедността и недохранването. Глобалната продоволствена криза провокира рязко покачване на цените на храните, последицата от което е намаляване на реалните доходи на домакинствата, задържайки процеса на преодоляване на бедността и глада в много страни по света. По този начин храната постоянно действа като необходима и безспорна част от средствата за съществуване, а увеличаването, поради една или друга причина, на нейния дефицит с право се възприема като бедствие, което изисква ефективни политически и икономически решения за преодоляването му.

Сериозността и мащабът на продоволствените кризи са се увеличили от 2020 г. насам в резултат на конфликти, икономически сътресения и екстремни метеорологични явления или комбинация от тези фактори, като през 2021 г. близо 193 милиона души са страдали от остра продоволствена несигурност и са се нуждаели от спешна продоволствена помощ – най-големият брой хора в света, страдащи от остра продоволствена несигурност, регистриран в глобалния доклад относно продоволствените кризи в рамките на шестгодишното му съществуване; като има предвид, че между 720 и 811 милиона души гладуват и се счита, че пет държави са изложени на риск от масов глад, включително Южен Судан, Етиопия, Мадагаскар, Нигерия (16 щата и територията на федералната столица) и Йемен[55].

Световният продоволствен проблем е икономически факт, който може да доведе до значителни политически последици. Много експерти смятат, че в основата на световните революции и катастрофи е скокът в цените на храните. Например в Близкия изток и Африка бедните хора харчат около 50 % от доходите си за храна, което означава, че нарастващите цени на основните храни гарантират невероятно голямо въздействие върху разходите на домакинствата. Недостигът на храни се превръща във все по-голяма грижа за милиони хора, по-специално в Африка и Азия и особено в държавите, които са вече засегнати от глад.

Според Организацията на ООН за прехрана и земеделие (ФАО) се очаква търсенето на храни в световен мащаб да се увеличи със 70 % до 2050 г. Световното население от 7 милиарда днес ще достигне 8,5 милиарда през 2030 г и повече от 10 милиарда до 2050 година. Световното производство на храни ще трябва да се увеличи на фона на протичащите глобални промени в климата, на намаляващите природни ресурси, като биоразнообразието, водните ресурси, работната ръка и състоянието и площта на обработваемата земя. Това означава, че светът ще трябва да произвежда повече храна, като същевременно използва по-малко вода, по-малко земя, по-малко енергия, по-малко торове и по-малко пестициди.

По своята същност *кризата* представлява заплаха за жизнено важните интереси на държавата, като може да има национален и международен обхват. В Република България, понятието „криза" се разглежда в Доктрината на въоръжените сили като „*нестабилност в политическата и обществената сфера, предизвикваща рязка промяна на установеното състояние на икономиката и обществения живот*"[56]. Следователно, кризата представлява рязка промяна в установения ред на съществуване сред дадено общество, като тази промяна се характеризира с налична заплаха за човешкия живот и благоденствие, голямо страдание и липса на сигурност.

На глобално и регионално ниво основните заплахи за сигурността на храните се отнасят по-специално към два фактора. Макроикономически сътресения, предавани чрез капиталови потоци или стокови потоци, влияят на достъпа до храна чрез тяхното въздействие върху доходите и богатството на домакинствата и – заедно с глобалните промени в климата, могат да намалят наличието на храна чрез промени в производствените стимули и увеличаване на колебанията в регионален план[57].

Войната на Русия в Украйна води до рекордно високи цени на храните и предизвиква световна продоволствена криза. От средата на 2020 г., на фона на възстановяването от

[55] Глобален доклад относно продоволствените кризи за 2021 г., актуализация от септември.

[56] Доктрина на въоръжените сили на Република България, Издание (А), ноември 2017 г., Национална публикация на въоръжените сили на Република България, НП – 01, МО, чл. 69

[57] Димитров Д, Цветков Цв., Икономическа сигурност, кризи и среда за иновации в сектора за сигурност и отбрана, стр. 10, https://www.unwe.bg/uploads/Yearbook/Yearbook_2014_No3_D%20Dimitrov, %20Tsv%20Tsvetkov.pdf

пандемията от COVID-19, стремително повишаващите се цени на торовете и енергията и влошаването на глобалните макроикономически условия, световните цени на селскостопанските стоки непрекъснато се покачват. Военната агресия на Русия срещу Украйна от февруари 2022 г. влошава положението, като предизвиква още по-голямо повишаване на цените на стоките и намалява наличността на храни в световен мащаб. Според Организацията на обединените нации през май 2022 г. световните цени на храните са били с почти 30 % по-високи, отколкото преди една година. Настоящата продоволствена криза оказва непосредствено въздействие върху цените на храните и наличието на доставки за голяма част от световното население и това въздействие вероятно ще продължи в дългосрочен план, особено в развиващите се страни.

Според ФАО почти 50 държави зависят от Русия и Украйна за най-малко 30 % от нуждите си от внос на пшеница, като 26 от тези държави осигуряват над 50% от своя внос на пшеница от двете държави; като има предвид, че Световната продоволствена програма закупуваше почти половината от световните си доставки на пшеница от Украйна и е посочила, че най-силно засегнати ще бъдат настоящите продоволствени кризи в държави като Афганистан, Етиопия, Сирия и Йемен.

Според ***световна продоволствена програма (WFP)*** на ООН през 2022 г. броят на изпитващите остра продоволствена несигурност може да нарасне с 47 милиона души, като нивата ще са най-високи в Африка на юг от Сахара. Нововъзникващите пазари и развиващите се страни неизбежно страдат най-много от последиците от световната криза. Очаква се средната инфлация да нарасне най-много в тези страни – с 8,7 %. Милиони деца в развиващите се страни са изложени на голям риск на остро недохранване в резултат на недостига на храни и по-високите цени. В ЕС не се очаква недостиг на храни благодарение на стабилното производство, гарантирано от общата селскостопанска политика на ЕС. Основният проблем е ценовата достъпност на храните. Най-засегнати са групите с ниски доходи и уязвимите групи.

Хранителните кризи не са нищо ново за стотици милиони хора по целия свят, които винаги са страдали от хроничен недостиг на храна и от недохранване. Новото обаче е в степента, в която това явление засяга общества, които отдавна са приели намаляващите цени на храните за даденост[58].

Географски примери за хранителни кризи [59]:

1) **Африка** – е един от континентите, които са най-уязвими за изменението на климата поради многобройните давления и ниската адаптивна способност. В Северна Африка и Сахел нарастващата суша, недостигът на водни ресурси и нерационалното земеползване ще причинят деградация на почвите и биха могли да доведат до загубата на 75 % от обработваемата земя, напоявана от валежи. Делтата на Нил би могла да бъде застрашена, както от покачването на морското равнище, така и от засоляване в селскостопанските райони, а 12 до 15 % от обработваемата земя може да изчезне вследствие повишаване на морското равнище през настоящото столетие, което ще засегне 5 милиона души до 2050 г. Понастоящем изменението на климата вече оказва сериозно въздействие върху конфликта в и около Дарфур.

В региона на Африканския рог намаляването на валежите и повишаването на температурите ще окаже значително негативно влияние върху тази област, която е силно подат-

[58] Baris Karapinar, Christian Haberli, и World Trade Forum, Food Crises and the WTO World Trade Forum (Cambridge; New York: Cambridge University Press, 2010), http://site.ebrary.com/id/10387017.

59 Документ от върховния представител и Европейската комисия до Европейския съвет, Изменение на климата и международна сигурност, S113/08 14 март 2008 г.

лива на конфликти. В южната част на Африка засушаванията са също фактор за лошите реколти, което води до несигурност на прехраната в няколко области, като милиони хора се очаква да бъдат изправени пред недостиг на хранителни продукти. Миграцията в този регион, както и миграцията през Северна Африка от други региони към Европа (транзитна миграция) вероятно ще се засили. В Африка, както и на други места, изменението на климата се очаква да окаже отрицателно въздействие върху здравето, по-специално поради разпространението на „векторни заболявания", което още повече ще изостри напреженията.

2) **Близък Изток**. Водните системи в Близкия Изток вече са изправени пред сериозни трудности. Приблизително две трети от арабския свят зависи от източници на вода, които се намират извън границите на арабските държави. Очаква се водите на реките Йордан и Ярмук да намалеят значително, което ще засегне Израел, Палестинските територии и Йордания. Почти сигурно е, че съществуващите напрежения по отношение на достъпа до водни ресурси в този регион ще се засилят, което ще доведе до още по-голяма политическа нестабилност с пагубни последици за енергийната сигурност и останалите интереси на Европа. В рамките на настоящото столетие е възможно водоснабдяването в Израел да намалее с 60 %. В резултат на това прогнозите са за значително понижение на селскостопанските добиви в тази област, която вече до голяма степен е пустинна или полупустинна. Съществени понижения на добивите се очакват в Турция, Ирак, Сирия и Саудитска Арабия, като по този начин се засяга стабилността на един регион от голямо стратегическо значение за Европа.

3) **Южна Азия**. Има вероятност покачването на морското равнище да застраши местообитанията на милиони хора, тъй като 40 % от населението на Азия (почти 2 млрд. души) живее в рамките на 60 km от бреговата линия. Недостигът на вода и намалената производителност в селското стопанство ще затруднят изхранването на нарастващото население на Азия, което освен това ще бъде изложено и на увеличаване на инфекциозните болести. Измененията в мусонните валежи и намаляването на топящите се води от Хималаите ще засегнат повече от 1 млрд. души. Конфликтите по повод на оставащите ресурси и неконтролираната миграция ще доведат до нестабилност в региона, който е важен икономически партньор на Европа с фактори на производството и разпределението, съсредоточени по продължение на уязвимата брегова ивица.

4) **Централна Азия** – е друг регион, тежко засегнат от изменението на климата. Вече може да се забележи нарастващ недостиг на вода, която представлява както ключов ресурс за селското стопанство, така и стратегически ресурс за производството на електроенергия. Ледниците в Таджикистан са загубили една трета от повърхността си само през втората половина на двадесети век, а в Киргизстан през последните четири десетилетия са изчезнали над 1000 ледника. Следователно в този регион, в който протичащите стратегически, политически и икономически процеси, както и нарастващите трансрегионални предизвикателства, имат пряко или косвено въздействие върху интересите на ЕС, е налице значителен допълнителен потенциал за конфликти.

5) **Латинска Америка и Карибският басейн**. В по-сухите области на Латинска Америка изменението на климата ще доведе до засоляване и опустиняване на селскостопанските земи, както и до намаляване на производителността по отношение на важни земеделски култури и животни. Това ще има вредни последици за продоволственото осигуряване. Прогнозите са, че покачването на морското равнище ще повиши риска от наводнения в ниско разположените области. Повишението на температурата на морската повърхност вследствие изменението на климата се очаква да окаже вредно въздействие върху ко-

раловите рифове и да причини разместванията в местоположението на рибните запаси. Държавите от Латинска Америка и Карибския басейн вече са подложени на пагубните въздействия, в т. ч. много екстремни явления, свързани с цикъла на Ел Ниньо. Измененията в режима на валежите и изчезването на ледниците се очаква да окажат значително въздействие върху наличието на вода както за консумация от човека, така и за селското стопанство и за производството на енергия, например в района на Андите. Държавите от Карибския басейн и Мексиканския залив вече във все по-голяма степен биват засегнати от силни урагани. Това ще се изостри допълнително от изменението на климата и ще доведе до социални и политически напрежения в този регион, в който структурите за управление често пъти са слаби.

6) **Арктика**. Бързото топене на полярните ледници, по-специално в арктическия регион, води до появата на нови водни пътища и международни търговски маршрути. Освен това, повишената достъпност на огромните въглеводородни ресурси в арктическия регион променя неговата геостратегическа динамика, което има потенциални последици за международната стабилност и за европейските интереси в областта на сигурността. Пример за очертаващите се нови стратегически интереси е издигнатото неотдавна на Северния полюс руско знаме. Все по-голяма е необходимостта да се отдели внимание на засилващия се дебат относно териториални претенции и достъпа до нови търговски пътища от страна на различни държави, които отправят предизвикателство към способността на Европа да гарантира ефективно своите търговски и енергийни интереси в региона и могат да окажат натиск върху отношенията й с ключови партньори.

Ярки нови доказателства за въздействието на изменението на климата върху способността на човечеството да произвежда обилна и питателна храна се появиха на различни континенти. Рояци от скакалци, провокирани от необичайно проливни дъждове, унищожават реколтата в големи части на Източна Африка и Югозападна Азия, нарушавайки доставките на храни. Тъй като наводненията затрудняват китайското земеделие, правителството осигурява продоволствената сигурност, като ограничава хранителните отпадъци. Жега и пламтящи пожари в западните райони на САЩ застрашават реколтата и добитъка, а бурята опустошава милиони акра насаждения на царевица и соя в Средния Запад. Силната суша във Франция нанесе хаос на селскостопанската продукция и накара фермерите да призоват правителството за помощ.

Промяната на климата е общата нишка, която предизвиква или влошава тези ужасяващи условия и води до опустошително въздействие върху наличността на храна, поминъка и човешкото здраве. Тъй като светът изпитва все по-тежки климатични въздействия върху селскостопанското производство, много от нашите хранителни системи са изтласкани до точката на пречупване.

Дългосрочните тенденции в недохранването подчертават забележимото разпространение на хроничния глад в страните, които преживяват хранителни кризи в продължение на няколко последователни години. Такива кризи могат да възникнат по всяко време и навсякъде по света поради *неблагоприятни метеорологични условия, природни бедствия, икономически шокове, конфликти или комбинация от тези фактори*. В подкрепа на навременните действия за изглаждане и предотвратяване на по-нататъшно влошаване на продоволствената сигурност в засегнатите страни Глобалната система за информация и ранно предупреждение (Global information and early warning system) на ФАО непрекъснато наблюдава ситуацията на всички континенти и съставя списък на страните в криза. Много от тези страни остават в списъка на GIEWS за дълго време или често са включени в него и се

разглеждат като „горещи точки" на глада - области, където значителна част от населението е хронично или периодично гладно или недохранвано.

Анализът на същността и основните причини за минали и настоящи хранителни кризи от съществено значение е да се подготвят подходящи спешни интервенции и политически реакции за премахване на „горещите точки" на глада. Този анализ предоставя основа за оценка на въздействието на бързото нарастване на цените на селскостопанските стоки, храните и горивата върху страните в криза (както и много други страни, които са силно уязвими от подобни ценови шокове). Пред лицето на несигурността, въздействието на бързо нарастващите цените на храните и горивата по държави, домакинства и лица по света, разграничението между държави, които вече са „в криза" и други „в риск", стана по-малко ясно, създавайки редица предизвикателства за мониторинг и за своевременно и подходящо ранно предупреждение за предстоящите хранителни кризи.

Според модели, изработени от учени от университета в Оксфорд (Springmann и съавт., 2016), до 2050 г. климатичните промени ще доведат до намаляване с 3.2% (на човек) в глобалната наличност на храна, с 4.0% в консумацията на плодове и зеленчуци и с 0.7 % - в консумацията на червено месо. Тези промени ще бъдат свързани с 529 000 допълнително смъртни случая в целия свят, свързани с климата, като повечето от тях се очаква да се случат в Югоизточна Азия, три-четвърти от всички случаи се падат на Китай и Индия. Очаква се също Гърция и Италия да бъдат силно засегнати.

Необходимо е да се укрепи *Световната мрежа за борба с продоволствените кризи* в работата й за справяне с продоволствените кризи чрез многостранни и многосекторни интервенции, изграждане на устойчивост и знания и осъществяване на връзката между хуманитарните действия, развитието и мира.

ИЗВОДИ:

1. Основните фактори за продоволствената и хранителната несигурност и недохранването, които се влошават, са конфликтите, изменението на климата и екстремните метеорологични явления, влошаването на околната среда, повишаващите се цени на енергията, ограниченият достъп до вода, икономическите сътресения, хроничната бедност и високите и трайни равнища на неравенство, включително неравенството между половете, липсата на достъп до основни социални и здравни услуги, нарастването на населението в световен мащаб и неуспешното управление, което впоследствие може да доведе до необходимостта от миграция.

2. Още преди войната в Украйна няколко страни се намираха в състояние на голяма несигурност поради уязвимости, свързани със сигурността, икономиката и климата и най-вече ефектите с пандемията от Ковид-19, която повиши с близо 120 милиона броя на хората, страдащи от недохранване в света. Заради пандемията и някои регионални конфликти малко под 770 милиона души изпаднаха в краен глад през 2021 г.

3. Войната в Украйна нанесе тежък удар на продоволствената сигурност на милиони хора. Последствията от тази война прескачат границите на Украйна и се усещат в целия свят: всички страни са засегнати от покачването на цените на земеделската продукция, но ефектът най-силно се усеща от населението на някои развиващи се страни, които вече се намират в състояние на значителна продоволствена несигурност и недохранване. Продоволствената криза, предизвикана от тази война ще накара повече хора да напуснат домовете си в по-бедните страни, което ще доведе до рекордни нива на глобално разселване и бежански вълни.

4. Според последните налични оценки в световен план приблизително 811 милиона души страдат от глад. В края на 2021 г. 193 милиона души са се намирали в положение на продоволствена криза в 53 страни или територии. Разпределението на двата милиарда души, които са изправени пред остри и умерени форми на продоволствена несигурност е както следва: 1,03 милиарда живеят в Азия, 799 милиона в Африка, 205 милиона в Латинска Америка и Карибите, 88 милиона в Северна Америка и Европа и 5,9 милиона в Океания.

References

1. Глобален доклад относно продоволствените кризи за 2021 г., актуализация от септември.

2. Доклад за състоянието на продоволствената сигурност и изхранването в световен мащаб, 2021 г.: https://www.fao.org/3/cb4474en/cb4474en.pdf

3. P9_TA(2022)0287, Справяне с продоволствената сигурност в развиващите се страни, Резолюция на Европейския парламент от 6 юли 2022 г. относно справянето с продоволствената сигурност в развиващите се страни (2021/2208(INI)),

4. Глобални цели и ангажименти на ЕС в областта на изхранването и продоволствената сигурност по света Резолюция на Европейския парламент от 5 октомври 2016 г. относно следващите стъпки за постигане на глобалните цели и ангажиментите на ЕС в областта на изхранването и продоволствената сигурност по света (2016/2705(RSP)), https://www.europarl.europa.eu/doceo/document/TA-8-2016-0375_BG.pdf

5. Караденчева Анна, Хуманитарната криза като една от най-тежките за човечеството ситуации, https://ejournal.vfu.bg/pdfs/%D0%A5%D1%83%D0%BC%D0%B0%D0%BD%D0% B8%D1%82%D0%B0%D1%80%D0%BD%D0%B0%20%D0%BA%D1%80%D0%B8%D0%B7%D0%B0% 20rec.pdf

6. Доктрина на въоръжените сили на Република България, Издание (А), ноември 2017 г., Национална публикация на въоръжените сили на Република България, НП – 01, МО

7. Димитров Д, Цветков Цв., Икономическа сигурност, кризи и среда за иновации в сектора за сигурност и отбрана, стр. 10, https://www.unwe. bg/uploads/Yearbook /Yearbook_2014_No3_D%20Dimitrov, %20Tsv%20Tsvetkov.pdf

8. Baris Karapinar, Christian Haberli, и World Trade Forum, Food Crises and the WTO World Trade Forum (Cambridge; New York: Cambridge University Press, 2010), http://site.ebrary.com/id/10387017.

9. Документ от върховния представител и Европейската комисия до Европейския съвет, Изменение на климата и международна сигурност, S113/08 14 март 2008 г.

10. Положение дел в области продовольственной безопасности и питания в мире, http://www.fao.org/publications/sofi/ru/

ONE OPTION FOR DETERMINING THE EFFECTIVENESS OF ANTI-TANK MEASURES AGAINST ARMORED TARGETS

Atanas Stavrev Atanasov

Military academy "Georgi S. Rakovski", Faculty " Command-staben", Department "Land forces", a.atanasov@rndc.bg

***Abstract**: The report presents an option for determining the combat effectiveness of anti-tank weapons based on paint modeling through the Lanchester equations, using different methods of determining the significance of individual components to determine the characteristics of the comparability coefficients. the report does not pretend to be exhaustive of the topic, but sets the stage for its discussion.*

ЕДИН ВАРИАНТ ЗА ОПРЕДЕЛЯНЕ НА ЕФЕКТИВНОСТ НА ПРОТИВОТАНКОВИТЕ СРЕДСТВА В БОРБАТА ИМ С БРОНИРАНИТЕ ЦЕЛИ

Атанас Ставрев Атанасов

Военна академия "Георги С. Раковски", факултет „Командно – щабен", Катедра "Сухопътни войски", a.atanasov@rndc.bg

Системите въоръжение, в това число и артилерията, са предназначени за нанасяне на огнево поразяване на различни обекти и цели на противника, намиращи се на различни отдалечения от нашите войски. Затова ефективността на техния огън в операциите и боя, т.е. ***бойната ефективност на въоръжението***, се оценява преди всичко по нивото на нанесените на противника загуби. От своя страна, противникът също ще се стреми да нанесе загуби на нашите войски. Величината и скоростта на нанасянето на загубите оказва решаващо влияние на изхода на операцията (боя) за всяка от страните, и затова определянето на загубите има изключително важно значение при оценката и прогнозирането на бойната обстановка.

При планирането и в хода на бойните действия се определят количеството въоръжение (артилерия) и боеприпаси, необходими за огневото поразяване на противника и се вземат специални мерки за тяхното рационално използване. Но потребното количество

средства за поразяване (боеприпаси и средства за тяхната доставка) зависи от редица фактори, като: величината на зададените загуби, противодействието на противника, вида и размерите на обектите, точността на определянето на данните за стрелба, избора на точки на мерене, и т.н. Изследването на тези фактори и определянето на зависимостта между тях и необходимото количество средства за поразяване са едни от най-важните проблеми в теорията на бойната ефективност.

За да се направят анализите на ефективността на противотанковите средства следва да се разгледат факторите, които са от решаващо значение за тази ефективност. Те могат да бъдат разделени на два раздела: първият факторите за ефективността на системата - вероятността за попадение в целта, вероятност от поразяване (унищожаване, разрушаване) на целта, скорострелност (брой изстреляни снаряди, ракети за единица време), надеждността и жизнеспособността на разчета и системата (отчитане на огневото противодействие на противника). И вторият раздел външните фактори, които могат да намалят ефективността – фактори на средата (като дъжд и прах), противодействие на противника (като тук следва да се включат и елементи като камуфлаж) и човешкия фактор (като боен стрес и качеството на обучението на разчета). Като правило проучванията (както таблиците за стрелба) се изготвят при идеални условия на оценка на ефективността и след това се прави оценка на степента на влияние на възможните фактори, които могат да намалят драстично ефективността и следва да се отчитат при определени условия.

Известно е, че противотанковата отбрана се изгражда в дълбочина, която се осигурява от системата на разпределение на противотанковите единици включващи различни типове управляеми и неуправляеми системи в зависимост от тяхната далекобойност и ефективност, която се осигурява от точността на попаденията (за управляемите системи зависи от устойчивото функциониране на системата за управление); способност за преодоляване на динамичната защита; - бронебойното действие върху многослойни и екранирани прегради на корпуса и куполата на бронираната цел.

За определяне на необходимите разнородни противотанкови средства в състава на определена групировка се използва коефицента за бойна ефективност на всяко от средствата включени в нейният състав. По този начин на етап предварително планиране, може с достатъчна достоверност да се обосноват възможностите на противотанковите средства.

Значенията на коефициентите на бойна ефективност на противотанковите средства може да се получи чрез моделиране на боя между противотанковите средства и атакуващите танкове, като за целта следва да се отчетат такива фактори като: точност на стрелбата на противотанковите средства и танковете и тяхната скорострелност; характеристика на поразяващото действие на снарядите на базата на защитеността на противостоящото средство; размерите на танковете и противотанковите средства; бойната скорост на атакуващите танкове; време за разкриване на целта, както от страна на танковете, така и за противотанковите средства (отчита се факта, че повечето от съвременните противотанкови средства, а и някои стари образци са на базата на бронирани машини); бойният ред на противотанковите средства и на атакуващите танкове; разстоянието между противотанковите средства и атакуващите танкове (рубежа за откриване на огън от противотанковите средства).

При извършване на моделирането има и някои особености като това, че не може да се отчета влиянието на подготовката на личния състав върху протичащите процеси, не се отчита въздействието на информацията върху управлението на средствата, под въпрос е отчитането на синергетичното влияние върху протичането на огневия двубой при повече единици техника и т.н.

За извършване на моделирането може да се използват редица модели за моделиране на бойните действия, като един от тези методи се основава на диференциалните уравнения на Ланчестър, който през 1916 г. предлага система от две диференциални уравнения за моделиране на въздушният бой. Трябва обаче да отбележим (с цел коректност), че до този момент подобен модел е публикуван и от руският математик М. П. Осипов, но поради редица причини се утвърждава модела на Ланчестър.

По този метод относителната бойна мощ на всяка от страните, се характеризира със средният брой разчетни единици съхранили боеспособността си, в които и да е момент от времето. При използване на този метод се правят следните допускания:

- не е задължително типът на въоръженията от двете страни да бъде еднакъв. Това означава че могат да се разглеждат боеве между танкове и противотанкови средства, което напълно удовлетворява извеждането на коефициента на бойна ефективност;

- всяка разчетна единица попада в зоната за поразяване на всички противникови разчетни единици. При това с един изстрел може да се порази само една цел (т.е. не се отчита вероятност за поразяване на няколко цели с един изстрел). Огънят е разпределен равномерно по всички противникови цели;

- полетното време на снаряда (ракетата) може да се пренебрегне;

- отчита се организираността на боя.

• За високоорганизиран бой стрелбата е прецизна и се води с отчитане на резултатите от нея. В случай на поразяване на целта огънят се пренася по друга цел.

• За лошо организиран бой се предполага, че стрелбата не е прецизна, а се разпределя на площ. Целите не са разузнати и поразяването на целта е случайно явление, поради което не се пренася огъня по друга цел.

- Целта не се възстановява след нейното поразяване всяка една разчетна единица може да бъде само в две състояния: поразена или непоразена.

За да се състави системата от диференциални уравнения, които описват състоянието на съвкупността от разчетни единици по време на боя се използва уравнението на Ланчестър.

В най общ вид уравнението на Ланчестър може да бъде записано така:

$$\begin{cases} \frac{dx}{dt} = ax + bxy + cy + d \\ \frac{dy}{dt} = ey + fyx + gx + h \end{cases}$$

Където: *a* и *e* определят скоростта на небойните загуби; b и f – скоростта на загубите в следствие на поразяването на площните цели; c и g - скоростта на загубите на предният край и d и h – подхождащите резерви.

Тъй като в нашият случай ние търсим само двубоя между танкове и противотанкови оръдия, диференциалните уравнения на Ланчестър ще придобият вида:

$$\begin{cases} \dfrac{dx(t)}{dt} = -\Lambda * y(t) \\ \dfrac{dy(t)}{dt} = -\Lambda * x(t) \end{cases}$$

Началните условия на тази система диференциални уравнения са:

$$\begin{cases} x(t=0) = N_1 \\ y(t=0) = N_2 \end{cases}$$

Където $N_1; N_2$ са количествата средства за въздействие на двете страни.

Отчитайки факта, че за устойчивост на резултатите е целесъобразно да се вземат повече от по една единица противоположно средство (т.е. не е целесъобразно да се разглежда двубой между един танк и едно противотанково средство) се взема двубой между танкова рота и противотанкова батарея.

При това положение е необходимо да се вземе интензивността на въздействие на всяка от страните U .

Където: $U_2 = \Lambda_2 \dfrac{N_2}{N_1}$, при t=0.

Изразът $\Lambda_2 * N_2$ в числителят има смисъл на среден брой успешни въздействия, които може да възпроизведе втората страна със своя първоначален състав. Като се раздели на N_1 - се получава средната стойност на средствата които могат да поразяват първата страна в началото на боя.

В хода на боя: $U_2 = \Lambda_2 \dfrac{m_2(t)}{m_1(t)}$ при t=0,

Където: $m_1(t)$ - математическото очакване на непоразените разчетни единици от състава на първата страна, към момента t;

- $m_2(t)$ - математическото очакване на непоразените разчетни единици от състава на втората страна, към момента t;

Условието за решаване на уравненията е, че Λ_2, Λ_2 са = константа. При това положение $m_1(t) = c_1.e^{\sqrt{\Lambda_1.\Lambda_2}.t} - c_2.e^{-\sqrt{\Lambda_1.\Lambda_2}.t}$, аналогично за $m_2(t)$.

Окончателно уравненията на Ланчестър добиват вида:

$$\begin{cases} m_1(t) = N_1.ch(\sqrt{\Lambda_1.\Lambda_2}.t) - N_2.\sqrt{\dfrac{\Lambda_2}{\Lambda_1}}.sh(\sqrt{\Lambda_1.\Lambda_2}.t) \\ m_2(t) = N_2.ch(\sqrt{\Lambda_1.\Lambda_2}.t - N_1.\sqrt{\dfrac{\Lambda_1}{\Lambda_2}}.sh(\sqrt{\Lambda_1.\Lambda_2}.t) \end{cases}$$

Където:

$$ch(x)=\frac{e^{x}+e^{-x}}{2};sh(x)=\frac{e^{x}-e^{-x}}{2}$$

Системата от диференциални уравнения дава възможност да се използват само крайни резултати. Методът дава възможност да се изследват резултати от противоборството между еднородни елементи от състава на противоборстващите страни. Когато се използват разнородни единици се използват коефициенти за съпоставиност между тях, въпреки, че използването на коефициенти за съпоставимост не винаги е убедително.

Използването на коефициенти за съпоставимост обикновено се извършва на базата на бойните потенциали на въоръженията, като за база на изчисленията се приемат характеристиките получени по един от следните методи:

- Съгласно метода на „U.S. Army Concepts Analysis Agency" - в извършване на сравнителен анализ между средствата по отношение на възприетият за еталонно средство образец. Всеки един образец въоръжение и бойна техника се оценява по показателите огнева мощ, мобилност и живучест. Изчисляването на значението на коефициента за ефективност (WEI) се определя по формулата:

$$\mathrm{WEI}=\mathrm{C}_{F}\times\mathrm{F}+\mathrm{C}_{M}\times\mathrm{M}+\mathrm{C}_{S}\times\mathrm{S}$$

където:

WEI – тежестен коефициент за ефективност;

$\mathbf{C_F, C_M, C_S}$ – тежестен коефициент на съответния показател;

F – показател (индекс) за огнева мощ;

M – показател (индекс) за мобилност**;**

S – показател (индекс)за живучест**.**

Изчисляването на стойността на всеки един показател става по следната формула:

$$\mathrm{Index}=\sum_{i=1}^{n}\mathrm{Q}_{i}\times\mathrm{C}_{i}$$

където:

Q_I – скала за качество (в рамките от 0-1) на техническите характеристики;

C_I – теглови коефициент за относителната важност на дадената характеристика;

n - брой на оценяваните характеристики;

При определяне на показателите за ефективност на даден образец въоръжение или техника могат да се включат неопределен брой характеристики, като отчитането на всички характеристики ще доведе до коректен резултат (при съвременната техника това не е непосилна задача).

- Съгласно метода на ***(Historical Evaluation And Research Organization (HERO)*** се залага на "Количествено обоснован метод за анализ" в основа на който е строго количественият подход за определяне математическата величина на индивидуалната

поразяваща способност на всяка оръжейна система или т.н. ***Теоретичен индекс (коефициент) за поразяване*.**

Изчисляването на числената стойност на показателя за поразяващата способност на определен вид въоръжение или бойна техника се извършва по формулата:

$$TLI = RF \times PTS \times RIE \times RN \times A \times RL$$

като при това се отчита комплексното влиянието на следните основни показатели:

• **Rate of Fire (RF)** – режим/темп на огъня;

• **Number of Potential Targets per Strike** (PTS) - Очакван брой цели, от състава на приетата за еталон цел (формирование от хора, в което всеки отделен индивид е заема площ 1 м^2), които могат да поразени с един изстрел.

• **Relative Incapacitating Effect (RIE)** - Относителни загуби на целта – щети, понесени в жива сила, техника и въоръжение, изразени в число или процент от поразяваните цели.

• **Accuracy (A)** – Вероятност за попадение (точност).

• **Effective Range (RN)** – Зона за поразяване/поразяващо действие

• **Reliability (RL)** – Надеждност (безотказност)

При определяне на теоретичния индекс на мобилните образци въоръжение и бойна техника се отчита влиянието и на тези конструктивни особености, чиито променливи величини оказват непосредствено влияние върху стойността на индекса.

Изчисляването на числената стойност на показателя за поразяващата способност на мобилните образци въоръжение или бойна техника се извършва по формулата:

$$TLI = \left[\sum_{i=1}^{n} \left[TLI_{(i)} \times BM \times RA \right] + RF \right] \times RFE \times FCE \times ASE \times CL$$

където:

TLI - Total Lethality Index – Сумарен индекс за поразяване

BM - Battlefield Mobility – Проходимост – отчита влиянието на проходимостта на машината върху нейната поразяваща способност $BM = 0{,}2 \times \sqrt{K}$

RA - Radius of Action – далечина на действие/запас от ход - $RA = 0{,}08 \times \sqrt{R}$ където, R - максимална дължина на прехода в километри

PF - Punishment Factor – бойна устойчивост на машината

RFE - Rapidity of Fire Effect – скорострелност;

ASE - Ammunition Supply Effect – возим боекомплект;

CL - Ceiling Effect – пределна височина на полета;

i – брой статични оръжейни системи монтирани върху машината

Известно е, че разработването на противотанкови оръжия е инициирано от разработването на бронирани машини. Причината за създаването на нови видове боеприпаси винаги е продиктувано от появата на обещаващ (дори все още не съществуващ в момента) танк.

Посоченият вариант за определяне на бойната ефективност на противотанковите средства **НЕ** изчерпва теорията на бойната ефективност. Налице са и други методи за определянето на коефициента на бойна ефективност: на базата на относителният дял на всяко средство в дадена операция; на обобщен критерии на ефективността на системата във времето по формулата:

$$K_{ep}(t) = \frac{C_{\sum(t)}}{E_T} = \frac{\sum_{i=0}^{t}[\sum_{j=1}^{m_{pr}}\sum_{k=1}^{n} C_{ijk}^{пр} + \sum_{j=1}^{m_{из}}\sum_{k=1}^{n} C_{ijk}^{из} N_{ijk}^{из} + \sum_{j=1}^{m_e}\sum_{k=1}^{n} C_{ijk}^{e} N_{ijk}^{e}}{\alpha_\beta \alpha_g \alpha_t \alpha_c \alpha_H \alpha_M} \longrightarrow \min$$

Където:

$C_{\sum(t)}$-общи разходи за проектиране, създаване и експлоатация на изделието; E_T – техническа ефективност на изделието; α_β – коефициент за огнева мощ; α_g – коефициент за далекобойност; α_t – коефициент за точност; α_c – коефицент за скорострелност; α_M – коефицент за маневреност; α_H – коефицент за надежност;

Използваните в последно време високоточни боеприпаси за поразяване на танковете доведе до разработването на средства за противоборства, както за тези системи, така и за противодействие на системите за управление на ПТРК. Това от своя страна предизвика ответен отговор на разработването на нови образци въоръжение и бойни припаси за тях, предизвикани от факта, че поразяването на брониранте цели е основен способ за снижаване на бойния потенциал на противника в операцията, която съчетана с маньовъра способства за неговия разгром.

References

1. Атанасов И. Изследване възможностите за повишаване ефективността на противотанковите бойни средства. София. 1980 г.

2. Градев К., Подход за оценка на бойните потенциали и бойните възможности на тактическа бойна група от Сухопътни войски в процеса на трансформация. Годишник на факултет "Командно щабен", 1/2010, 124-132 стр. Военна академия „Георги Стойков Раковски" София, 2011 ISBN 978-954-9348-27-9

3. Н. М. ФЕНДРИКОВ, В. И. ЯКОВЛЕВ. Методы расчетов боевой эффективности вооружения

4. Торнев Г.Б. Метод за прогнозиране развитието на бойните действия чрез моделиране. Дисертация. София. Рег № 3017-42. 2005 г.

5. В. ВОРОТНИКОВ, Г. СТЕРНИК - Математическая модель мишени для оценки эффективности противотанковых снарядов -http://btvt.info/5library/vbtt_1975_01_mbt80.htm

SOME CONCLUSIONS ABOUT THE USE OF ARTILLERY IN THE UKRAINIAN CONFLICT

Atanas Stavrev Atanasov

Military academy "Georgi S. Rakovski", Faculty " Command-staben",
Department "Land forces"
a.atanasov@rndc.bg

Abstract: *The report presents some conclusions about the use of artillery, based on the recent events of the conflict in Ukraine. The events that will happen subsequently will either confirm or reject some of the conclusions, which will show whether some of the markers were correctly counted. Only information from public sources is used in the report.*

НЯКОИ ИЗВОДИ ЗА ИЗПОЛЗВАНЕ НА АРТИЛЕРИЯТА В УКРАЙНСКИЯ КОНФЛИКТ

Атанас Ставрев Атанасов

Военна академия "Георги С. Раковски", факултет „Командно – щабен",
Катедра "Сухопътни войски"
a.atanasov@rndc.bg

Мирът, за който всички говорим, е възможен само тогава, когато поколението е изживяло ужасите на войната, сблъскало се е от първо лице със смъртта и е осъзнало, че трябва да се правят компромиси и от двете страни в името на това да продължим да съществуваме като хора. Характерно за хората обаче е, че човешката памет е къса и бързо забравя това, което е било. Само след едно поколение (участвало във война) след втората световна война, когато всички (или поне повечето от нас) си мислихме, че на територията на стария континент няма да има война, сме свидетели на поредната такава (макар и определяна от някой за специална военна операция). Това трябва да ни подскаже, че мирът е онова крехко създание (почти неукрепнало във времето), което във всеки един момент може да бъде унищожено от зверовете на човешката слабост. Затова познаването на законите на войната, необходимите средства за воюване и техните възможности са в основата на подготовката ни за запазване на мира, чрез изграждане на силни, боеспособни и добре въоръжени формирования.

Украйна се включи във военния конфликт с близо 1800 артилерийски системи, разпределени към 25 линейни бригади, пет отделни артилерийски бригади и резервни и териториални формирования. Почти всички системи са руски модели, включително по 122-милиметрови 2С1 и 152-милиметрови 2С3 самоходни гаубици, около 203-милиметрови самоходни гаубици 2С7, 500 буксирни гаубици, близо 400 ракетни системи и 300 минохвъргачки.

По не потвърдени данни, освен постсъветското въоръжение от началото на конфликта в армията на Украйна постъпва следното артилерийско въоръжение: РСЗО М142 HIMARS - 16 бр.; РСЗО М270 MLRS – 9 бр – от които от обединеното кралство - 3 бр. модел М270В1, от Норвегия и Германия по 3 бр. ; 155-мм САУ М109А3GN, М109А4BE, М109А5Ö - над 50 бр,; 155-мм САУ PzH 2000 -18 бр. от които 10 бр. от Германия – 8 бр. от Нидерландия; 155-мм САУ AHS Krab - 18 бр. от Полша; 155-мм САУ CAESAR - 18 бр. от Франция; 155-мм САУ ShKH Zuzana 2 – 4 бр. от Словакия; 155-мм Буксируема гаубица М777 – 136 бр от които 126 от САШ, 6 бр. от Австралия и 4 бр. от Канада; 155-мм Буксируемя гаубица FH70 – повече от 8 бр. - от Италия и Естония; 105-мм Буксируемя гаубица М119 – 16 бр. от САЩ; 105-мм Буксируемя оръдие L119 – 36 бр от Великобритания; 120-мм минохвъргачки 120 Krh/40 -12 бр. от Германия.

Или общо като помощ Украйна е получила артилерийски системи с калибър на 100 мм – повече от 340 единици и над 70 000 артилерийски снаряда калибър 155 (които според някои източници трябва да достигнат 183 000 артилерийски снаряда само за М777) и над 50 000 снаряда калибър 105 mm. Като само по последния обявеният 13-ти пакет помощ за Украйна (общо 450 милиона долара) са 36 000 снаряда калибър 105 mm. Това е необичайно, понеже повечето от артилерийските системи, предоставени на Украйна, са с калибър 155 mm, който е стандартният калибър за НАТО. И всички предоставени системи са с този калибър с изключение на предоставените от САЩ и Великобритания системи 105 мм. Тези системи по принцип са част от десантните сили тъй-като 105 mm системи са леки и лесни за пренасяне и са предпочитани за някои леки сили, като парашутистите, където по-тежката система е твърде обемиста и тежка за транспортиране. За РСЗО М142 HIMARS и М270 MLRS към момента сведенията са за предоставени само управляеми боеприпаси, като САЩ, въпреки че **НЕ** са подписали конвенцията за касетъчните боеприпаси не са предоставили стандартния касетъчен боеприпас М26. Към настоящият момент няма и сведения за предоставяне на високоточни боеприпаси за артилерията, както и тактическата ракета MGM-140 ATACMS (последната поради възможността и да се поразяват цели на територията на Русия).

Последният пакет помощ в състав от 105 мм боеприпаси показва засилването на десантните сили и леката пехота с артилерия предназначена да действа в дълбочина на противниковата отбрана, които в комбинация с поддръжка от далекобойните системи РСЗО могат да постигнат значителен превес над определени райони.

Особености в използването на артилерията

В началото на конфликта Руската артилерия има над 3:1 превъзходство в огнева мощ. По не потвърдени сведения руската артилерия изстрелва средно по 20 000 снаряда дневно, в сравнение с 6000, изстреляни от украинската артилерия. Още по-голямо е съотношението при пускове на реактивната артилерия и балистични ракети.

Въпреки, че голяма част от артилерията е децентрализирана и придадена на батальонните и бригадните тактически групи (от 1 до 3 батареи в ББГ и 1 до 2 дивизиона в БрБГ в това число дивизион РСЗО), по голямата част от артилерията остава на централно подчинение като се сформират артилерийски групи към бригадите и дивизиите.

Ефективността на артилерията се определя от наличието на дронове за коригиране на стрелбата и наблюдение на резултатите в реално време. В същото време може да се води наблюдение върху колони и да се предприеме поразяване тогава, когато е необходимо. Освен това за контрабатарейната борба е от съществено значение поразяването на целите в реално време, поради маневрения характер на конфликта. От друга гледна точка наличието на дронове за разузнаване и коригиране на стрелбата не изисква голямо количество артилерия и определени задачи могат да се изпълняват от взвод, а понякога и от едно РСЗО. Това обаче не е широко разпространена тактика поради неясни причини. Когато обаче се използва ответният огън е в рамките на до 3 минути. Само най-модерните мобилни артилерийски системи на Украйна, доставени от Запада, могат да стрелят достатъчно бързо, за да избегнат ответният удар. В резултат на това украинските артилерийски батареи редовно разполагат преносими ракети за противовъздушна отбрана – за предпочитане оптично насочвани ракети Starstreak/Marlet – за да свалят дронове. Конфликтът осигурява още едно напомняне за важността на пасивната защита. В ерата на широко разпространените сензори и дронове, трябва да се обмислят нови начини за камуфлаж и защита на силите.

Използването на артилерията от страна на руската армия се характеризира със следните особености: гаубиците се използват за поразяването на единични цели и взодни опорни пунктове, докато РСЗО се използва за възпрепятстване движението и поразяването на колони. За контрабатарейна борба са оставени ракетните системи Точка-У. Най-често използваната тактика е стандартната артилерийска подготовка с последващо преминава на войските в настъпление. Докато артилерията поразява позициите на противника подразделенията от спецназ и механизираните формирования се придвижват флангово и веднага след завършване на стрелбата на артилерията атакуват отбраняваните позиции. Тук обаче руските войски се натъкват на нова тактика от страна на украинската армия. Артилерията е изведена назад и е подготвила огън по позициите, където са били украинските сили. В момента на началото на огневата подготовка на руската артилерия украинските сили се извеждат от позициите и с началото на атаката по тези позиции украинската артилерия открива огън. Това води до необходимостта от нов подход от руска страна за водене на боя. От гледна точка на руските военни това е така наречения *«отсекающий огонь»*. С този метод артилерията използва около два до три пъти повече снаряди, отколкото с "огневия вал". Това не е просто увеличение на количествените показатели, но и различно разпреде-

ление на огъня. Нещо повече, той е инсцениран: първо се обстрелват предни позиции с нарезна артилерия, след това онези райони, където въоръжените сили на Украйна могат да се укрепят и откъдето могат да открият огън с реактивни системи за залпов огън. Този метод не може да се използва когато отбраната се изгражда пред населен пункт поради големите отклонения на руските реактивни системи за залпов огън. Доколко една такава тактика на артилерията е оправдана не може да се каже, но това подсказва на украинците, че артилерийският двубой може да се спечели с лишаването на артилерията от боеприпаси. Именно и тук се намесват системите РСЗО HIMARS за стрелба по складове и пунктове за снабдяване на артилерията с бойни припаси.

Разположението на руската артилерията остава класическо като артилерийските части обикновено се разполагат приблизително на една трета от максималната си далекобойност - минохвъргачките са разположени до голяма степен на 1,5 км назад от линия на съприкосновение, артилерийските групи, подчинени на бригади, на 8 км назад, а тези въоръжени със системи с по-голям обсег, предназначени за дълбоко поразяване на 10-15 км назад. Взводовете обикновено се разполагат в зона 100×300 метра, с 20-40 метра между оръдията. Извън всякаква логика ракетно-пусковите системи се разполагат и линейно, с до 150 метра между машините. За въвеждане на противника в заблуда се използват артилерийски батареи с предимно повредени/унищожени оръдия. Преместването на артилерията и от двете страни в конфликта обикновено се извършва нощем, особено ще се касае за 155-мм САУ CAESAR и буксируемите М777 от украинска страна.

Изводи:

1. Предоставената от страна на САЩ, Канада и страните от европейския съюз артилерия за украинската армия поставя тенденцията за стабилно преминаване на Украйна към стандартната система на НАТО и се отдалечава от руския стандарт.
2. Предоставянето на 105 мм гаубици и оръдия както и боеприпаси за тях показва тенденция към укрепване на десантно щурмовите групи и тяхното използване в близко бъдеще.
3. Очертава се тенденция за използване на все по малки артилерийски формирования в едно с дронове за нанасяне на прецизни удари. За ефективна борба с дроновете се използват преносими ракети за противовъздушна отбрана.
4. Предоставянето на системи РСЗО от типа на HIMARS ще се ограничи до това ниво, поради липсата на доставки на стандартния боеприпас М26 а с наличните управляеми боеприпаси системите са достатъчни.
5. За въвеждане на противника в заблуда ще се продължава да се използва пасивната защита чрез камуфлаж и повредена техника.

В заключение следва да се посочи, че **НЕ** е необходимо да бъдем въвлечени във военен конфликт за да обърнем внимание на собственото си състояние, а напротив – армията се изгражда в мирно време със съвременно въоръжение, способно да се противопоста-

ви на евентуален противник. Отчитайки това за артилерията е все по належащо да се вземе решение на къде ще се върви (не като калибър, а като това дали на колестна или на верижна база) и какви системи в кои структури следва да се заложат.

References

1. Новая тактика «отсекающего огня» ВС РФ стала настоящей проблемой для ВСУ https://polit.info/23599060-novaya_taktika_otsekayuschego_ognya_vs_rf_stala_nastoyaschei_problemoi_dlya_vsu

2. The Secrets of Russia’s Artillery War in Ukraine https://www.19fortyfive.com/2022/07/the-secrets-of-russias-artillery-war-in-ukraine/

3. Artillery leading the fight in Ukraine https://www.washingtontimes.com/news/2022/may/20/artillery-leading-fight-ukraine/

4. Latest Ukraine Package: More Artillery and the Beginnings of a New Navy June 27, 2022 https://www.csis.org/analysis/latest-ukraine-package-more-artillery-and-beginnings-new-navy

5. New US weapons for Ukraine.. support for the “artillery battle” against the Russians https://www.archyde.com/new-us-weapons-for-ukraine-support-for-the-artillery-battle-against-the-russians/

6. The king of battle’ — How US artillery in the hands of Ukrainians may reshape the war with Russia https://taskandpurpose.com/news/us-military-artillery-ukraine-russia-war/

COMBAT AERIAL VEHICLE DEPLOYMENT IN SIXTH GENERATION WARFARE

Stoyan N. Chanev

Assistant Professor at the Department of Air Defense, Artillery, Air Defense and CIS Faculty at the Vasil Levski National Military University, tel. 054/801040, ext. 54266, e-mail: st.chanev@abv.bg

Annotation: *The paper examines the characteristics of sixth-generation warfare and the ways in which combat aerial vehicles can be used. The trends and the order of increasing efforts are indicated, as well as the objects for their application. In research of the composition of the strikes, the potential structure and tasks of the individual echelons are shown.*

Key words: *sixth-generation warfare, combat aerial vehicles, massive missile strike.*

БОЙНО ИЗПОЛЗВАНЕ НА СРЕДСТВА ЗА ВЪЗДУШНО КОСМИЧЕСКО НАПАДЕНИЕ ПРИ ВОЙНА ОТ ШЕСТО ПОКОЛЕНИЕ

Стоян Н. Чанев

Главен асистент в катедра "Противовъздушна отбрана", факултет "Артилерия, ПВО и КИС" на НВУ "Васил Левски", тел. 054/801040, вътр. 54266, e-mail: st.chanev@abv.bg

Анотация: *В доклада са разгледани характеристиките на война от шесто поколение и способите за използване на средствата за въздушно космическо нападение. Посочени са тенденциите и реда за нарастване на усилията, както и обектите за прилагането им. При изследване на състава на ударите е показана потенциалната структура и задачите на отделните ешелони.*

Ключови думи: *война от шесто поколение, средства за въздушно космическо нападение, масиран ракетноавиационен удар.*

Увод

Войната по своята същност представлява решаване на международни противоречия чрез силово налагане на волята над опонента. Последните шест хиляди години от човешката история са белязани от над 15000 въоръжени конфликти и войни с над 3,5 милиарда жертви и пострадали [3], което показва, че войната е често срещано явление. Тя възниква, когато международните отношения вследствие на проблемногенериращи ситуация са трайно и остро влошени и такава ситуация не може да се реши по мирен път. Според военния историк Базил Лидъл Харт целта на войната е постигане на мир, по-добър от предвоенния. В съвременните условия основна пречка пред избухването на пълномащабен военен конфликт се явява възпиращия ядрен потенциал на Великите сили. Нарастващите противоречия в световен мащаб до степен на цивилизационно про-

тивопоставяне и бурното развитие на научно-техническия прогрес предпоставят търсенето на „приемливи решения" за водене на военни действия в условия на използване на ядрено оръжие с минимизиране на последствията – чрез изпреварващ удар, развитие на противоракетната отбрана и приоритетно използване на високоточни оръжия на стратегическо, оперативно и тактическо ниво при минимално участие на персонал в зоната на огъня на оръжейните системи. Най-пълно тези изисквания биха се изпълнили при масово използване на средства за въздушнокосмическо нападение (СВКН), поради тяхната досегаемост, мобилност, и автономност.

1. Война от шесто поколение

Опита от войните и въоръжените конфликти показва влиянието на развитието на въоръжението и техниката както върху характера на войната, така и върху стратегията за воденето й. Класификацията на поколенията войни според характера на използваното въоръжение, мащаба на действията и поставените цели са представени в таблица 1 [6]. Войните до пето поколение са считани за инструмент на политиката и нейно допустимо продължение при необходимост. Ядрената война от пето поколение при пълномащабен конфликт е възможно да доведе до унищожаването както на противоборстващите страни/коалиции, така и на човешката цивилизация като цяло.

Таблица 1

Класификация на поколенията войни

Характеристика на използваното въоръжение	**Мащаб на действията**	**Цели**
Първо поколение		
Хладно оръжие	Тактически	Унищожение на противника, овладяване на територия.
Второ поколение		
Огнестрелно, гладкоцевно	Тактически, оперативно-тактичерски	Унищожение на противника, овладяване на територия или нейното контролиране.
Трето поколение		
Огнестрелно, нарезно, многозарядно, с повишена точност и дакекобойност	Оперативно-тактичерски, тактически	Разгром на групировките на ВС на противника, установяване на контрол на територия и ресурси.
Четвърто поколение		
Автоматично и реактивно, обособяване на видовете ВС и родовете войски от ВС, развита логистика и комуникации	Оперативно-стратегически	Разгром на ВС на противника, разрушаване на икономическата и политическата система.
Пето поколение		
Ядрено оръжие	Стратегически	Разгром на ВС на противника, разрушаване на икономиката, смяна на политическия строй.
Шесто поколение		
Високоточно оръжие (ВТО) с наземно, въздушно и морско базиране, информационно-космическо осигуряване	Стратегически, оперативно-стратегически и оперативни	Установяване на контрол над ресурси и население, установяване на лоялна власт над територията, където се намират тези ресурси.

Влияние на характера на бъдещата война от шесто поколение ще окаже основно въвеждането на въоръжение на:

– хиперзвукови оръжейни системи – това ще доведе до глобален характер на потенциалната война, главните цели за поразяване ще се търсят в оперативно-стратегическата и стратегическата дълбочина на противника. За нанасяне на удари ще се използват балистични и крилати хиперзву-

кови ракети и планиращи бойни блокове. Времето за нанасяне на удари в зависимост от дистанцията ще бъде от минути до час, а обхвата – на един или няколко театъра на военните действия (ТВД). Хиперзвуковото оръжие лежи и в основата на теорията за бърз, мълниеносен глобален удар (Promt Global Strike), целящ обезвреждането на по-голяма част от ядрения потенциал и стратегическото ръководство на противника;

– оръжейни системи от ново поколение – лазерно, високочестотно, електромагнито;

– роботизирани комплекси с военно предназначение;

– специализирани безпилотни летателни апарати (БЛА) – разузнавателни, за електронна война (EW), ударни, лъжливи цели за ПВО/ПРО на противника. В перспектива ще се използват и множество малогабаритни БЛА под формата на организирани рояци със сложна йерархична структура.

Воденето на война от шесто поколение ще изисква и формирането на единно информационно-комуникационно пространство на базата на създаване на спътникова групировка, включваща специализирани разузнавателни и комуникационни сателити. Бойното пространство следва да се насити със сензори, следящи придвижването, развръщането и действията на противника в цялата дълбочина на ТВД. Особено значение се отделя на системите за ранно предупреждение, регистриращи изстрелването на балистични ракети – разузнавателни спътници за инфрачервено и радиолакационно разузнаване, както и специализирани РЛС за откриване на балистични цели при навлизането им в горните слоеве на атмосферата. Възможностите на коалиционни сили на НАТО при война от шесто поколение за създаване на единно информационно-комуникационно пространство на ТВД (настоящи и в близка перспектива) и довеждане на разузнавателна информация до потребителите, включително и на тактическо ниво са представени в таблица 2 [2].

Таблица 2

Възможности на системата на разузнаване на коалиционните сили на ТВД

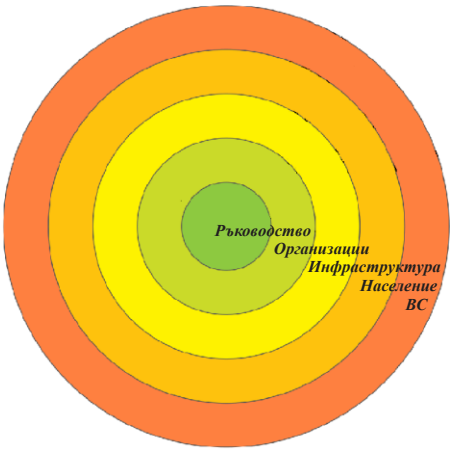
№	Критерий за оценка	Съществуващи	Прагови	Очаквани
1	Довеждане на информацията от средствата за РЛР с възможност за селекция на движещи се цели до потребителите на ТВД	< 1 min	≤ 10 sec	≤ 5 sec
2	Довеждане данните от визуалното разузнаване до потребителите на ТВД	< 20 min	≤ 5 min	≤ 2 min
3	Довеждане на обобщена информация за обстановката на бойното поле на база на РЛР и визуално разузнаване с възможност за селекция на движещи се цели до потребителите на ТВД	≥ 30 min	≤ 20 min	≤ 5 min
4	Предоставяне достъп на командирите от всички звена до потока от разузнавателна информация - формиране на единна картина на обстановката на бойното поле	-	≤ 5 min	≤ 1 min
5	Пренасочване на средствата за разузнаване на коалиционните сили	≥ 30 min	≤ 10 min	≤ 2 min
6	Идентификация на средства в зоната на видимост	≥ 30 min	≤ 12 min	≤ 3 min
7	Предаване на данни за ЦУ до всяко едно средство за поразяване на ТВД	≥ 30 min	≤ 5 min	≤ 2 min
8	Възможност за интеграция на ново разузнавателно средство във вече функционираща система за бойно управление, свръзка и разузнаване на бойното поле	месеци	≤ 1 седмица	≤ 1 ден

Основни характерни черти на войните от шесто поколение са:

– главно оръжие ще се явява ВТО;
– възможност за поразяване на войски и обекти на цялата територия на воюващите държави;
– отсъствие на пряко съприкосновение с противника (безконтактна война);
– активно информационно противоборство;
– възможност за асиметрични действия;
– широко използване на космическото пространство за осигуряване и водене на бойните действия.

Тези особености водят и до създаване на нова концепция за водене на военните действия – мрежоцентрична война.

Основоположник на теорията за мрежоцентричната война е **Джон Уорден** (John Warden), специалист в използването на военновъздушните сили (ВВС), сформирал виждане за избора на стратегически цели за войната на XXI в. Предлага използването на въздушнокосмическите сили (ВКС) като доминиращи за извеждане от строя на противника чрез поразяване на жизнено важни за функционирането му центрове, наричайки ги „центрове на тежестта" [7]. През 1988 г. предлага модел за декомпозиция на тези центрове в пет сфери, показани на фиг.1, като пет концентрични кръга.



Фиг. 1. Декомпозиция на центровете на тежестта

Според теорията на Уордън всеки стратегически обект може да се раздели на пет части, като в най-вътрешния кръг се намира най-критичния елемент на системата – нейното ръководство. Във всеки кръг съществуват множество обекти. Измежду тях се намират и „центровете на тежестта", един или няколко, като елиминирането или неутрализирането им води до преставане на функционирането на целия кръг. Първоначалния анализ откроява първия пласт на откриване на тези центрове, но с последващо задълбочаване на изследванията се достига до системните връзки, свързващи както елементи от даден кръг, така и елементи от друго йерархично ниво. Така извършения системен анализ позволява да се изготви план на стратегическо ниво за конкретен противник, отчитайки неговите особености – държавна власт, военно, икономическо и социално положение на обществото. Тази теория изследва противника в статика, без да отчита възможността за противодействие и възможните цикли „действие-реакция" в хода на конфликта.

Теорията на циклите на Джон Бойд (John Boyd), полковник от ВВС на САЩ позволява да се изследва въоръженото противостоянието между две страни в динамика. В основата на модела е разглеждането на четири последователно повтарящи се взаимосвързани цикъла: Observe – Наблюдение, Orient –, Decide – Решение, Act – Действие. Оттам идва и наименованието на модела – OODA (НОРД) [9]. Значението на отделните цикли е както следва:

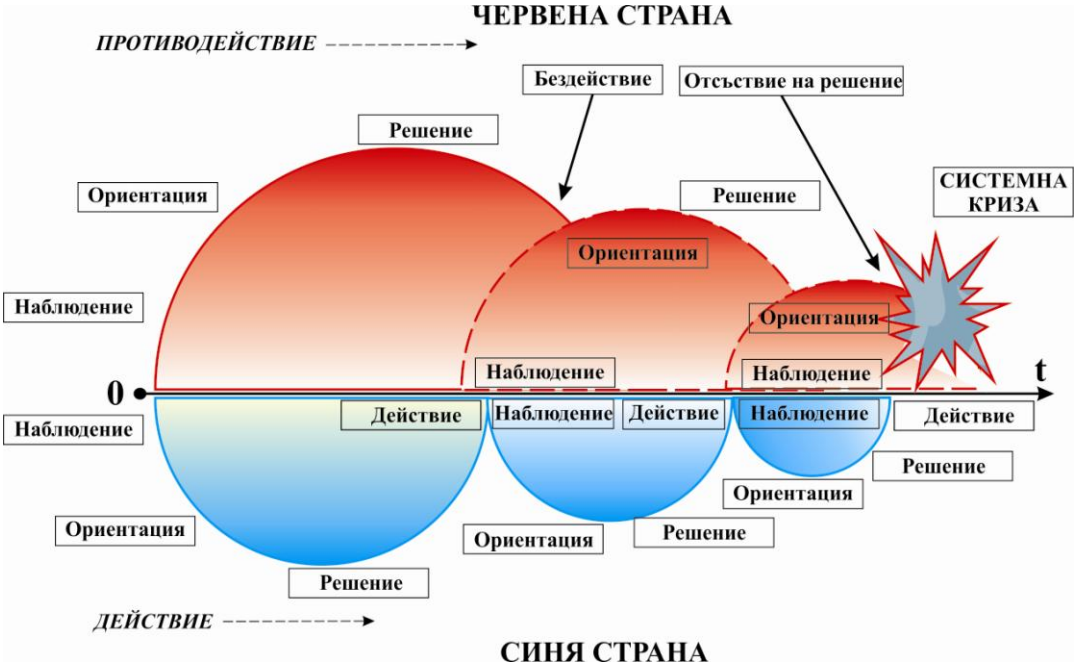
– наблюдение – процес на сбор на информация, необходима за вземането на решение;

– ориентация – най-сложния етап. Състои се от декомпозиция на множество малки елементи, подлежащи на когнитивен анализ и впоследствие обединяването им в общ план за действие – синтез;

– решение – при наличие на повече от един вариант за действие на база на уточнени процедурни правила се избира един от тях за реализация;

– действие – практическа реализация на избрания вариант за действие.

В хода на военните действия страната имаща инициативата и възможността за ускорено провеждане на четирите цикъла, но с необходимото за целта качество на изпълнението, заставя противника да го следва. На всеки ход неговото изоставяне води до невъзможност на завършване на цикъла и вземането на нови решения под диктовката на волята на противостоящата страна. На фиг. 2 е представен цикъл на Бойд в две фази. Синята страна изпреварва червената. В първата фаза не се стига до действие, т.к действието на червените налага промяна на решението. На втората фаза изоставането води до невъзможност за вземане на адекватно решение и оттам на следващата фаза се получава системен срив (поражение) на червените.



Фиг. 2. Системна криза за две фази на цикъл НОРД

Тези две теории са основополагащи за концепцията за мрежоцентрична война. Мрежоцентричните операции се провеждат в мрежева среда, включват елементи на въоръжението и информационна осведоменост на всички нива. Характерно е високо ниво на децентрализация, гъвкавост и ефективност в условията на неопределеност, както и използване на военни и граждански ресурси за постигане на целите [1]. Намеренията на старшия командир са база на която се основава процеса на планирането, а самата реализация на задачите често се извършва автономно от интегрирани формирования с всестранно осигуряване, независимо от йерархичното им ниво. Това позволява бързо и правилно целеполагане и съкратен НОРД цикъл, оттам и превъзходство над противника по отношение на оперативност и изземване на инициативата [5, 8].

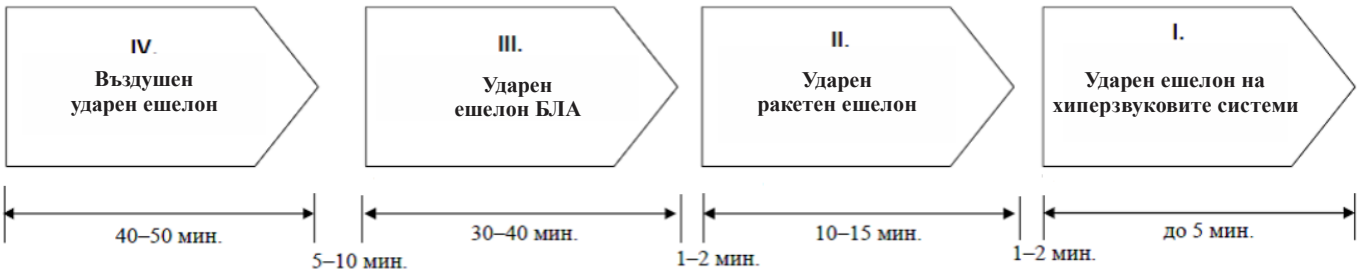
Самия конфликт може да бъде разделен на четири периода: *подготвителен* (с продължителност, зависеща от конкретната обстановка) – включва информационно, икономическо и хибридно противоборство; *активен* – военни действия с масово използване на ВТО и СВКН – цел се явяват държавно и военно ръководство, критична инфраструктура, включително и на стратегическите ядрени сили, стратегически пунктове за управление и комуникации; *наземна операция* (при необходимост) – с цел унищожаване на сухопътната групировка на противника, окупация и налагане

на контрол на населението; *провеждане на операция по стабилизация* – по същество информационно-психологически операции. Не само факта, че основоположниците на концепцията за мрежоцентричната война са с афинитет към СВКН, но и самата структура на такъв конфликт показва, че водеща роля ще има използването на въздушнокосмическото (в активния период) и въздушното пространство (в третия период).

2. Бойно използване на СВКН при война от шесто поколение

В съвременните военни конфликти през 21 в. се очертава тенденцията за засилване ролята на въздушното и космическото пространство като основно място за завоюване на решително превъзходство над военния противник при конфликти с различна интензивност, с което най-често се предрешава и техния изход. Едновременно с това се развиват формите и способите за действие на ВП, целящи минимално излагане на СВКН под въздействието на изградените системи за ПВО и ПРО – увеличени дистанции за използване на ВТО, комплексно въздействие в цялата дълбочина на ТВД, широко използване на безпилотни средства и разузнавателно-ударни системи за извършване на пробив в системата за ПВО/ПРО и последващо завоюване на превъзходство във въздуха.

Въздушните удари при такива операции ще са от различни по тип СВКН (БР, КР, БЛА, авиация), като направленията, интервалите между групите и тяхното построение са различни в зависимост от фазата на операцията и решаваните задачи. На практика се размиват ешелоните във ВУ, т.к. се въздейства от голяма дистанция (БР, КР), в зоната на огъня се намират СВН от различен тип (БЛА и пилотируема авиация), част от тях ще са непрекъснато в тази зона, а не за ограничено време (тактически БЛА). Въпреки това се наблюдава тенденция на построението на ВУ, насочена към минимално излагане на зенитния огън на пилотируемите СВН и нанасяне на удари без влитане в зоната на ПВО/ПРО. Поради широкото използване на ракетно въоръжение тези удари се явяват ракетновъздушни авиационни. На фиг.3 е представено примерно построение на масиран ракетновъздушен авиационен удар (МРВУ) [4].



Фиг. 3. МРВУ

Първите два ешелона въплъщават възгледите за водене на безконтактна война с масово използване на ВТО и са характерни за началния етап на всеки въоръжен конфликт.

Ударния ешелон на хиперзвуковите системи е предназначен за високоточни удари по елементи на системите за ПВО и ПРО за осигуряване преминаването на дозвуковите и свръхзвуковите БР и КР от втория ешелон. Основни цели за него се явяват и пусковите установки на балистичните ракети – междуконтинентални и за средно разстояние (ПУ МБР БРСР), както и РЛС за ранно предупреждение.

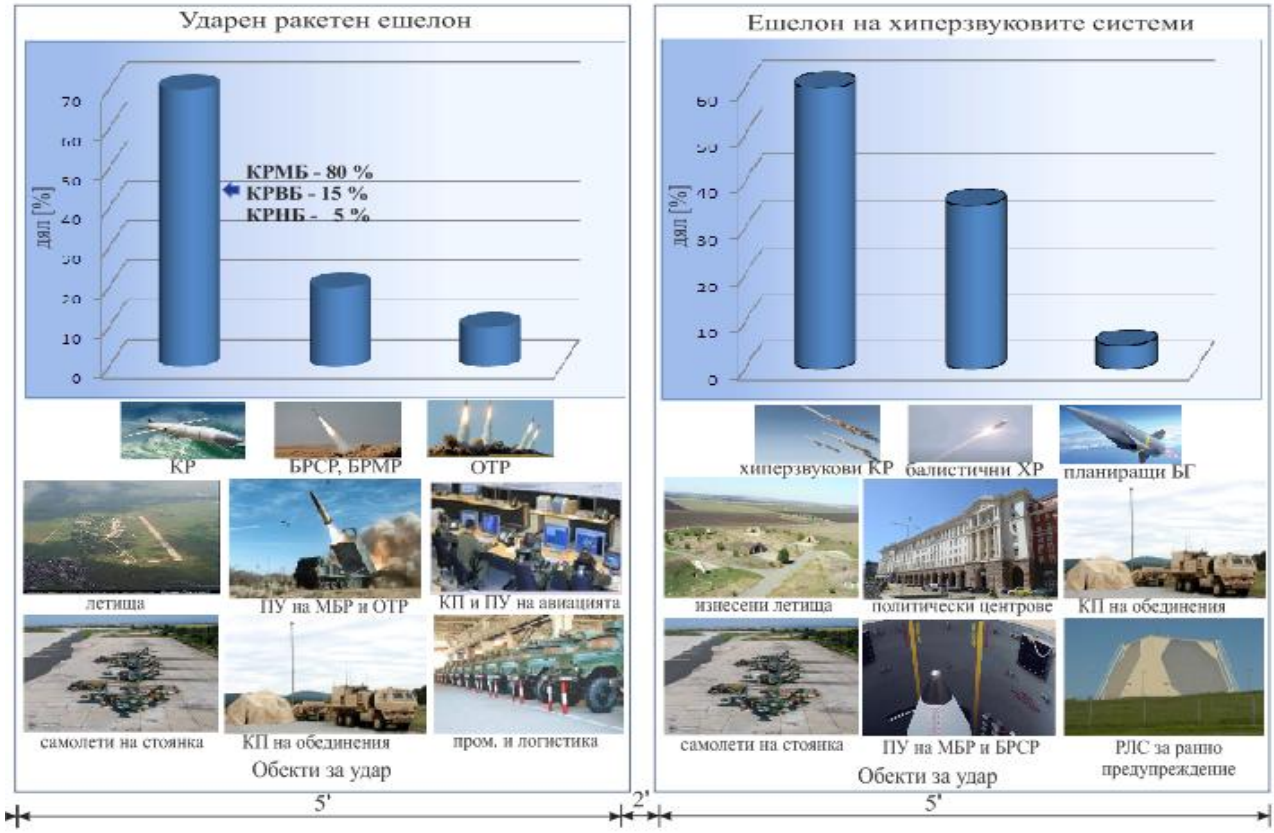
II-ви ешелон (КР) осигурява безконтакто водене на бойни действия с използване на ВТО. Основните цели са предотвратяване на загуби на личен състав и ефективно изпълнение на задачите, характерни за началния етап на въоръжения конфликт – подавяне на системата за ПВО и завоюване на господство във въздуха. Цели се явяват и ПУ на МБР и опертивно-тактически ракети (ОТР). Ударния ешелон КР е предназначен за нанасяне на удари в цялата дълбочина на построение на войските.

Ешелонираното и масово използване на БЛА е насочено към изпълнение на последващите основни задачи и създаване на условия за разгром на противника от ешелона на пилотируемата авиация (ПА). Перспективни БЛА ще осигуряват действията на оперативните и стратегическите БЛА чрез:

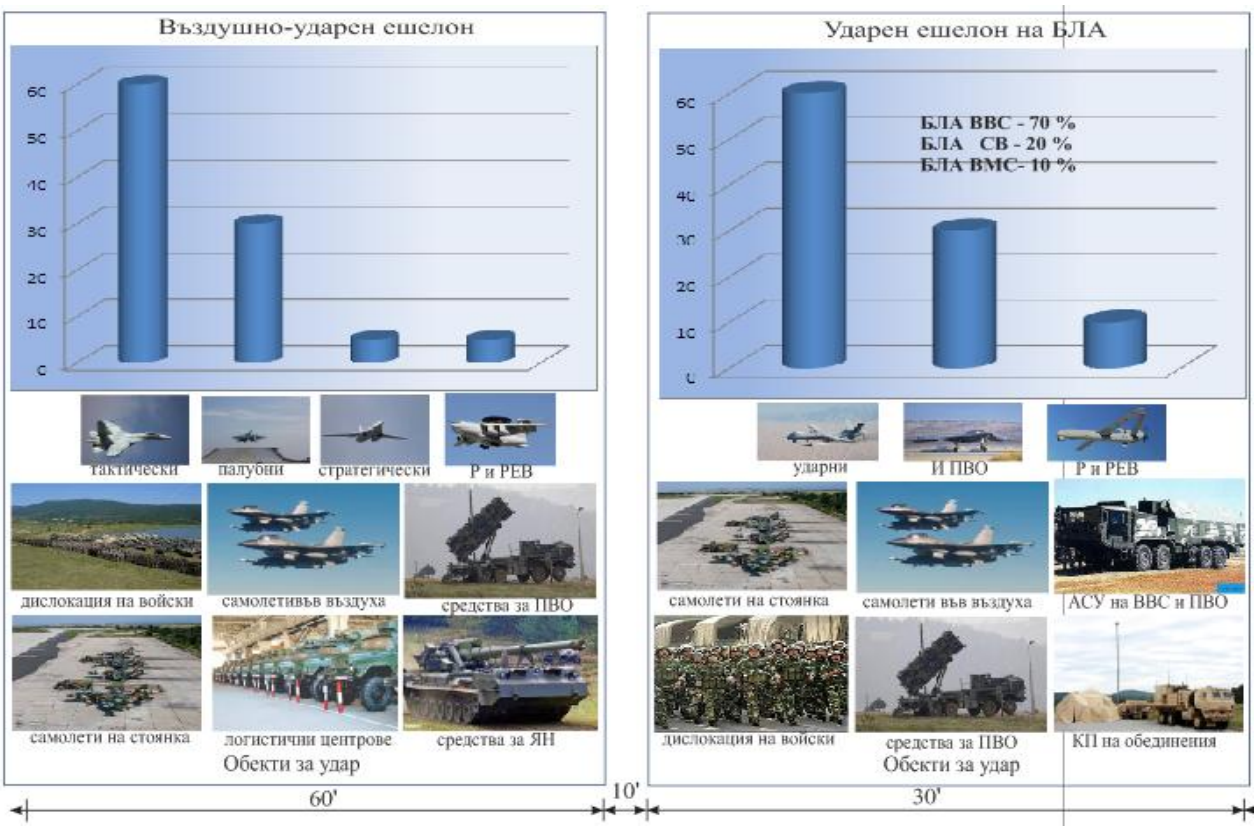
- откриване на РЛС, зенитноракетни комплекси (ЗРК), командни пунктове (КП), пунктове за управление (ПУ) и др. обекти;
- предаване на целеуказване (ЦУ) на ударните БЛА по откритите цели;
- подсвет на цели за авиационните средства за поразяване (АСП) с лазерно насочване;
- унищожаване, в т.ч. и чрез „таран“ на особено важни обекти;
- отвличане на огъня на ПВО (в ролята на лъжливи цели).

Задачата на оперативните и стратегическите БЛА са:

- унищожаване на въздушни и земни цели;
- блокиране на летища;
- патрулиране по линиите за комуникации;
- подавяне на РЛС, средства за свръзка и управление.



Фиг. 4. Структура, състав и обекти за удар на I и II ешелон от МРВУ



Фиг. 5. Структура, състав и обекти за удар на III и IV ешелон от МРВУ

Ударния ешелон на ПА се явява завършващ елемент от построението на МВРАУ. Основните усилия тук са насочени към окончателния разгром на противника и изпълнение на всички задачи на МВРАУ. Предходните ешелони са изпълнили основните задачи по завоюване на превъзходство във въздуха. За унищожаване на неподавени или отново открити средства за ПВО се назначават отделни тактически групи, а изтребителите за прикритие от състава на ешелона следват в общ боен ударните групи и отразяват противниковите изтребители по маршрута на полета и в районите на обектите за удар. Стратегическата авиация (СА) извършва пускове на КРВБ и нанася бомбови удари.

На фиг. 4 и фиг. 5 са показани състава на отделните ешелони и основните обекти за удар на всеки от тях. Такава структура на МВРАУ предполага минимален брой човешки загуби при нарастващо усилие за изпълнение на поставените задачи.

Заключение

При война от шесто поколение се залага на безконтатни методи за водене на военните действия, а дълбочината на нанасяне на ударите с ВТО нараства до цялата дълбочина на ТВД. Построението на МРВУ осигурява изпълнение на задачите с нарастване на усилията. Всеки предшестващ ешелон освен своите специфични задачи изпълнява и такива, осигуряващи следващия. Решаваща роля ще имат хиперзвуковите оръжейни системи, поради факта, че към момента се явяват неуязвими за системите за ПВО и ПРО. Освен това те поемат и основната тежест при намаляване на ракетноядрения потенциал за ответен удар.

References

1. Кацев, И. Анализ на предимствата и недостатъците от използването на мобилни GPS приемници за военни цели, Сборник доклади от Международна научна конференция на факултет „Артилерия, ПВО и КИС" 2017, с. 435-441, 2017, ISSN 2367-7902.

2. Кондратьев, А. Проблемные вопросы исследования новых сетецентрических концепций вооруженных сил ведущих зарубежных стран. Военная мысль, №11, 2009, с. 61-74, ISSN: 0236-2058

3. Макаренко, С., Иванов, М. Сетецентрическая война – принципы, технологии, примеры и перспективы [онлайн] – URL: http://viperson.ru/uploads/attachment/file/950986/Makarenko_Ivanov_-_Netcentric_wars_2018.pdf (прегледан на 11.09.2022)

4. Михайлов, Д. Война будущего: возможный порядок нанесения удара средствами воздушного нападения США в многосферной операции на рубеже 2025–2030 годов. Воздушно-космические силы. Теория и практика, №12, 2019, с. 44-52, eISSN: 2500-4352

5. Остапенко О., Баушев, С., Морозов, И. Информационно-космическое обеспечение группировок войск (сил) ВС РФ: Учебно-научное издание. – СПб.: Любавич, 2012. с. 368

6. Сипченко, В., Системный анализ процессов вооруженной борьбы в конфликтах и войнах в период с 1991 года и по настоящее время. Безопасность Евразии №4 (14), 2003, с. 377-385, ISSN: 1607-7334

7. John warden’s five ring model and the indirect approach to war. Strategic Studies Institute, US Army War Collegehttps [онлайн] – URL: //www.jstor.org/stable/pdf/resrep12025.30.pdf (прегледан на 13.09.2022)

8. Net-Centric Environment Joint Functional Concept, 2005 [онлайн] – URL: http://www.dtic.mil/futurejointwarfare/concepts/netcentric_jfc.pdf (прегледан на 13.09.2022)

9. Richards, C. Boyd’s OODA Loop. Necesse 2020, [онлайн] – URL: https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2683228/Boyds%20OODA%20Loop%20Necesse%20vol%205%20nr%201.pdf?sequence=1&isAllowed=y (прегледан на 12.09.2022)

HYPERSONIC COMBAT AERIAL VEHICLES

Stoyan N. Chanev

Assistant Professor at the Department of Air Defense, Artillery, Air Defense and CIS Faculty at the Vasil Levski National Military University, tel. 054/801040, ext. 54266, e-mail: st.chanev@abv.bg

Annotation: *The report examines the three main types of hypersonic combat aerial vehicles – ballistic missiles, hypersonic cruise missiles and planning warheads. The special features of their construction are shown, as well as their advantages over existing ballistic missile defense.*

Key words: *hypersonic ballistic and cruise missiles, planning warheads, ballistic missile defense.*

ХИПЕРЗВУКОВИ СРЕДСТВА ЗА ВЪЗДУШНО-КОСМИЧЕСКО НАПАДЕНИЕ

Стоян Н. Чанев

Главен асистент в катедра "Противовъздушна отбрана", факултет "Артилерия, ПВО и КИС" на НВУ "Васил Левски", тел. 054/801040, вътр. 54266, e-mail: st.chanev@abv.bg

Анотация: *В доклада са разгледани трите основни типа хиперзвукови средства за въздушно-космическо нападение – балистични ракети, хиперзвукови крилати ракети и планиращи бойни блокове. Показани са особеностите при конструирането им, както и предимствата им над съществуващите системи за противоракетна отбрана.*

Ключови думи: *хиперзвукови балистични и крилати ракети, планиращи бойни блокове, системи за противоракетна отбрана*

Увод

Развитието на средства за въздушнокосмическо нападение (СВКН) винаги е изпреварвало развитието на средствата за противовъздушна отбрана (ПВО) и противоракетна отбрана (ПРО). Това изпреварване може да се компенсирано първо чрез промяна в тактиката на бойното използване на силите и средствата за ПВО/ПРО. При редица зенитноракетни комплекси и системи (ЗРК/ЗРС) в момента на конструирането не са заложени задачи по унищожаване на по-късно възникнали СВКН. Така например след войната в залива срещу Ирак (1990-1991 г.), където за пръв път беше демонстрирано широко използване на високоточно оръжие (ВТО) с приоритет на крилатите ракети (КР), се наложи промяна на тактиката на войските за ПВО – сгъстени бойни редове, ешелониране в дълбочина и повишаване плътността на зенитния огън. Днес задачата по унищожаване на КР, макар и със затруднение е усвоена. С началото на XXI в. започна и бурно развитие на безпилотните летателни апарати (БЛА) с военно предназначение. Последните военни конфликти (Сирия, Либия, Нагорни Карабах, Украйна) нагледно показаха затрудненията пред ПВО при опитите да се неутрализира тази нова заплаха: малки габарити, ниска скорост, ниска себестойност и възможност за групово използване. Ниската ефективност на ПВО се преодолява чрез: организацион-

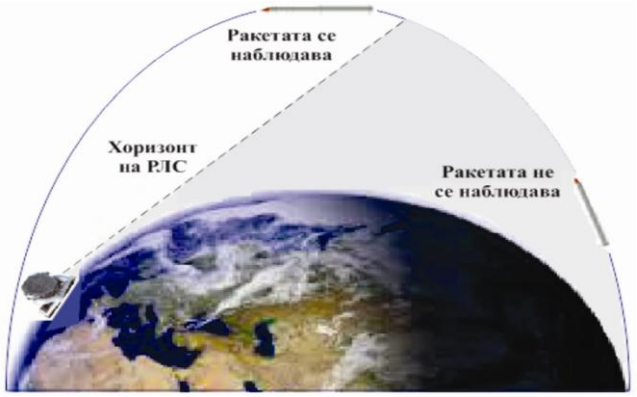
но придаване към системите за ПВО/ПРО на комплекси за близко действие с цел самозащита, използване на боеприпаси с малка себестойност и интегриране на средства за електронна война (EW). Промяната в бойното използване все пак има ограничени възможности. Спечеленото време е необходимо за разработване на сили и средства за ПВО/ПРО от ново поколение, способни да неутрализират заплахата от въздуха в целия диапазон от височини и скорости. Т.к. при война от 5-то поколение (пълномащабна ядрена война) е възможно взаимно унищожение, никоя от държавите не е правила опит да използва масово СВКН на етап на временно технологично превъзходство. По този начин към момента имаме паритет. На фиг.1 е представено хронологично сравнение на противоборстващите сили.

Фиг. 1. Развитие на СВКН и силите и средствата за ПВО/ПРО

1. Необходимост от използване на хиперзвукови (ХЗ) СВКН

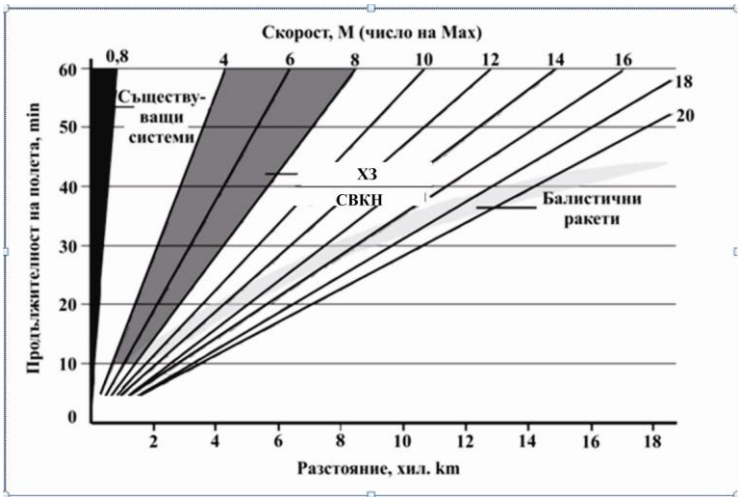
Днес е ясно, че все още един от пътищата за решаване на остри противоречия между държави/блокове е войната като крайно средство. Ядреното сдържане не позволява ескалация на регионалните конфликти, но на дневен ред е разработването и приемане на въоръжение на СВКН с конвенционални (неядрени) поразяващи елементи, които ще позволят нанасянето на изпреварващ „обезоразяващ" удар. Цел на такъв удар приоритетно ще бъдат стратегическото държавно и военно ръководство на противника; центровете за вземане на решения; ракетноядрения потенциал: пунктове за управления (ПУ) и шахтови пускови установки на междуконтинентални балистични ракети (МБР), дислокациите на стратегическата бомбардировъчна авиация и подводния флот [1,6]. По дефиниция такъв „изпреварващ" удар трябва да е състояние да порази целите в рамките на 1 h, независимо от местоположението им [2]. Това условие може да се изпълни само от ХЗ СВКН. За ХЗ се считат тези СВКН, чиято скорост превишава скоростта на звука (M ≈ 331 m/s в атмосферата) няколко пъти (4÷5). МБР и сега са в състояние да развият ХЗ скорост, но извън атмосферата. Това не позволява управляем полет. При навлизане в атмосферата се отделят бойните блокове, които в общия случай са неуправляеми (летят по балистична траектория) и поради съпротивлението на въздуха бързо губят скорост [6]. Тези два факта ги правят непригодни за „обезоразяващ" удар. Ниската точност в съчетание с конвенционални бойни глави не гарантира унищожаването на целта, а ниската скорост на завършващия етап от полета води до уязвимост от системите за ПРО. За да се избегнат тези недостатъци се пристъпва към създаване на ХЗ СВКН, които да са управляеми (полет в атмосферата) и да са в състояние да извършат дълъг висикоскоростен полет (високо челно съпротивление и температура). Височинния диапазон на тези средства се определя от профилираното действие и възможностите на противодействащите сили и средства. Максималната височина на полет на пилотируемата авиация е 20÷25 km и там са съсредоточени

усилията на системите за ПВО/ПРО на театъра на военните действия (ТВД). Полета на МБР е на височини над 140 km и там е акцента на стратегическата ПРО. Ракетите прехващачи тук зависят от момента на откриване ма МБР. Поради линията на хоризонта на РЛС откриването се осъществява от специализирани РЛС, осигуряващи активните средства, които са насочени към възможните траектории на МБР (най кратък път) [3]. От фиг. 2 е видно, че на по-малки височини на полета на ХЗ СВКН точката на откриване ще е много близо до целта, определена за удар и времето за реакция ще е крайно недостатъчно.



Фиг. 2. Развитие на СВКН и силите и средствата за ПВО/ПРО

От величината на достигнатата скорост зависят както продължителността на полета, така и изминатото разстояние. За достигане на междуконтинентални разстояния от ХЗ СВКН и възможност за поразяване на цели в цялата дълбочина на територията на противника е необходимо $V_{ХЗ} > 20\ M$. При по-малки скорости разстоянието намалява и за поразяване на цели в рамките на час ще е необходимо запускането на ХЗ СВКН да е от територия/въздушно пространство/акватория в близост до противника или на ТВД. На фиг. 3 е показана зависимостта на продължителността на полета и разстоянието му от скоростта за различни СВКН [5].



Фиг. 3. Зависимост на продължителността и разстоянието на полета от скоростта

2. Видове ХЗ СВКН

Повишаване на точността при неядрени бойни глави се постига чрез използването на една от следните хиперзвукови системи за големи разстояния: МБР с маневриращи бойни глави (ХЗ МБР); хиперзвукови планиращи летателни апарати (ХЗ ПЛА) осъществяващи планиращ полет на

голямо разстояние; хиперзвукови крилата ракета (ХЗ КР). По същество ХЗ ПЛА и ХЗ КР се явяват бойни комплекси, които в повечето случаи се състоят от две части – носител и ХЗ оръжие.

ХЗ МБР

Точността на съвременните балистични ракети е около 100 m. За да се гарантира поразяване на цел от МБР с бойна глава от конвенционален (неядрен) тип е необходима много по-голяма точност от порядъка на няколко метра. Най-достъпен способ за повишаване на точността е използването на маневриращи бойни глави, снабдени с навигационни системи и аеродинамични управляващи елементи, което позволява управлението на полета им при навлизане в атмосферата.

ХЗ ПЛА

Хиперзвуковата ракетно-планираща система се запуска с помощта на ракета и е така конструирана, че скоро след ускоряващия участък на полета отново навлиза в атмосферата. Тук тя може да преодолее големи разстояния (хиляди km) не заради реактивна тяга, а вследствие на аеродинамически сили.

ХЗ КР

Хиперзвукова крилата ракета – подобно на планера тя създава аеродинамична сила, но по време на полета действа и сила на тягата от хиперзвуков правопоточен въздушно-реактивен двигател (ХПВРД). На по-високи скорости въздухът подаван в двигателя може да остане със свръхзвукова скорост, като този принцип лежи в основата на ХПВРД. За ефективната работа на такива двигатели е необходимо летателния апарат предварително да е развил висока скорост, за което запуска е възможно да се извърши от самолет носител или със специален допълнителен ракетен ускорител [7]. Скоростта на полета на ХЗ КР е чувствително по-малка от ХЗ ПЛА и режима на полета е по-добре изучен. Тук основните трудности са свързани с извънредно високата температура на преминаващия през двигателя въздух – при скорости на ракетата 6М постъпващия въздух може да се нагрее до 1400°С, а реактивната струя (отработените газове) – до 2400°С. При по-големи скорости ситуацията се усложнява допълнително.

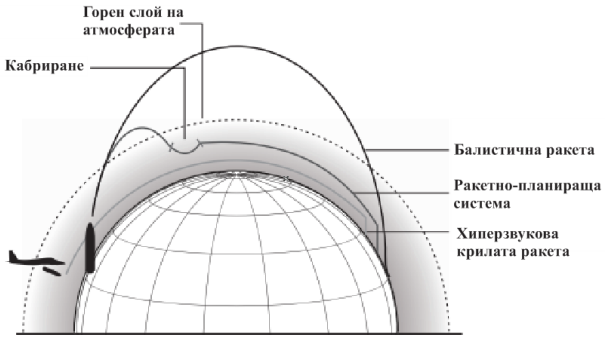
Основните характеристики, които следва да се отчитат при сравняването на ХЗ системи са обхват (междуконтинентален, глобален/неограничен, регионален/на ТВД) и способност за маневриране на средния и крайния участък от траекторията на полета (преодоляване на ПРО и ПВО), които са показани в таблица 1 [5].

Таблица 1

Сравнение на характеристиките на видовете ХЗ СВКН

Характеристика	**ХЗ МБР**	**ХЗ ПЛА**	**ХЗ КР**
По разстояние	*Междуконтинентална*	*Глобална*	*На ТВД*
Способност за маневриране на средния участък на траекторията	*Няма*	*Висока*	*Висока*
Способност за маневриране на крайния участък на траекторията	*Ограничена*	*Средна*	*Средна*

Различните профили на траекториите на полет на ХЗ СВКН (фиг. 4), както и способът за запуск, позволяват наличието на различно време за тактическо предупреждение за използването им. Откриването им може да се осъществи както от сателити (за разузнаване в инфрачервения диапазон), така и от РЛС на системите за предупреждение за ракетно нападение (СПРН). Понастоящем такива развърнати системи притежават САЩ и Русия, а Китай е в процес на създаване.



Фиг. 4. Сравнение на траекториите на полета на видовете ХЗ СВКН

Възможности по откриването, макар и по-ограничени, притежават и някои модифицирани РЛС на системите за ПВО, но само по отношение на ХЗ ПЛА и ХЗ КР, т.к. средният и крайният участък на траекторията им е в атмосферния слой (таблица 2) [5]. Тук е дадено време за тактическо предупреждение, затова е включена балистична ракета за междинни/средни разстояния (БРСР). ХЗ ПЛА се движи с висока скорост в атмосферата и създава плазмен облак, поради което се открива по-рано от сателитите от СПРН.

Таблица 2

Време за предупреждение за удар с ХЗ СВКН

Вид ХЗ СВКН		**ХЗ БРСР**	**ХЗ ПЛА**	**ХЗ КР**
Разстояние до целите [km]		*3500*	*11000*	*1500*
Тактическо предупреждение [min]	Сателити от СПРН	*19*	*33*	*16*
	РЛС от СПРН	*14*	*4*	*11*
	РЛС ПВО	*0*	*3*	*8*

3. ХЗ СВКН, приети на въоръжение

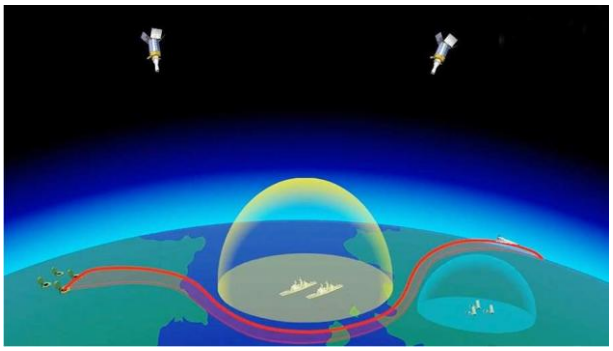
ХЗ ПЛА „АВАНГАРД“

Ракетен комплекс „Авангард“ – включва два основни елемента: МБР (носител) и хиперзвуков планиращ блок. За носител е предвидена МБР УР-100Н УТТХ, а в перспектива ще бъде използвана РС-28 „Сармат“. Полетът на бойния блок се извършва в плътните слоеве на атмосферата, за разлика от традиционните бойни блокове на МБР, които летят към целите по балистична траектория. Разстоянието на полета е междуконтинентално (с обсега на МБР става глобално), а скоростта е хиперзукова (>20 М). По време на полета е в състояние да маневрира по курс и по височина с помощта на аеродинамични и газови кормила. Това позволява да извършва непредсказуеми маневри, оставайки неуязвим за съвременните средства за ПРО, а така също и да обхожда зоната на огъня на зенитните средства (фиг. 5). Траекторията на полета е под минималната височина на прехват на средствата за ПРО, предназначени за борба с МБР до влизане в плътните слоеве на атмосферата. Прехват от средствата за ПРО за близки разстояния е невъзможен поради високата скорост и използването на комплекс от съвременни мерки за противодействие [4]:

– висока скорост (V_{max} = 27 *M* ≈ 33÷37 *km/s*). При такава скорост бойният блок достига до определената цел за минимално време, съкращавайки критично времето за реакция на средствата за ПВО и ПРО на противника;

– нова система за автоматично управление. Изменението на траекторията е в реално време, т.е. тя е непредсказуема и прави блока труден за прехват;

– голям боен радиус (10000 *km*).



Фиг. 5. Траектория на управляемия полет на ХЗ ПЛА „Авангард"

Използването на нови композитни материали и титан, позволява продължителния управляем полет при високи скорости да се извършва в т.н. „плазмен облак". Температурата на повърхността на изделието достига 1600÷2000°C. Предполага се, че „Авангард" е с клиновидна форма с неголеми крила-стабилизатори, разполага се в МБР на мястото на традиционните бойни глави, но габарита му ги надвишава. Оптималния полет на апарата към целта му позволява да запази високата си скорост. В качеството на бойна част може да се използва ядрен заряд със средна или малка мощност, но не трябва да се пренебрегва и възможността за унищожаване на целта за сметка на огромната кинетична енергия (при неядрено снаряжване) – към високата скорост трябва да се добави масата на изделието ≈ 2 t. И в двата случая необходимата бойна ефективност се постига за сметка на висока точност на попаденията [8].

ХЗ КР „Кинжал"

„Кинжал" е авиационно-ракетен комплекс. Носител на комплексът се явява модернизиран за целта самолет МиГ-31БМ (фиг. 6). Типовата бойна скорост в зоната на пуска е в диапазона 2400÷2800 *km/h* на височина 16000÷20000 *m*. Потенциални носители в бъдеще са и Су-57, Ту-22М3 и Ту-160.

ХЗ КР няма официално наименования но редица експерти използват означението название Х-47М2. Траекторията на полета е близка до класическа крива. След пуска ракетата се издига на височина от порядъка на 50 *km*, където двигателя се изключва, след което бойната част се отделя и снижавайки се, без тяга, достига скорост от порядъка на 10 *M*. Управлението се извършва от аеродинамични кормилни повърхности (при тази скорост не са необходими крила). Такава траектория се нарича квазибалистична (или аеробалистична). Насочването се извършва от триосно инерциално навигационно устройство, с корекции по данни на спътниковата система ГлоНаСС или по релефа на местността. По неокончателни данни стартовата маса на Х-47М2 е 4000 kg, масата на бойната част (БЧ) е 480 kg. Максималната постигната скорост при изпитанията е 10740 km/h, което съответства на 10 *M*. Максимално разстояние – 500÷200 km [10].

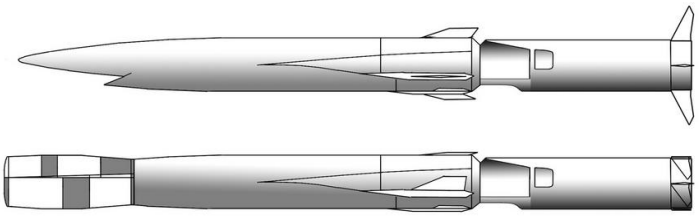
Фиг. 6. Запуск на ХЗ КР „Кинжал" от МиГ-31БМ

Защитата на авиационно-ракетния комплекс„Кинжал" от перспективните средства за ПВО от типа на ЗРК ПВО НАТО MIM-104 Patriot PAC-3 е гарантирана, т.к. ефективното разстояние на стрелбата по свръхзвукови самолети е до 200 *km* и МиГ-31БМ ще изстреля ХЗ КР без да влиза в

зоната му за поразяване. Най-новия американски мобилен комплекс за ПРО THAAD (Terminal High Altitude Area Defense) не работи по въздушни цели, а само по балистични на ТВД. Скоростта на ракетите достига 8,2 *M* (недостатъчна за Х-47М2), а разстоянието на стрелбата до 200 *km*. Единствената ракета отговаряща по скорост и разстояние на ХЗ КР е RIM-161 SM3, но тя е предназначена за стрелба по неманеврират цели.

ХЗ противокорабна ракета (ПКР) Комплекс 3К-22 Циркон – 3М-22

Предполага се, че ракетата е изпълнена по схема "носещ корпус" и се състои от маршева степен със собствени маршеви двигател и стртова-разгонна степен с двурежимен ракетен двигател на твърдо гориво (фиг.7). Конструкцията на маршевата степен е разчетена за нагряване при движение в атмосферата до ≈ 1500 °C.



Фиг. 7. Вероятен изглед на 3М-22 в маршево и стартово положение

На модернизирани ракетни крайцери проект 11442М се предвижда използване на ХЗ ПКР 3М-22 от универсални пускови установки за вертикален пуск УВПУ 3С-14-11442М. Също така се разработват и са изпитани варианти с въздушно, наземно и подводно запускане. Основните ТТХ в противокорабен вариант на ракетата (има и вариант за използване по земни цели) са [9]:

- дължина ≈ 10 *m*;
- разстояние на използване ≈ 450 *km*;
- скорост >8 *M*;
- височина на полета - 28000 *m*;
- времетраене на полета 4,5 *min*.

Заключение

ХЗ СВКН са революционен скок в развитието на средствата за доставяне на ВТО поради неуязвимостта си от всички съществуващи към момента средства за ПВО и ПРО. Високата скорост предоставя и възможност за нанасяне на удари по цялата планета за ограничено време. Това не са само позитиви, т.к. едностранното изпреварващо въвеждане на ХЗ технологии ще доведе до дисбаланс във въоръжаването и възможност да се планира пълномащабен военен конфликт, при който неутрализирането на ядрения потенциал на противника на практика не е гарантирано.

References

1. Кацев, И. Damage functions evaluation coherent to weapon target interaction, International scientificjournal „Machines, Technologies and Materials", 2018, p.124-126, ISSN: 1313-0226

2. Квартальнов, А. Эволюция и перспективы развития концепции быстрого глобального удара / Ред. Е.Г. Чобанян. М.: ПИР-Пресс, 2021. – 41 с. – (Индекс Безопасности– Научные записки) [онлайн] – URL: https://elibrary.ru/download/elibrary_46629733_86607339.pdf (прегледан на 15.09.2022)

3. Макаренко, С., Иванов, М. Сетецентрическая война – принципы, технологии, примеры и перспективы [онлайн] – URL: http://viperson.ru/uploads/attachment/file/950986/Makarenko_Ivanov_-_Netcentric_wars_2018.pdf (прегледан на 11.09.2022)

4. Осьмушкин, В., Тимохович, А. Нововведения в ракетном комплексе „Авангард" актуальные проблемы авиации и космонавтики, Красноярск, 13–17 апреля 2020 г., с.: 201-202

5. Acton, J. Silver bullet?. Carnegie Endowment for International Peace, 2013 [онлайн] – URL: https://carnegieendowment.org/files/cpgs.pdf (прегледан на 14.09.2022)

6. Ballistic and cruise missile threat. Defense intelligence ballistic missile analysis committee [онлайн] – URL: https://irp.fas.org/threat/missile/bm-2020.pdf (прегледан на 14.09.2022)

7. Soaring at Hypersonic Speeds. 2015 Status of High Speed Air Breathing Propulsion by Dora E. Musielak, PhD and Bayindir H. Saracoglu PhD [онлайн] – URL: https://silo.tips/download/soaring-at-hypersonic-speeds (прегледан на 15.09.2022)

8. https://iz.ru/715170/nikolai-surkov/giperzvukovoi-avangard (прегледан 14.09.2022)

9. http://militaryrussia.ru/blog/topic-718.html (прегледан 14.09.2022)

10. https://naukatehnika.com/vks-rossii-prinimayut-giperzvukovyie-raketyi-kinzhal.html (прегледан на14.09.2022)

INTERCONTINENTAL BALLISTIC MISSILE COUNTERFORCE AGAINST BALLISTIC MISSILE DEFENSE SYSTEMS

Stoyan N. Chanev

Assistant Professor at the Department of Air Defense, Artillery, Air Defense and CIS Faculty at the Vasil Levski National Military University, tel. 054/801040, ext. 54266, e-mail: st.chanev@abv.bg

Annotation: *The paper presents a complex of measures to counterforce intercontinental ballistic missiles from Ballistic Missile Defence (BMD) at various stages of their flight, including up to launch. The following main courses were considered - basing, flight trajectory, false targets, radio-electronic countermeasures, striking elements.*

Key words: *intercontinental ballistic missiles (ICBMs), counterforce from mobile and silos based Ballistic Missile Defence (BMD), false targets, warheads.*

ЗАЩИТА НА МЕЖДУКОНТИНЕНТАЛНИ БАЛИСТИЧНИ РАКЕТИ ОТ СРЕДСТВАТА ЗА ПРОТИВОРАКЕТНА ОТБРАНА

Стоян Н. Чанев

Главен асистент в катедра "Противовъздушна отбрана", факултет "Артилерия, ПВО и КИС" на НВУ "Васил Левски", тел. 054/801040, вътр. 54266, e-mail: st.chanev@abv.bg

Анотация: *В доклада са представени комплекс от мерки за защита на междуконтинентални балистични ракети от противоракетната отбрана (ПРО) на различни етапи от полета им, включително до старта. Разгледани са следните основни направления – базиране, траектория на полет, лъжливи цели, радиоелектронно противодействие, поразяващи елементи.*

Ключови думи: *междуконтинентални балистични ракети, противодействие на ПРО, мобилно и шахтово базиране, лъжливи цели, бойни блокове.*

Увод

Междуконтиненталните балистични ракети (МБР) са един от трите стълба на ядреното въоръжение, наред с подводните атомни ракетоносци и носителите на ядрено оръжие от стратегическата бомбардировъчна авиация. Използването им е от голяма дистанция, което ги прави уязвими от съществуващите системи за противоракетна отбрана (ПРО) поради относително голямото време за реакция. За преодоляването на този недостатък те се нуждаят от комплекс от технически решения и организационни мероприятия повишаващи устойчивостта им. Такива решения са възможни на всеки един етап от полета им: до старта; на активния участък; в средния участък на полета, протичащ извън атмосферата и в крайния участък при навлизане в атмосферата. В начал-

ния и крайния участък МБР могат да бъдат поразени и от развърнати мобилни системи за ПРО, а извън атмосферата – от специализирани балистични ракети въоръжени с бойни блокове с дистанционно взривяване (с ядрена бойна глава или конвенционална) или контактни такива.

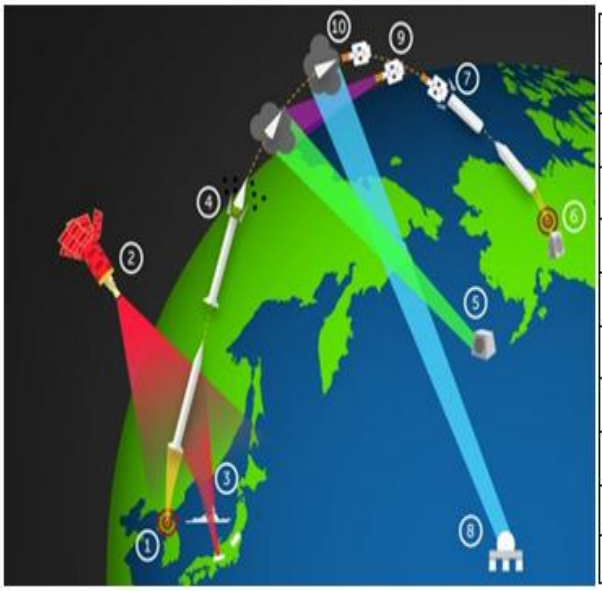
1. Принцип на функциониране на система за ПРО

САЩ са световен лидер в изграждането на системи за ПРО, като елементите на тези системи са със земно, морско, въздушно и космическо базиране. Към момента е завършена регионалната система за ПРО (но тя е насочена към отразяване на ракетно нападение от една посока – през северния полюс, като най кратък път). Стремежът е да се изгради глобална система, но за целта е необходимо разполагане и активиране на елементи на територията на съюзни държави. До въвеждането на глобалната система на въоръжение потенциалните заплахи извън регионалния обхват ще се неутрализират от съществуващи мобилни модули със земно и морско базиране, способни да се дислоцират в застрашения район. Такива мобилни системи /The Aegis Ballistic Missile Defense - морски компонент на системата, Terminal High Altitude Area Defense (THAAD)- предназначен главно за защита на войски и обекти на театъра на военни действия (ТВД)/ са предназначени за защита от балистични ракети със среден и малък обхват и имат ограничени възможности за противодействие на междуконтинентални балистични ракети (МБР) – главно на началния (активния) и крайния участък на траекторията им. За успешното функциониране е необходимо използването на единна система за командване, контрол, наблюдение и комуникация [4, 5]. Поради тази причина дори унищожаването на МБР на средния етап от траекторията над територията на САЩ е зависимо от множество изнесени/и мобилни елементи (фиг. 1)

Фиг. 1. Разположение на елементите на система за ПРО [9]

На фиг. 2 е представено функционирането на Ground-based Midcourse Defense (GMD) - наземно разположената система за ПРО, предназначена да поразява МБР на средния участък на траекторията им. Елементи на системата се явяват [8, 9, 10]:

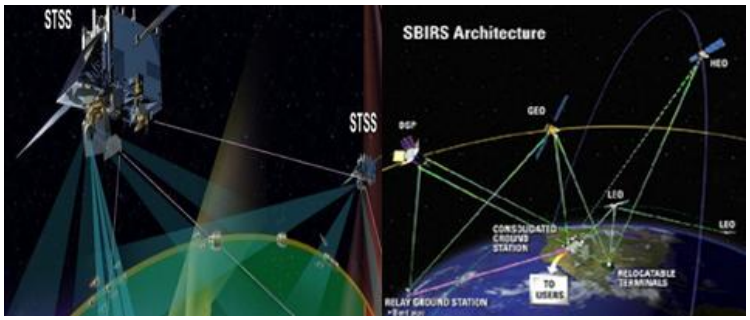
Space Tracking and Surveillance System (STSS) е космическа система, разработена и управлявана от Агенцията за противоракетна отбрана (MDA), която открива и проследява балистични ракети (интегрирането на тази система е на експериментална фаза).



Етапи на реализация на прехващането	
1.	Заплаха от изстрелване на ракета
2.	Сателитите от SBIRS регистрират изстрелването
3.	Предно базираните (изнесените) радари проследяват траекторията на полета на ракетата
4.	Ракетата отделя бойните глави и примамките (облачна заплаха)
5.	Наземно базираните радари проследяват облачната заплаха
6.	Изстрелване на наземно базиран прехващач (GBI)
7.	Кинетичната глава (EKV) се отделя от прехващача
8.	Морско базираните X-band радари (SBX) следят облака от цели и опитват да отсяват лъжливите цели
9.	EKV открива облачната заплаха
10.	Прехващане на бойния блок

Фиг. 2. Етапи на прехващането на МБР от GMD[9]

Space-based Infrared System (SBIRS) е съвкупност от интегрирани сателити в геосинхронна орбита, висока елиптична орбита, наземни центрове за обработка на данни и командване и контрол. Осигурява ранно предупреждение за изстрелване на балистични ракети и да поддържа осведоменост за бойното пространство. В най-общ вид архитектурата на STSS и SBIRS е показана на фиг. 3.



Фиг. 3. STSS и SBIRS

Предно базирани (изнесени) радари (фиг. 4):

AN/SPY-1 е многофункционален 3D радар с фазирана решетка, който предоставя данни за търсене, откриване, проследяване и разделяне на въздушни и надводни цели. Това е основният радар за управление на огъня за бойната система Aegis, с която са оборудва както корабите Aegis, и регионалните системи Aegis Ashore, разположени в Румъния и Полша (в процес на развръщане).

AN/TPY-2 (Army-Navy Transportable Radar Surveillance) е мобилен радар с висока разделителна способност, работещ в X-band диапазон, разработен заедно със системата за отбрана от балистични ракети THAAD.

Фиг. 4. AN/SPY-1 и AN/TPY-2

Наземно и морско базирани радари (фиг. 5).

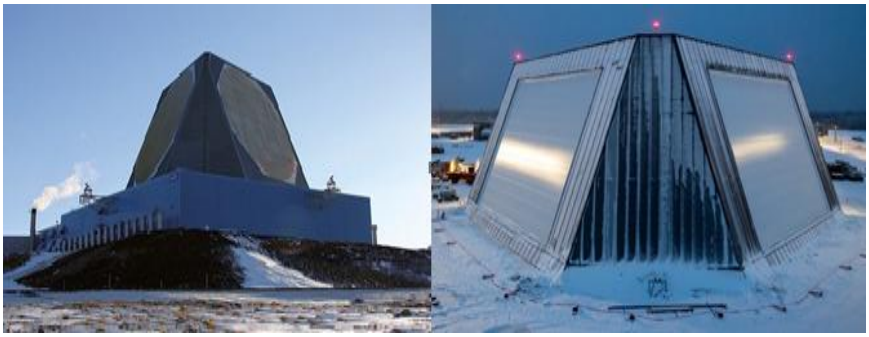
Cobra Dane Radar е радар работещ в L- band диапазон, разположен на остров Shemya , Аляска. Диаметъра на антената е 29 m и осигурява азимутно покритие на 136 градуса. Може да открива обекти на разстояние до 2000 мили и предоставя данни за проследяване и класификация на ракети, достатъчно точни, за изстрелването на прехващачи и актуализиране на данните на целта по време на полет на прехващача.

Sea-Based X-band Radar (SBX) е разположен върху изведена от експлоатация морска платформа в Северно море. Притежава висока разделителна способност и главното им предназначение е да отсеят бойните блокове на МБР от лъжливите цели след отделянето им в общ „облак на заплахата“.

Фиг. 5. Cobra Dane Radar и SBX

Upgraded Early Warning Radars (UEWR) – имат 240÷360° покритие и служат за космическо наблюдение и сателитно проследяване и са в състояние да открият атака/и с МБР (фиг.6).

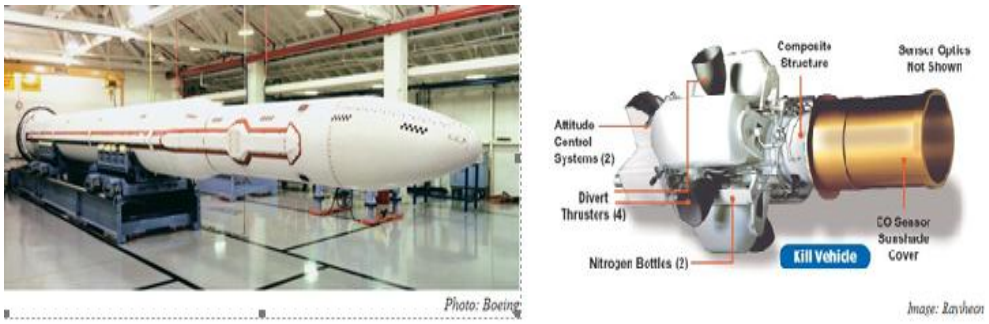
Long Range Discrimination Radar (LRDR) – предназначен за прецизни метрични данни с цел отделяне на бойните блокове на МБР като цели на фона на примамките и лъжливите цели (фиг. 6).



Фиг. 6. UEWR и LRDR

Ground-based Interceptor (GBI) – разположени са в ШПУ и са предназначени да прехващат МБР извън атмосферата в най-високия участък от траекторията на полета им. Имат кинетична бойна част.

Exoatmospheric Kill Vehicle (EKV) – предназначени да унищожават бойни глави на МБР чрез пряк контакт, с помощта на високата кинетична енергия (висока скорост)



Фиг. 7. GBI и EKV

2. Защита на МБР от ПРО

Защита до старта на МБР

Еволюцията на защитата до старта на МБР е в пряка връзка с развитието на технологиите, включително усвояването на космоса за военни цели. При настъпателна ПРО операция обект за удар ще бъдат стратегическите ракетни войски на местата за дислокацията им.

Първоначалните варианти на МБР стартират от открити стартови площадки. За предпазване от противниковото оптикоелектронно разузнаване се извършва маскировка (слабоефективна), която е много трудоемка – височинна и във всякакви условия на обстановката. Това в съчетание с опасността от унищожаване от изпреварващ ядрен удар (основна цел за който се явяват МБР до изстрелването им) налага базирането да е в ШПУ (фиг. 8). Оборудването на шахтите е специализирано и осигурява оцеляване на МБР в условията на ядрен взрив. За управление на група ШПУ се предвижда един команден пункт (КП), разположен във видоизменено ШПУ [2].

Фиг. 8. ШПУ

С повишаване точността и мощността на изпреварващия удар се оказва, че с едно попадение може да се изведе от строя целия комплекс за групов старт. Това налага разсредоточаване на ШПУ и използването на автономни КП изключващи поразяване на повече от един елемент с една ракета. Такъв единичен шахтен комплекс се състои от 6 ШПУ разположени на 8÷10 km една от друга и дистанционно управляеми от един КП. Т.к. такива съоръжения, особено на етапа на изграждането им е трудно да бъдат скрити от сателитното разузнаване се пристъпва към изграждане на повече от необходимите ШПУ, като не всички са заредени с МБР, освен това периодично се извършва ротация.

Появата на високоточни управляеми бойни блокове и на конвенционални оръжия с висока скорост (оттам и висока кинетична енергия) застрашават боеготовността на шахтно базираните МБР, поради вероятността от деформация на капаците на ШПУ и компрометиране на старта. Отговора се намира в използването на МБР с ракетни двигатели на твърдо гориво, които поради своята компановка и размери са подходящи за разполагане на автомобилни шасита. Високата мобилност се постига чрез патрулиране по маршрути в определени райони и изстрелване на МБР

от предварително подготвени стартови позиции (СП), където се извършва и предстартовата подготовка.

С въвеждане в експлоатация на сателити за радиолокационно разузнаване със синтезирана апертура (SAR) откриването на мобилните установки вече не е проблем. Те са способни да формират изображения на земната повърхност с разделителна способност 1 m и извършват обиколка на планетата за 90 минути. За наблюдение на целия район за патрулиране са необходими 10÷12 часа.

Поредното предизвикателство е преодоляно чрез създаване на високо мобилни комплекси, патрулиращи в обширни райони, с автоматизиране на предстартовата подготовка и възможност за пуск на МБР без заемане на предварително подготвени СП (с помощта на глобална навигационна спътникова система ГЛОНАСС). За МБР „Топол" района за патрулиране е с площ 125000 km^2, а изстрелването се извършва за по-малко от 2 минути след подаване на команда от която и да е точка по маршрута (фиг.9). Трудността за свързване на КП с мобилните установки поради влияние на релефа на местността в района за патрулиране е решена по два начина: с използване на КП с подобрени характеристики и с командна ракета [1].

Фиг. 9. Хангари за МБР „Топол" и мобилни установки по маршрут за патрулиране

Друг подход за използване на високомобилни МБР е създаването на бойни железопътни ракетни комплекси (БЖРК) [6]. Идеята е да се маскира разположението им като се влеят в потока от влакови композиции движещи се по цялата територия на страната. Такъв БЖРК е „Молодец" (РТ-23 УТТХ), от които 12 броя са въведен на въоръжение в периода 1985÷1994 г. Причина за свалянето му от въоръжение са редица експлоатационни трудности и демаскиращи признаци. Поради голямата тежест се движи само по модернизирани жп линии, подсилени с бетонни траверси. Движещата сила е от три локомотива, но за разлика от гражданските композиции единият е в края на състава. Преди изстрелването на МБР, специално устройство е необходимо да отведе контактната мрежа встрани. Освен това е необходимо преди изстрелването да пристигне в специални точки по маршрута за топопривързване.

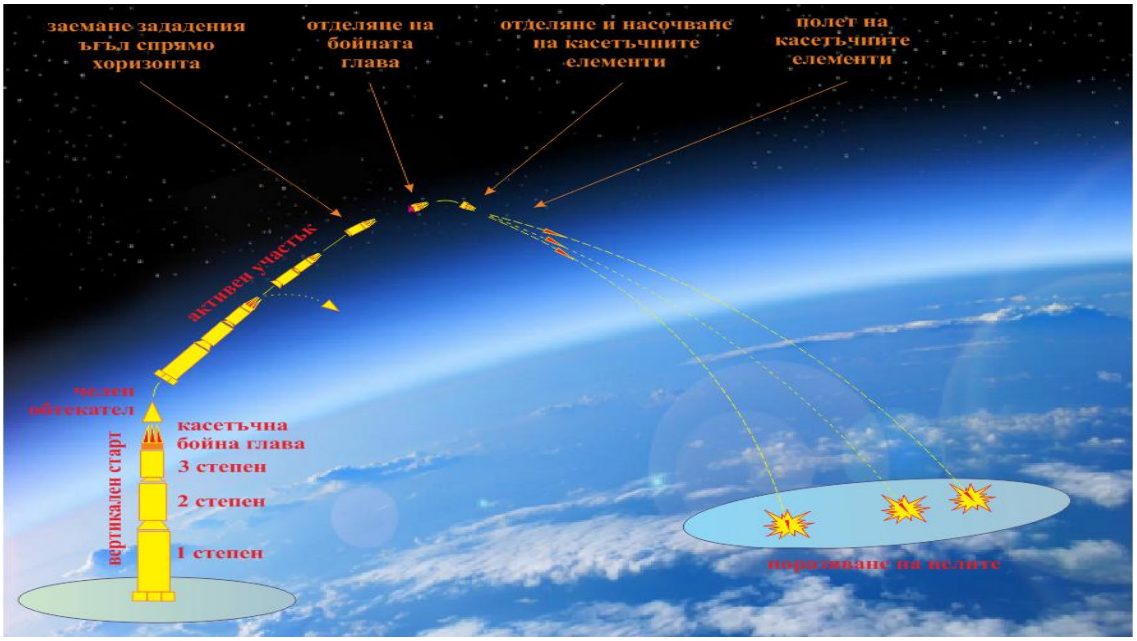
Фиг. 10. БЖРК „Молодец по маршрут и в бойно положение

От 2015 г. постъпва информация за възстановяване на дейностите по въвеждане в експлоатация на съвременен БЖРК в отговор на развитието на системите за ПРО. Предполага се, че БЖРК „Баргузин" ще преодолее недостатъците на предшественика си чрез редица нововъведения – помалка БР, използване на ГЛОНАСС, съвременни елементи на жп състава (фиг.11).

Фиг. 11. Перспективен БЖРК „Баргузин“ [6]

Защита на МБР от ПРО по време на полета.

На фиг. 12 е представена обща схема на конструкцията и траекторията на полета на МБР.



Фиг. 12. Полет на МБР

Траекторията на полета се разделя на активен участък (до отделяне на втората степен), среден участък (изцяло извънатмосферен) и краен/терминален участък (обратно навлизане на поразяващите елементи в атмосферата). При МБР от по-старо поколение първия участък е с продължителност 5÷8 минути, около 5 минути са необходими за отделяне на бойните глави, т.к. всяка от тях трябва да се отдели в точно определен момент за да порази по балистична траектория определената цел. В този интервал от полета (≈ % 40 от целия полет) МБР са най-уязвими. Съкращаването продължителността този участък в съвременните ракети се постига чрез:

- използване на квазибалистична траектория. При МБР максималната височина на полета е 1/10 от далечината на полета, те. 800÷1000 km. Топол-М“ е с квазибалистична, т.е. различна от

класическата балистична, а началния й участък преминава основно през плътните слоеве на атмосферата, като отделянето на бойната глава може да стане непосредствено след излизане от тях (над 150 km). Продължителността на активния участък от полета е намалена до 3 минути. Това значително скъсява и разстоянието за откриване от РЛС, съответно и времето за реакция на системата за ПРО. За да се намали вероятността за прехващане на активния участък, "Топол-М" извършва, макар и ограничено, маневриране с помощта на спомагателните ракетни двигатели на първата степен [3];

- използване на Multiple Independently targetable Reentry Vehicle (MIRV) – касетъчни елементи, летящи извън атмосферата, с индивидуално насочване на всяка бойна глава. Отделянето на бойните глави става едновременно, а след това те коригират позицията си чрез собствена двигателна тяга, така, че касетъчните елементи да се насочат по балистична траектория към зададената цел [7].

При 10÷15 MIRVs на носител, преодоляването на ПРО от част от масирания удар с МБР гарантира взаимно унищожение или поне неприемливи поражения. Това са и двата подхода при съвременните ракети – такива с по-малко бойни глави, но с предимства в траекторията на полета или тежки МБР с повече поразяващи елементи.

Защита на МБР чрез лъжливи цели.

За защита на бойните глави на МБР от прехващане се използват лъжливи цели [1]. Заедно с бойните блокове те образуват сложна балистична цел („облак на заплахата"), принуждавайки системата за ПРО да отделя ресурси и време за отсяване на целите. Подразделят се на леки, квазитежки и тежки,

Леки лъжливи цели – надуваеми балони с метализиран външен слой, които се сгъват и стотици от тях се поставят в бойната глава. Преди разпръскване се надуват и се изхвърлят, създавайки стотици лъжливи отметки на екраните на РЛС, маскирайки по този начин истинската цел. Друг вариант на такава защита е използването на стотици хиляди малки отрязъци проводници – диполни отражатели, които се разпръскват около бойната глава и предизвикват същия ефект. С навлизането в горните слоеве на атмосферата балоните и диполните отражатели изостават и губят защитните си свойства.

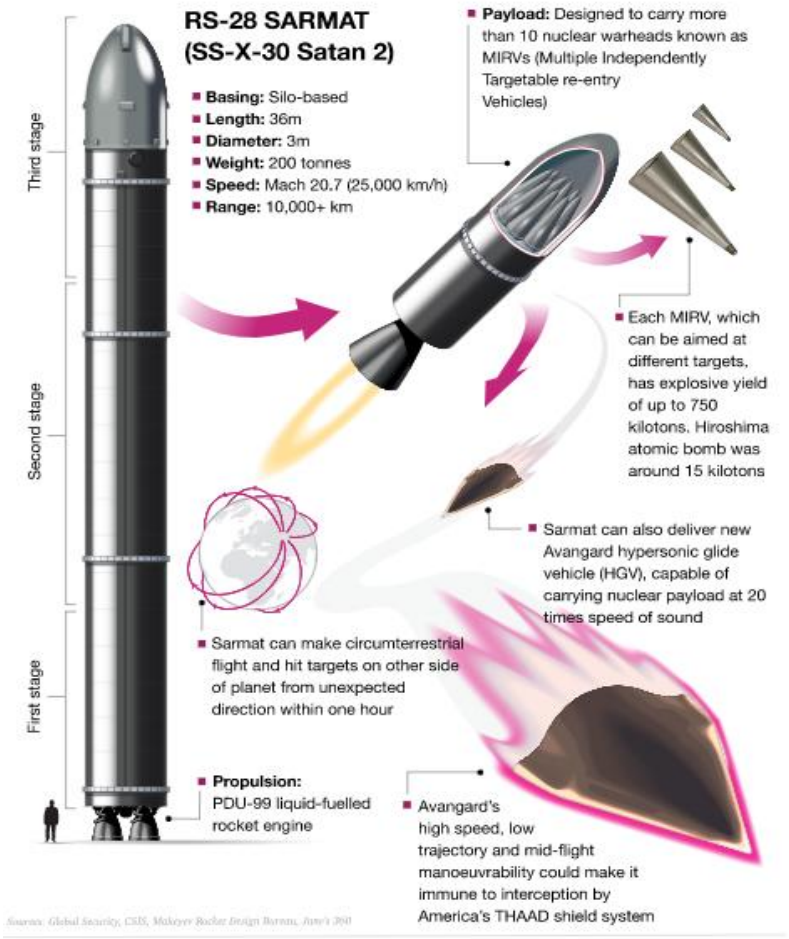
Квазитежки лъжливи цели – с форма на миниатюрна ракета и не изостават от бойната глава по време на полета и не изгарят в плътните слоеве на атмосферата.

Тежки лъжливи цели – разполагат се в касети и се монтират на определени места в бойната глава. Изстрелването им се извършва с барутни заряди.

Освен пасивни лъжливи цели се създават и средства за излъчване на електромагнитни трепетения, както и използване на радиопоглъщащ материал върху бойната глава с цел смущаване работата на земно базираните РЛС за ранно предупреждение.

Защита от електромагнитен импулс (ЕМИ) при ядрен взрив – чрез използване на външно защитно покритие на корпуса, на устойчиви на ядрено въздействие градивни елементи в системата за управление, отделна защита чрез специално покритие на секцията, в която се монтира системата за управление и специална екранировка на кабелните мрежи.

Последната тежка МБР, с шахтово базиране РС-28 „Сарамат" [11] е с редица предимства пред системите за ПРО (фиг. 13) – възможност да атакува целта от всяко направление, хиперзвукова скорост над 20 *M*, както и възможност за въоръжаване с бойна глава от типа Maneuverable Reentry Vehicle (MARV) – планиращ хиперзвуков управляем боен блок.



Фиг. 13. Способи за преодоляване на ПРО от РС-28 „Сарамат" [11]

Заключение

Съвременните МБР разполагат с разнообразни способи (в зависимост от своята конструкция и предназначение) за защита от ПРО. Преодоляването на системата за ПРО на 10 % от целия състав на масирания удар е в състояние да нанесе неприемливи щети. Въвеждане на въоръжение на МБР с бойни глави от типа MARV изисква противодействие от глобална система за ПРО и наличие на прехващачи, способни да поразяват хиперзвукови поразяващи елементи. Тази задача, освен че не е решена технически, е и финансово непосилна за момента.

References

1. Гергинов, Г. Балистични стратегически, С. 2016
2. Евдокимов В. Защита шахтных пусковых установок. Защита и безопасность № 2 (73), 2015, с. 27-28, ISSN: 2075-9924
3. Каракаев, С. Ракетные войска стратегического назначения современной России [онлайн] – URL: https://elibrary.ru/download/elibrary_41829627_83305947.pdf (прегледан на 16.09.2022)
4. Кацев, И. Damage functions evaluation coherent to weapon target interaction, International scientificjournal „Machines, Technologies and Materials", 2018, p.124-126 ISSN: 1313-0226
5. Макаренко, С., Иванов, М. Сетецентрическая война – принципы, технологии, примеры и перспективы [онлайн] – URL: http://viperson.ru/uploads/attachment/file/950986/Makarenko_Ivanov_-_Netcentric_wars_2018.pdf (прегледан на 11.09.2022)

6. Толстиков, В. Боевой железнодорожный ракетный комплекс: история и перспективы [онлайн] – URL: https://elibrary.ru/download/elibrary_34946725_32031381.pdf (прегледан на 16.09.2022)

7. Торжевский, И., Олейников, Е. Анализ ракетных комплексов и тенденции развития РВСН России [онлайн] – URL: https://elibrary.ru/download/elibrary_44788026_63423440.pdf (прегледан на 17.09.2022)

8. Missile Defense Project, "Sensors," *Missile Threat*, Center for Strategic and International Studies, June 14, 2018, last modified June 7, 2021, https://missilethreat.csis.org/system/sensors/. (прегледан на 15.09.2022)

9. Missile Defense Project, "Ground-based Midcourse Defense (GMD) System," *Missile Threat*, Center for Strategic and International Studies, June 14, 2018, last modified July 26, 2021, https://missilethreat.csis.org/system/gmd/ (прегледан на 15.09.2022)

10. Missile Defense Project, "Interceptors," *Missile Threat*, Center for Strategic and International Studies, March 3, 2021, last modified August 3, 2021, https://missilethreat.csis.org/system/interceptors/ (прегледан на 15.09.2022)

11. https://www.news.com.au/technology/innovation/military/sign-putin-could-use-russias-nuclear-weapons-on-ukraine/news-story/ea5c01da565485e9210e372aa38a11c5 (прегледан на 18.09.2022)

METHOD FOR HAZARD ANALYSIS IN INDUSTRIAL ACCIDENTS

Hristo A. Desev

National Military University "V. Levski", Artillery, "Air Defense and CIS" Faculty
Shumen, "K. Scorpil"str. № 1

Abstract*: Civilization is faced with the contradiction of the technologies used and the threat they pose to life, human health and the environment. The presentation characterizes the sources of threats and proposes an order for the analysis of potential risks from man-made events. Organizational measures for the management of occupational risks and safety in enterprises have been optimized. The procedure for the analysis of the functioning of the industrial safety management system, development and implementation of corrective measures aimed at eliminating the identified inconsistencies;*

Key words: *risk, organizational measures*

МЕТОД ЗА АНАЛИЗ НА ОПАСНОСТИТЕ ПРИ ПРОМИШЛЕНИ АВАРИИ

Христо А. Десев

Актуалността на проблема с поддържането на безопасността в съвременния етап нараства пропорционално с неравномерното развитие на технологичните производства и прилагането на традиционни методи за тяхното потребление. Цивилизацията се сблъсква с противоречието на използваните технологии и заплахата, която представляват те за живота, здравето на хората и околната среда.

Авариите в съвременната техносфера са сравними с колосалните природни катастрофи и разрушителните последствия от въоръжените конфликти. В световен мащаб се счита, че загубите от аварии и посттравматизма достига до 10-15% от националния продукт на развитите страни, а екологичните последствия върху околната среда довеждат до летален изход на 20-25% от населението.

Основните причини за спешните ситуации според статистиката на произшествията са възникналите в съоръженията на индустрия аварии от незадоволителното състояние на техническото устройства, сгради, структури, несъвършенство на технологиите или конструктивни недостатъци, нарушение на работната технология и грешките в персонала.

Основните причини за опасните промишлени ситуации с голяма потенциална опасност подлежат на анализ и могат да характеризират производствените процеси със затруднения. Този факт се определя от отсъствието от аналитична количествена оценка на опасностите от технологичните процеси и производство.

Натрупаните проблеми показват, че трябва да се разработи подходящ математически апарат, анализ на данните за опасности, формиране на показатели, характеризиращи тежестта на произшествията и съответните методи за тяхната оценка.[2]

Тъй като всяка авария се определя от първоначалните събития, начина за протичане и последствията, основният показател за опасността от повреди в оборудването се явява риска. За да се използва правилно риска е необходима оценка за несигурността в неговото определяне.

Източниците на несигурност в количествения анализ на риска са:

1. Непълно признаване на основни опасности;

2. Екстраполирането на данни води до факта, че те могат подведат анализа и да не регистрират опасности при преминаване към оборудване с по-големи размери;

3. Ограничения на теорията на „дърветата на отказите“ за опростяване на системата;

4. Непълнота на анализа на честотата, с използване на метода „дървета на отказите и събития“;

5. Неопределеност в изходните данни;

6. Данните могат да бъдат неточни, непълни или непоследователни на реалностите.

Освен това, когато оценява вероятността от нежелано събитие, не се отчитат индивидуални характеристики на оборудването (материал, метод за производство, условия за работа, местоположение на индустриалната площадка и т.н.) стойността и е еднаква за еднакъв тип оборудване.[1]

При съществуващите принципи на поставянето на технологично оборудване, когато един и същ тип устройства се комбинират в блокове (топлообменници, електрически дехидратори, колони) е важно да се отчита възможността за възникване на ефекта на "доминото." Всеки апарат от обекта на изследване може да бъде източник на ефекта „домино“ и да участва в неговото развитие.

Опасността от оборудване от степента на влиянието му върху по -нататъшното развитие на аварийната ситуация на основа на обобщен интегрален параметър (ОИП). ОИП се определя като сумата от отделни интегрирани параметри на устройства, разположени в зоните с максимални влияния на вредните фактори на спешни ситуации, които се разглеждат.

За обективна и пълна оценка на текущото състояние на СТС от гледна точка на опасността, която тя представлява, е подход, който покрива идентифициране на всички възможни източници на опасност, тяхното класиране и анализ.

Основната задача на етапа на идентифициране на източниците на опасност е разкриването и ясното описание на всички присъщи за системата опасности.

В същото време механизмите за появата и развитието на произшествието като правило, има сложни сценарии, включващ различни видове събития, аварийни ситуации при това броят на възможните сценарии може да достигне няколко хиляди. Определено е, че най -често се наблюдават пожари (разливи и "кълбовидни взривове"), експлозии (детонационни и дефлаграционни) и емисии от токсични вещества.

В предприятията с наличието на опасни производствени съоръжения се създават системи за управление на индустриалната сигурност (СУИС) и корпоративни системи за управление на охрана на труда и промишлена безопасност и системи за управление на околната среда в индустрията (СУОСИ).[2]

В контекста на пазарната икономика и регулиране в областта на индустриалната безопасност, защита при спешни ситуации, защита на труда и развитие на околната среда и системите за промишлена сигурност е спешна задача за преработка на нефт и газ, въглища, добив, химически, металургични и други индустрии, които управляват опасни производствени съоръжения.

Системата за управление на индустриалната сигурност е механизъм, за осигуряване на непрекъснат и целенасочен процес на въздействие върху индустриална безопасност включително комплекс от правни мерки, организационни, технически, икономически, информация, образование, насочена към предупреждение, превенция и ликвидация на аварии в съоръжения за опасни производства.[3]

Според това определение документацията на СУИС трябва да съдържа:

- политиката на експлоатационните организации в областта на промишлеността;
- регулиране на системата за управление на индустриалната безопасност;
- регулиране на контрола на производството върху спазването на изискванията за промишлена безопасност в опасните производствени съоръжения;
- документи за планиране на мерките за намаляване на риска от злополуки в опасни производствени съоръжения;

За успешното регулиране на системата за управление на индустриалната безопасност организациите трябва да поддържат следната информация:

- задачите на опериращите организации в областта на индустриалната сигурност;
- описание на структурата на системата за управление на индустриалната безопасност и нейното място в общата система за управление на експлоатиращата организация;
- списък на съоръжения за опасни производства, за които засягат работата на системата за управление на индустриалната безопасност;

Фиг. 1. Последователност на анализа

- функциите, правата и задълженията на ръководителите на операционните организации в областта на индустриалната сигурност;
- процедурата за провеждане на консултации със служители от опасните производства обекти и техните представители относно осигуряването на сигурност;
- организацията на ресурсното осигуряване;
- процедурата за планиране на дейностите в рамките на системата за управление на индустриалната безопасност и списък на планиращите документи за повишаване на мерките за намаляване на риска;
- процедурата за анализа на функционирането на системата за управление на индустриалната безопасност, развитие и прилагане на коригиращи мерки, насочени към премахване на идентифицираните несъответствия;
- организация на информационната поддръжка в рамките на системата за управление индустриална безопасност;
- процедурата за провеждане на пригодно обучение и сертифициране в зоната на индустриалната безопасност на мениджъри и служители;
- процедурата за провеждане на обучение и тестване на знанията на служителите;
- процедурата за работа с договарящи организации, които извършват дейности в съоръженията с опасно производство;
- осигуряване на сигурността на експерименталното приложение на техническото устройства;
- процедурата за идентифициране на опасности и оценка на риска при аварии.

Основните цели и цели на СУПБ са осигуряване на безопасна работа на съоръженията за опасно производство, предотвратяване на наранявания, злополуки и инциденти. Нейната ефективност зависи от осигурените от организацията ресурси(човешки ресурси, знания и опит, технологии и финансови средства)

Организацията трябва да установи и поддържа в актуално състояние процедурите за идентифициране на възможността за бедствия и аварийни ситуации и реакция за тях, както и превенция и омекотяване на влиянията върху околната среда.

Организацията трябва да анализира и преразгледа в случай на необходимост, процедури относно готовността си за реакция на спешни ситуации, особено след възникване на бедствието.

Организацията трябва да установи и поддържа в работно състояние документираните процедури за мониторинг и измерване на основните параметри и характеристики на операциите и дейностите

Разработването и използването на една или повече програми е ключов елемент за успешното внедряване на система за управление на околната среда. Програмата трябва да опише как ще бъде постигната цели и планирани показатели за околната среда на организацията, включително срокове и персонал, отговорен за прилагането на политиката на околната среда на организацията

Формирането на механизми за осигуряване и управление на професионалните рискове в рамките на разглежданите системи се постига чрез въвеждането на процедури, регулиращи дейността на персонала във всеки елемент. [4]

Контрола на системата се осъществява от работодателя. Той трябва да гарантира контрола на функционирането на системата за управление на професионалния риск чрез изпълнение на процедурите за мониторинг и вътрешен одит на системата.

Процедура за мониторинг в системата за управление включва качествени и количествени измервания и оценки на състоянието на изпълнение на изискванията на регламента, извършено с цел за получаване на информация за състоянието и ефективността на работата на системата

Мониторингът трябва да включва следните основни елементи:

а) мониторинг на условията на труд и оценка на професионалните рискове;

б) Мониторинг (разследване) на злополуки, влошаване на здравето на работници, болести, и професионални заболявания;

в) Мониторинг на несъответствията в областта на осигуряването на безопасни условия на труд и здраве на работниците;

г) Мониторинг на програми за постигане на целите в областта на и здраве на работниците;

д) Мониторинг на програми за рехабилитация за работници и финансовите разходи, свързани с увреждане на здравето и безопасността на работниците.

Разгледаните проблеми имат проява при оценка основно на техногенния риск, но техните характеристики могат да се имплементират в другите типове бедствия. От предложения модел могат да се изведат групи от организационни мерки, касаещи ръководствата на организациите (държавни и корпоративни) и определящи политики и мерки за превенция на рисковете от аварии и бедствия. Основните изводи са насочени към системите за контрол на управлението на промишлената безопасност и цялостен мониторинг на процесите като:

1. Анализиране на технологичните характеристики на производствените процеси и разкриване на потенциално опасните фактори.

2. Определяне на заплахите съобразно важността на отделните производства, технологии и инфраструктурно разпределение.

3. Възприемане на модели за непрекъснат мониторинг на състоянието на системата за оценка на професионалния риск.

Прилагането на такива подходи към оценката на техногенните заплахи е предпоставка за формирането на ефективни механизми за осигуряване и управление на професионалните рискове. Те водят до реализиране на ресурсите, необходими за своевременно третиране на заплахите и осигуряването безопасни условия на труд.

References

1. Бозов К.Д., Управление безопасностью в кризисных ситуациях природного и техногенного характера, КРСУ, 2011.

2. Тимофеева С.С. Хамидуллина Е.А., Оценка техногенных рисков. – Москва, 2015.

3. OHSAS 18001:2007. Occupational health and safety management systems – Requirement.

4. Файнбург Г.З. Проблемы формирования эффективной системы оценки и управления профессиональными рисками, сп.“Безопасность и охрана труда“, №3. – 2009

THE MILITARY LEADER – FACTORS AND CONDITIONS FOR FORMATION

Stancho G. Stanchev, Veliko P. Petrov

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

Abstract: *Leadership is a process of social influence in which the leader seeks the voluntary participation of his associates in the achievement of organizational goals. The most important characteristic of leadership is that it is a process in which an individual exerts influence on others based on his persuasive ability, motivating them to strive enthusiastically and selflessly towards the achievement of set goals.*

Keywords*: Leadership, factors of leadership and specificity of leadership behavior.*

ВОЕННИЯТ ЛИДЕР – ФАКТОРИ И УСЛОВИЯ ЗА ФОРМИРАНЕ

Станчо Г. Станчев, Велико П, Петров

Катедра „Артилерия и геодезия", Факултет „Артилерия, противовъздушна отбрана, комуникационни и информационни системи", гр. Шумен, България

Въведение

Изграждането на курсантите като ефективни командири е една от главните задачи на професионалната им подготовка в НВУ „В. Левски" за чието решаване досега като че ли се разчиташе повече на утвърдилото се като практика, отколкото на нововъведенията в обучението и във възпитанието на личността. Опитът показва, че добри резултати дава умелото съчетаване на подготвеността по специалността с умението да се командва и лидерства. Във връзка с това ситуативно ориентираното лидерство, появило се като контрапункт на неразрешимите противоречия между теорията за чертите на личността и теорията за поведенческите стилове, все повече се очертава, като най-предпочитаната платформа при формирането и развитието на ръководния състав на организациите.

Лидерството е процес на социално влияние, в който ръководителят търси доброволното участие на сътрудниците си в постигането на организационните цели. Някои автори развиват идеята, че липсата на доброволност обезценява и преиначава смисъла на този термин, доближавайки неговата семантика до авторитаризма и властването, които са само частен случай на влияние върху околните хора или последователите.

Лидерската тематика е много популярна в сферата на мениджмънта, тъй като качеството на подбора и особено характерът на подготовката на лидерите и на последователите им до голяма степен влияят върху производителността, интеграцията и морала в организацията. Смята се, че откриването на добри лидери е изключително трудно, поради което организациите не успяват да подберат тези, които са им необходими. Те само съумя ват да селектират индивидите с такъв потенциал и се опитват с подходящи програми да доразвият техните качества и умения.

Според Абрахам Залезник въпреки наличието на немалко схващания за идентичността на мениджмънта с лидерството няма достатъчно основание тази теза да се приема за вярна. Лидери има не само по върховете на организацията, но и в групите, основаващи се на приятелство или на някакви интереси към определени дейности или теми. Съществува модел, според който не всички мениджъри се проявяват като ефективни лидери, но всяка организация е заинтересувана нейните мениджъри да притежават такива качества и умения.

Най-важната характеристика на лидерството е, че то е процес, в който един индивид упражнява влияние върху другите на основата на способността си да убеждава, като ги мотивира те да се стремят ентусиазирано и самоотвержено към постигане на поставените цели.

Недостатъчно популярният ръководител или възприеманият като бюрократ началник като правило се причислява към групата от управленци, които не са лидери. Към нея обаче е и опитният специалист, който познава отлично работата си, може да открие изход от най-заплетената ситуация, способен е да успокои, ободри и вдъхнови колегите си, т. е. притежава лидерски умения, но не е упълномощен да ръководи

Пак според Абрахам Залезник различията между мениджърите и лидерите са в ориентациите им спрямо целите и подходите на вземане на решение в работата, междуличностните отношения със сътрудниците и начина им на самовъзприемане.

Мениджърите си поставят относително ниски цели, доверяват се на проверени подходи, обичат да си сътрудничат и се възприемат като членове на организация или институция. Лидерите използват целите като средство и предизвикателство за промяна, прибягват до алтернативни варианти на решение, свързани с риск, демонстрират силна емоционална обвързаност и имат реалистична самооценка, която не се влияе от членството в организацията.

Спецификата на лидерското поведение се проявява в контекста на групата или организацията съобразно с текущата обстановка. Последният аспект се разглежда най-обстойно от ситуационните теории — конкретно за армията от модела за организационна култура Робърт Куин и Ким Камеръп. Полезността му се изразява в това, че позволява да се отразят възможните сценарии в мирновременна и бойна обстановка. Те разработват състезаващи се критерии, съгласно които лидерите трябва да са способни да разрешават парадокси и да превръщат конфликта в ангажираност и изпълнение на задачите. Обединяват се две, на пръв поглед противоречащи си,организационни тенденции — стабилност и иновации. Според тази теория решаването на един проблем има следните фази: начална или въвеждане в проблематиката, несигурност, трансформация, установяване на определен ред и последователност за практическа реализация.

За всяка от фазите са валидни определени ценности, придържането към които гарантира ефективността на процеса. Например за началната това са изясняване на целта, насоченост, решителност, продуктивност и въздействие. Втората, наричана несигурност, изисква умение за намиране на решения и на най-заплетени те проблеми, нововъведения и своевременно адаптиране към тях, както и осигуряване на необходимата външна поддръжка и видим растеж. За трансформационната фаза са от значение ценностите загриженост, морал, ангажираност, дискутиране, съучастие и откритост.

Последната — установяване на ред, изисква ценности, типични за вече установила компонентите и функционирането си система, които да предсказват надеждно поведението й. Става дума за правене на измервания, поддържане на коректна документация, управление на процеса, стабилност, контрол и приемственост.

Военния модел на Робърт Куин обяснява армейската среда и поведението на индивидите в нея чрез две основни димeнсии — уникалност и риск, позиционирани в координатна система (нисък — висок риск и уникалност — рутинност). Така има възможност да се визуализират по-ясно различни ситуации, съвместими с вече споменатите условия на функциониране на лидера в казармена среда и бойна ситуация.

Видно е, че основната идея в модела „битка — гаризон" е балансът. Това означава, съгласно ситуационно ориентираната концепция на Робърт Куин, че за да е ефективен, лидерът следва да осъществява балансирано поведение в две противоположни области, което трябва да бъде допълвано и от инициативи. Понякога се изисква той да влиза в диаметрално противоположни роли по едно и също време за неопределен период.

Оказва се, че това мислене се формира извънредно трудно поради много причини. Традиционната литература по въпросите на управлението обръща голямо внимание на рационалните аспекти и пренебрегва интуитивното мислене. Изискваните умения са коренно противоположни на натрупвания от отделните командири социален опит в армията, което насърчава рационалното за сметка на интуитивното мислене. За да се формира в курсантите правилно мислене, се налага да бъдат разработени програми, които да развиват комплексни лидерски умения.

Под военно лидерство се разбира преди всичко процеса на влияние върху другите хора, с цел да изпълнят определена задача, като им се дава ясна цел, посока на действие и необходимата мотивация.

Ще разгледаме четирите главни фактора на лидерството в армията, които винаги са актуални и влияят силно на предприеманите действия. Това са - последователите, лидерът, ситуацията и комуникациите.

Първият основен фактор на лидерството естествено са военнослужещите, за чието предвождане лидерът отговаря. В наръчника се подчертава идеята, че не всички военнослужещи трябва да бъдат предвождани по един и същи начин. Например, войник с нова за него работа или задание обикновено се нуждае от повече наставления от това на войник, който има опит. Войник, който не е достатъчно уверен задължително се нуждае от подкрепа и насърчаване от страна на лидера. Войникът, който работи упорито и прави нужните неща, заслужава похвала, но този който нарочно се проваля или нарочно не следва предписаните насоки и не отговаря на ясните стандарти, може би трябва да бъде санкциониран. В крайна сметка лидерът е този, който трябва правилно да използва компетентността, мотивацията и себеотдаването на войниците, така че те да предприемат правилните действия в подходящото време.

Практиката показва, че в групата (екипа) е полезно да бъде изграден такъв климат, който насърчава подчинените да участват активно и да желаят да помогнат на лидера в изпълнението на задачата. Ключовите съставки за развиване на такава връзка са взаимното доверие, уважението и увереността в правилността на решението.

Вторият главен фактор на лидерството е самият лидер. Той трябва да е честен пред себе си за това какво знае и какво може. Изисква се той да е наясно със способностите си и предела им така, че да може да се контролира. След това се взема под внимание равнището на компетентност на подчинените, мотивацията и решителността им за изпълнение на дадената задача или мисия. В една ситуация може да се наложи отблизо да се надзирава и насочва работата на подчинените. В друга може да се наложи да се дава кураж или да се изслушват идеи. Или пък всичко това заедно.

Комуникациите, четвъртият главен фактор в лидерството, представляват обмяна на идеи и информация. Осъществяването на ефективни комуникации става, когато другите разбират какво точно се опитва лидерът да им каже и след получаването на адекватна обратна информация от тях. Лидерът може да комуникира с другите писмено, устно или чрез жестикулации, както и чрез комбинация на посочените подходи. Той трябва да се осъзнае, че именно от лидера произтичат стандартите на поведение на основата на личния пример, поощрението или наказанието на определени постъпки. Начинът му на комуникиране в различни ситуации е много важен. Изборът на думи, тон и жестове въздействат по неповторим начин на войниците. Отбелязва се, че лидерството е нещо повече от това да служим за пример със смелостта си в дадена ситуация. Способността да кажем нещо правилно в точно необходимия момент по най-подходящия начин също е от значение за лидерството.

В мирно време лидерът следва да отработи начини на свръзка с подчинените си, така, че те да следват командите му. Изисква се той непременно да спечели доверието им.

За да спечели доверието на подчинените си от началника или лидера се изисква:

- да разбира отлично работата си;
- да е напълно убеден в целесъобразността на разпорежданията си;
- да държи за пълното и неизменно провеждане на тия разпореждания;
- да има доверие в хората си;
- да е спокоен, но твърд и решителен;
- да е хладнокръвен и със самообладание;
- да държи безусловно на дисциплината;
- да се грижи за подчинените;
- да се поставя при същите условия както подчинените си;
- да взисква първо от себе си след това от подчинените си.

Ефективните комуникации предполагат лидерът да се изслушва с внимание и да се разбира какво казва. И след като войниците слушат своят лидер, то трябва да се направи нещо, за да се разбере какво точно войниците се опитват да му кажат. Доброто слушане се постига с помощта на много усилия чрез системно учене и подходящ тренинг. На първо време бихме могли да се придържаме към няколко прости правила в поведението си, например да не прекъсваме другите, когато говорят; да гледаме в очите този, който говори; да слушаме активно, т.е. да следим какво е казал и как го е казал. От съществено значение е да се отчита влиянието на емоциите, проектирани основно в невербалните послания (мимики, жестове, интонация) и възможността това да бъде “съзнателно” контролирано. Някои съвременни изследвания доказват, че те са важна съставна част на комуникациите. С внимателното изслушваме подчинените си ние изграждаме нагласа и умение и те да ни изслушват с внимание.

Четирите главни фактора на лидерството са налице винаги, при всяка една ситуация, но е важно да се знае, че те си влияят взаимно по твърде различен начин. И на-важният фактор в една ситуация може да се окаже маловажен в друга. Необходимо е постоянно да се имат пред вид тези основни положения в лидерството и да се избира най-верният начин на действие.

Много съществени правила или принципи на лидерството, които могат да бъдат отличен пътеводител и крайъгълен камък за ефективната работа на командира и могат да се разглеждат като фундаментални положения, отстоели проверката на времето.

Създаване на условия, които да позволяват курсантите да опознайте самите себе си и да се стремят към самоусъвършенстване: За да познаваме себе си е необходимо да разбираме своята мисия и да познаваме предимствата, силните си черти, както и нашите недостатъци. Сам по себе си факта, че познаваме себе си ни гарантира възможността умело да използваме силните си черти и да преодоляваме слабостите си. Стремежът към самоусъвършенстване означава непрестанно обогатяване на силните качества и полагане на усилия за отстраняване на слабостите. Това ще повиши нашата компетентност и вярата на войниците в умението ни да ги обучаваме и командваме.

Гарантиране качеството на тактическа и техническа ни компетентност: от нас се очаква да сме тактически и технически компетентни за длъжността, която заемаме. Това означава, че ние бихте могли да изпълним задачи според стандартите, характерни за военно време. Ние развиваме тактическата и техническата си компетентност посредством съчетаването на различни процедури, които усвояваме в процеса на образованието ни във съответните учебни заведения (институционално обучение), посредством изпълнението на всекидневните си задължения (оперативни задачи) и посредством саморазвитие в съответната професионална област.

Насърчаване в търсенето и поемането на отговорност за действията си: лидерството винаги предполага отговорност. Ние бихте желали да имаме подчинени, които могат да поемат отговорност и да помогнат в изпълнение на съответните задачи. Когато установим проблем или

нещо нередно, не трябва да чакаме да ни се каже да действаме. Примерът ни, независимо дали е положителен или отрицателен, ще помогне за развитието на нашите подчинени.

Усвояване на изкуството да се вземат навременни и твърди решения: ние трябва да можем бързо да оценим дадена ситуация и да вземем навременно решение. Ако отложим или забавим вземането на решение ние може да предизвикаме нежелани последици и да провалим осъществяването на задачата Нерешителните лидери проявяват колебание, загуба на увереност и объркване. Ние трябва да можем да разсъждаваме и при най-тежки условия и бързо да предприемаме необходимите действия.

Създаване на нагласа да бъдат винаги за пример на подчинените си: нашите войници искат и се нуждаят от това да сме пример за тях. Ако очакваме решителност и компетентност от подчинените си, то ние трябва също да можем да ги демонстрираме. Ние трябва да поставим високи, но постижими стандарти (изисквания), да сме склонни да правим това, което изискваме от войниците си, да споделяме опасностите и несгодите заедно с тях.

Развиване чувството за отговорност у самите курсанти и на способност за формирането на такава у техните подчинените: Подчинените ни трябва да знаят и да разбират какво очакваме от тях. Те имат нужда да знаят какво искате да се свърши, какви са стандартите и кога искаме да бъде свършено. Те имат нужда да знаят дали една задача трябва да бъде свършена по специфичен начин. Надзирането над работата ни дава възможност да разберем дали войниците схващат заповедите ни. То също показва заинтересоваността ни от изпълнението на задачата. Все пак добре е да знаем, че прекомерното надзираване се приема с неодобрение от подчинените.

Развиване на умения да се контролира доколко поставената задача е осъзната от подчинените и има ли условия за ефективното й реализиране: Когато войниците научава за нови задачи необходимо е да им бъдат обяснени изискванията за изпълнение по определен начин, както и да им се покаже как да ги изпълнят. Необходимо е да ги оставим да опитат, да наблюдаваме изпълнението им, както и да приемем изпълненията, които отговарят на стандартите ни и награждавайте изпълнения, които ги надвишават. Коригирайте изпълнения, които не отговарят на изискванията. Трябва да обясним причината защо едно изпълнение е лошо и да предприемем необходимите действия. Когато държим сметка на подчинените си за техните изпълнения, те ще осъзнаят че са отговорили за изпълнението на задачи, като отделни личности и като екипи.

Формиране на умения за изграждането на екип за изпълнението на задачата: Сражението е колективно действие. Ние трябва да развиваме колективен дух у войниците, който да ги мотивира с желание и увереност да влязат в бой при ускорено преминаване от мирно време в условията на въоръжен конфликт. Войниците имат нужда да са уверени в способността ни да ги предвождаме, както и в собствената им способност да действат като екип. Ние трябва да тренираме докато постигнем увереност в техническите и тактически качества на екипа.

Заключение

Познаването на някои от съвременните фактори на лидерството ще ни помогне да осъществим задачите успоредно с осигуряване необходимата грижа за курсантите. Факторите на лидерството са винаги налице и въздействат на това какво и кога трябва да се направи. Съобразно факта, че всяка ситуация в лидерството е различна, ние трябва да можем да отчитаме спецификата на обстоятелствата и да решим какво да предприемем. Силно е въздействието чрез казаното, написаното и най-важното, чрез направеното от нас. Начина и предмета на нашата комуникация с останалите или ще подсили или отслаби взаимовръзките ни с тях.

Представеното тук не изчерпва въпроса за лидерството, нито открива нови постановки. То има за цел само да систематизира и осъвремени част от наличния опит в тази област и да подпомогне командирското изграждане на курсантите в условията на НВУ „В. Левски” като ефективни лидери за военните формирования на БА.

References

1. Baran, B. and Scott, C. 2010. Organizing ambiguity: A grounded theory of leadership and sense-making within dangerous contexts.

2. Dirks, K. and Ferrin, D. L. 2002. Trust in leadership: Meta-analytic findings and implications for research and practice.

3. Osborn, R., Hunt, J. and Jauch, L. 2002. Toward a contextual theory of leadership.

4. Porter, L. and McLaughlin, G. 2006. Leadership and the organizational context: Like the weather.

5. Samuels, S., Foster, C. and Lindsay, D. 2010. Freefall, self-efficacy, and leading in dangerous contexts.

6. Zaleznik, A. (1993). Managers and Leaders: Are they different? – In: W. E. Rosenbach and R. L. Taylor (Eds.). Contemporary Issues in Leadership Research.

TOOLS AND METHODS IN THE OPERATION PLANNING PROCESS

Danko D. Farazov

***Abstract**: One of the most critical moments for the success of any operation is the process of operational planning. This process involves a wide range of activities, but some of them are extremely important. Determining the key factors and building the design are the main keystone for success of operations.*

***Key words**: Planning Tools, Operations Planning, Assessment, NATO, requirements, Services.*

СРЕДСТВА И МЕТОДИ В ПРОЦЕСА НА ПЛАНИРАНЕ НА ОПЕРАЦИИ

Данко Д. Фаразов

Военна академия „Г. С. Раковски", бул. „Евлоги и Христо Георгиеви" № 82, гр. София
имейл: d.farazov@rndc.bg

Въведение

Планирането на многонационални съвместни операции е едно от предизвикателствата пред, което се изправя Алианса в днешните условия. Сложната среда за сигурност, както и изключително комплексния характер на съвременните кризи, налагат изключително високи изисквания към процеса на планиране. Огромния брой планиращи, непрекъснатия цикъл на планиране, постоянните промени в обстановката и огромните потоци от информация водят до висока динамика и сложност, които създават предпоставки за пропуски, инертност на процесите и лошо качество на работата. От друга страна наличието на широк спектър специалисти от всякакви области и организации, както и многонационалната среда внасят допълнителни трудности. Решаването на тези проблеми е подпомогнато от въвеждането на функционална софтуерна система за подпомагане на процеса на планиране на операции.

Инструменти за планиране (Planning Tools)

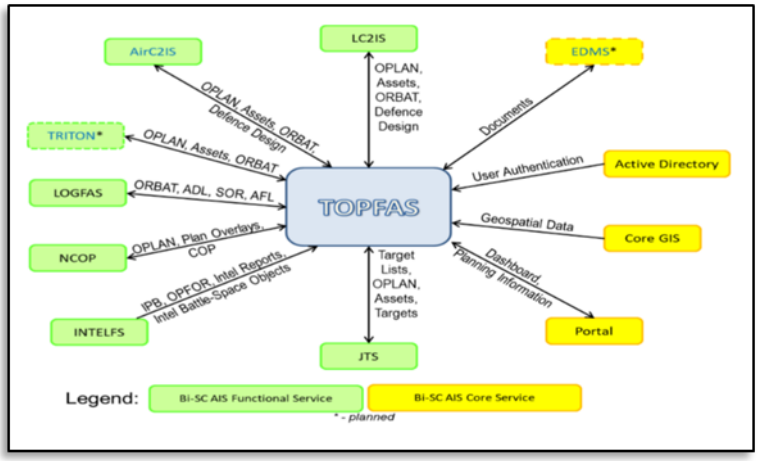
Представляват разработени от НАТО уеб базирани приложения с интегрирани функционални услуги. Те са предназначени да помагат щабовете при планиране и улесняват взаимодействието между планиращите нива от политическо, стратегическо и оперативно до тактическо. Използването им трябва да бъде възможно най-ефективно, защото улесняват навременното и ефективно съвместно планиране и значително подобряват цялостния процес. Изградените приложения от функционалната система отговарят на съответните изисквания описани в директивите и доктрините на НАТО. Въпреки, че са разработени за подпомагане на пълния процес на планиране и провеждане на операции, предоставят необходимата гъвкавост, която позволява ускорено планиране, като дава възможност за пропускане на етапи и стъпки от съдържанието на процедурите в съответствие с Директивата за всеобхватно планиране. Понастоящем се използват три основни приложения за подпомагане на процеса на планиране на операции и потребителите трябва да са наясно, че тези функционални софтуерни инструменти продължават да се развиват непрекъснато, за да осигурят по-голяма ефективност, както и наличието на ограничения, свързани с тяхното използване.

Функционална система за планиране на разузнаването (Intelligence Functional Support - INTEL FS). Тези софтуерни инструменти представляват в много отношения първата от функционалните услуги, която осигурява и подпомага процеса на планиране в областта на разузнаването. Пакетът от приложения за анализ на разузнавателната информация е предназначен да осигурява нейното споделяне, с цел да подпомогне управлението на разузнавателните процеси. Предоставя възможности за търсене и анализиране, генерира и управлява разузнавателни сведения, предоставя специализирани функционалности в насока към определени домейни (изображения, разузнаване и идентифициране на различни сигнали и тяхната достоверност) и позволяват разузнавателна координация и синхронизация. Функционалния софтуер за подпомагане на разузнавателната дейност, поддържа оперативна съвместимост с външни системи и управлява множество потребители, за да осъществи споделянето на информация във всички стационарни щабове на НАТО и тези разположени в театъра на операцията.

Функционална система за планиране на операции (Tool for Operations Planning Functional Area Services – TOPFAS). Представлява набор от инструменти, които подпомагат процеса на Управление на знанието[1], планиране и оценка за операции по интегриран начин на всички нива на операциите. Той позволява на планиращите в процесите на анализа и оценката да работят съвместно и паралелно, макар и тези дейности често се представят като последователни процеси, при планирането и провеждането на операции. Съответната информация за планирането е незабавно достъпна за информиране на вземащите решения и командирите, за да се улесни интегрираното и синхронизирано планиране. Системата е съвместима и с други инструмента за поддръжка на функционални услуги – инструменти за логистично планиране (LOGFAS) и тези за подпомагане на разузнавателната дейност (INTEL FS). Състои от три основни компонента:

- Софтуерни функционални инструмент за системен анализ (SAT);
- Софтуерни функционални инструмент за планиране на операциите (OPT);
- Софтуерни функционални инструмент за оценка на кампаниите (CAT).

Освен тези основни компоненти на системата, съществуват допълнителни функционални инструменти и приложения за специфични дейности показани на фигура 1. В процеса за подпомагане на планирането на операции – управление на процесите по генериране на силите, отчитане на готовността (Readiness Reporting), изисквания за информация (Request for Information – RFI) и система за управление на документооборота в бойни условия (Management and the Order of Battle Management Tool – OMT).



Фигура 1. Оперативна съвместимост на елементите от функционалната системата за планиране на операции[2].

[1] Knowledge Development – KD
[2] Директива за всеобхватно планиране на операции – Interim Version – 3.0. SHAPE, Mons, 2021

Функционални инструмент за системен анализ (System Analysis Tool - SAT). Използват се от самото начало на процеса на планиране в щаба съвместните сили. Основният състав, който работи с тези софтуерни приложения са органите по разузнаване за осъществяване на анализи и най-вече в процеса за управление на знанията. Тези инструменти позволява да се придобие и осигури необходимата информация и разбиране в театъра на операцията. Дава възможност да се идентифицират (ключови) фактори, условия, които трябва да бъдат променени, уязвимости, силни страни и слаби страни и други. Може да идентифицира и сравнява различен спектър от каскадно свързани ефекти, като промяната на едно или няколко условия може да въздейства върху останалите условия. Този динамичен анализ представлява съществен принос, който тази система предлага на планиращите. Различните опции на потенциални промени могат да помогнат за своевременното намиране на вариантите за реакция на противостоящите сили или собствените варианти за действие, тъй като опциите се идентифицират, и планиращите могат да помогнат да се остойностят параметрите на състоянието в зоната на операцията по отношение на приемливост при различните условия, които трябва да бъдат променени.

Инструмент за планиране на операциите (Operations Planning Tool - OPT). На основата на изводите от системния анализ, планиращите използващи функционалните приложенията за планиране на операции, могат да формулират проблема и мисията, която са получили. Възможностите на функционалните инструменти за планиране на операции подпомагат всички фази и стъпки, съгласно Директивата за всеобхватно планиране на операции. При необходимост обаче, ако ситуацията налага процес на бързо вземане на решение и процедура по съкратено планиране, приложенията на системата позволяват подпомагането на процеса на планиране и в този случай. Допълнително, също така подпомага създаването на рамкови проекции, документи, карти като поддържа презентации и брифинги. Всички нива, участващи в процеса на планиране, могат да получат достъп до съответната информация и резултатите от планирането на дадено ниво могат (когато е необходимо) да бъдат разработени с оглед на други нива. Това значително ускорява споделянето на важната и основна информация. Паралелно с планирането, системата позволява да се провежда и определянето на изискванията за способности, което може да бъде изведено незабавно, след анализ на действията на войските.

Функционални инструменти за оценка на кампаниите (Campaign Assessment Tool – CAT). Те са разработен в съответствие с Наръчника за оценка на операциите в НАТО[3] и позволява на планиращите да подготвят плана за оценка и плана за събиране на данни[4] в тясно сътрудничество с планиращите отговорни за процеса по управление на знанията и планиращите. Тази интегрирани характеристики осигуряват последователност на процеса на планиране и подпомагат валидирането на плана. По време на фазата за изпълнение на плана на операцията системата за оценка обработва данните и помага на служителите в щаба да изготвят необходимите съвети към командващия относно текущия напредък по линиите на операцията, установяването на критичните точки и постигането на целите. Също така позволява определянето на възможните тенденции за развитие на ситуацията.

Функционална система за планиране на логистичното осигуряване в НАТО (Logistic Functional Area Services – LOGFAS). Представляват набор от софтуер на НАТО, който поддържа логистично планиране, изпълнение и отчитане на операции по интегриран начин на всички нива на планиране. Програмите използват обща база данни за логистиката, така че данните могат лесно да се споделят и използват за различни функции, включително планиране на запасите и логистично отчитане. Приложенията за логистично придвижване и транспорт (M&T) позволяват на планиращите да извършат планиране на организацията на придвижването, мониторинг и обмен на данни, свързани с движението в ясен, детайлизиран и обобщен формат. Основните приложения на тази система са следните:

[3] NATO Operations Assessment Hand Book – NOAH
[4] Data Collection Plan – DCP

Функционална система за планиране на развръщането и придвижването в НАТО (Allied Deployment and Movement System ADAMS). предоставя инструментите за планиране и организиране на стратегическо и оперативно ниво. За операциите и ученията на НАТО, националните планове за предвижване трябва да бъдат ясно координирани между държавите-членки и НАТО с помощта на тази система. Постоянната съвместна група за логистична поддръжка[5] и Съюзен координационен център за придвижване[6] осъществяват планиране на придвижването със системата, в координация със съответното оперативно ниво и страната домакин като изготвят подробни планове за развръщане[7], за да бъде обединен в многонационален подробен план за развръщане[8], който представя всички планирани придвижвания на силите, ръководени от НАТО.

Система за мониторинг на придвижването (Effective Visible Execution – EVE). Представлява инструмент за изпълнение на придвижването и транспорта (M&T), за управлението на придвижването в страната домакин и в театъра на операцията. Това включва всички придвижвания, разполагания, включително и тези свързани с ротация на силите. В допълнение към основните си функции за управление на мобилността, системата осигурява онагледяване на текущи и планирани транспортни мисии и задачи до всички участващи държави и НАТО.

Система за планиране на коалиционното приемане, разполагане и последващо придвижване (Coalition Reception Staging and Onward Movement – CORSOM). В допълнение към функционалната система ADAMS, софтуерният инструмент CORSOM, позволява да се извърши подробно и детайлно планиране на приемането, организирането и последващо придвижване[9], осигурява визуализация и надзор на придвижванията в театъра на операцията по време на изпълнението и осигуряването. Важно е да се отбележи, че и трите системи споделят едни и същи данни и са направени да си взаимодействат помежду си, позволявайки безпроблемно преминаване от една фаза на операция в друга, както и тяхното едновременно използване.

Заключение

Съществуващите стандартни оперативни процедури, свързани с управление на знанията, планиране и оценка на операциите предстои да бъдат адаптирани, за да включват използването на функционалните инструменти във всяка фаза и стъпка от процеса на планиране на операции. Системата за подпомагане на процеса на планиране предлага само пакети от функционални инструменти, които не могат да заменят планиращите. Те само подпомагат работата на щаба при подготовката, организацията и улесняват процеса на вземане на решение.

References

1. ACO Comprehensive Operations Planning Directive – Interim Version – 3.0. SHAPE, Mons, 2021;
2. Allied Joint Doctrine for Stability Policing Edition A Version 1, 2016;
3. Allied Joint Doctrine for the Planning of Operations AJP-5, Edition A Version 2, 2019;
4. The operations process, Army Doctrine Publication ADP 5-0, Washington, 2019;
5. Command and Control Of Allied Land Forces, Edition B Version 1, 2016.

[5] Standing Joint Logistics Support Group – SJLSG
[6] Allied Movements Coordination Centre – AMCC
[7] Detailed Deployment Plans – DDPs
[8] Multinational Detailed Deployment Plan – MNDDP
[9] Reception, Staging and Onward Movements – RSOM

OPERATIONS DESIGN

Danko D. Farazov

***ABSTRACT**: One of the most critical moments for the success of any operation is the process of operational planning. This process involves a wide range of activities, but some of them are extremely important. Determining the key factors and building the design are the main keystone for success of operations.*

***KEY WORDS**: Ends, Ways, Means, Risks, Operating environment, Key factors.*

ОПЕРАТИВЕН ДИЗАЙН

Данко Д. Фаразов

Военна академия „Г. С. Раковски", бул. „Евлоги и Христо Георгиеви" № 82, гр. София
имейл: d.farazov@rndc.bg

Въведение

Осовни функции на командирът и щаба са разработването на плановете и издаването на заповеди чрез извършване на последователноста от дейностите в процеса на планиране на операции по време на „Анализ на мисията". Те съчетават изкуството и науката, като описват *начини*, с които съвместните сили чрез използването на своите *способности* ще постигнат целите за реализиране на *крайното състояние*. Оперативният дизайн предоставя подход на итеративно разбиране в рамкиране на дадения проблем, като улеснява командирите и щабовете при прилагането на оперативното изкуство. Това помага на командира и щаба да разбират оперативната среда и да могат да създадат ефективен план на операцията. С дизайна на операцията, командирът изразява визията си и разработва с помощта на щаба усъвършенстван модел, с който предоставя подробен и изпълним план за провеждане на операцията. Дизайнът на операциите се основава на ясното разбиране на политическия и стратегически контекст. Структурираните процеси, позволяват проектирането на операциите във времето и пространството с необходимите ресурси.

Крайно състояние, начини, средствата и рискове

Изясняването на целите, начините, средствата и рисковете е от основно значение за планирането на операциите. В процеса на планиране, планиращите трябва ясно да дефинират следните категории от изисквания – крайно състояние, начини, средства и риск.

Крайно състояние (End state). Условията, които трябва да бъдат постигнати по отношение на целите на старшия командир в подкрепа на крайното състояние. Отчитане на степента на приемливост на условията на средата в началото на операцията. Командирът отчита способностите на собствените сили спремо възложените целите. При промяна в политическите цели следва незабавно изискване за промяна в плана на операцията или изискване за нов план.

Начини за постигане(ways). Използването на колкото се може по-широк набор от похвати и подходи улесняват процеса по установяване и намиране на необходимите и подходящи условия за постигане на целите. Изясняване на последователността от действия и ефекти, с които е най-

вероятно да се постигнат благоприятаните условията. Определяне на точната система от инструменти за въздействие,които могат да се използват за създаване на последователни ефекти, които да доведат до необходимите условия. Определяне на последователноста от действията и ефектите във времето и пространството, за да се установят тези условия.

Средства за постигане (means). Установяване на необходимите ресурси и средства за постигане на определената последователност от действия и ефекти. Трябва да се дадат отговори, какви възможности и ресурси са на разположение и трябва да бъдат приложени за създаване на тези условия. Механизъм за интегриране и синхронизиране на военните и невоенните действия за постигане на условията.

Риск (risks). Рискът се оценява според вероятността за неговото възникване и тежестта на въздействието му и трябва да бъде смекчен по съответния начин. Нивото на риска може да бъде определено с някаква степен на достоверност, оценката на вероятностите и последиците е в компетенцията на преценката на командира. Степента на риска може да бъде значително намален чрез промяна на изискванията на някое от крайните състояния, адаптиране на начините за постигане на целите или промяна на изискванията към средствата. При констатиране на несъответстви, това може да се преодолее чрез промяна или дори с отказ от някои цели. Друго решение за преодоляване на несъответствия е да се намери по-ефективен начин за комбинация на военни и невоенни средства. В тази връзка Д. Гинев обобщава, че е необходимо „комплексното и хармонизирано прилагане на граждански (невоенни) и военни способности на държавата, допълвани и подпомагани от инструментите, предоставяни от колективната мощ на съюзите, в които членува страната." [1] Отговорността на командира е да прецени възможностите спрямо рисковете, да оцени потенциалното им въздействие и да идентифицира възможности, които предлагат най-голяма оперативна предпоставка за успех спрямо поетия риск.

Анализ на оперативната среда

Разбирането на оперативната среда е критична предпоставка за всички дейности в процеса на планиране, особено за изготвянето на дизайна на операциите. Той очертава основния подход в една операция и от него се извеждат всички останали дейности. Готовията дизайн на операцията предоставя контекста за разбирането на оперативния проблем. Съюзната съвместната доктрина за разузнаване, контраразузнаване и сигурност описва детайлно всички дейности свързани с прцеса на *Съвместната разузнавателна подготовка на оперативната среда*[2]. Описаните процеси дават значително по-широка предства в сравнение от традиционния фокус върху военните въпроси, като се обхващат всички аспекти – политически, военни, икономически, социални, информационни и инфраструктурни. Описват се основните характеристики и позволява на планиращите да оценят допълнително потенциалното въздействие на оперативната среда върху изпълнението на мисията. Командирът и щабът развиват споделено разбиране и цялостен поглед върху оперативната среда по отношение на кризисната обстановка, основните причини и специфичната динамика. Това позволява на командира да визуализира степента на проблема и как е възможно да променят оперативната среда. Този процес подпомага значително в информационно отношение вземането на решение.

Анализ на факторите и определяне на ключовите фактори. Съвременните конфликти и кризи се отличават със сложни взаимозависимости, комбинирани с исторически, политически, военни, социални, културни и икономически аспекти. „Правилния анализ на посочените аспекти предоставят една картина на ситуацията със взаимовръзките между отделните фактори на средата, първоизточниците на проблемите, силните и слаби страни, на базата на които се очертават необхо-

[1]Гинев. Д., Изграждане на граждански способности за отбрана на страната, АЛФА ВИЗИЯ, София, 2020 г. ISBN: 978-619-7595-00-0, стр. 14

[2] Joint intelligence preparation of the operating environment – JIPOE

димите способности за неутрализиране или овладяване на кризата" [3]**.** Това от своя страна изисква командирът и щабът трябва да изследват специфични аспекти, факти или условия на оперативната среда и възможностите, които предоставя. Това включва още необходимите цели за постигане, взаимоотношенията и взаимодействията между всички участници в кризата, за да се определи тяхното въздействие върху възможностите за оперативен успех. Взаимодействията включват намерения, потенциални възможности и способности, тенденции в района, напрежение между определени участници, идентифициране на силните и слаби страни. Командирът и щабът разглеждат въздействието на оперативната среда върху основните действащи лица и участници, както и върху силите на НАТО, тъй като те си взаимодействат във времето, пространството и информационна среда. Изводите и заключенията, получени от този анализ, определят границите за разработване на алтернативни решения. Тук е важно да се определи и „липсата на информация в дадено направление. Тази липса на информация е необходимо да се счете като риск. На базата на съществуващите и рискове и заплахи и липсващата информация е необходимо да се определи оценката на оперативните рискове и да се отчете степента и влиянието на тези рискове и заплахи" [4] На фигура 1 е показана принципна схема за анализ на факторите на средата. Освен това е важно определянето на ключовите фактори, които ще имат пряко отношение към това, което може да се наложи да бъде постигнато в областта на операциите, особено в рамката на какви обстоятелства и при какви условия ще се реализира.

В комбинация с възложените и произтичащи задачи, както указанията и намеренията от старшите нива, командирът и щабът определят желаните условия, водещи до бъдещо и приемливо състояние на оперативната среда. Разбирането на оперативната среда ще бъде от полза от прилагането на всеобхватен подход, включващ невоенни участници. Тези участници имат принос в дейностите при анализа на мисията.

Фигура 1. Принципна схема за анализ на факторите на средата.

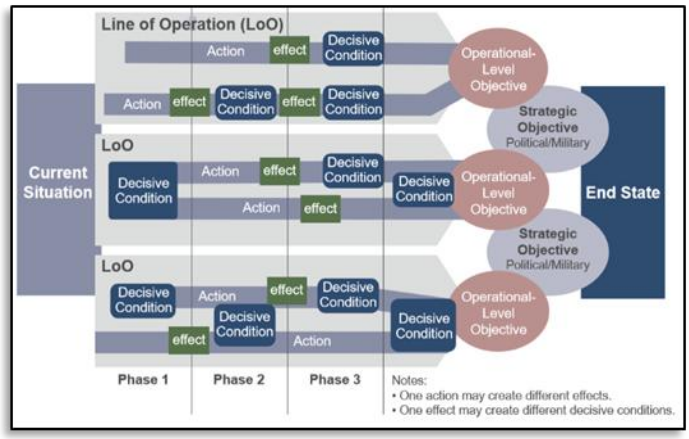
Интеграцията на невоенни участници може да не е възможна или препоръчителна в някои ситуации, в зависимост от конкретни обстоятелства, напр. за съображения за сигурност на операциите. За да се насърчи всеобхватното разбиране, командирите внедрят невоенна експертиза като обща насока и изпращат военни предствители за връзка с граждански организации.

[3] Георгиев, Валентин "Влиянието на факторите на средата върху процеса на планиране", International Scientific Conference ―Defense Technologies (DefTech 2019), Национален военен университет, факултет „Артилерия, ПВО и КИС" Шумен, 2019 г. Електронно издание: ISSN 2367-7902, стр.73

[4] Георгиев, Валентин "Влиянието на факторите на средата върху процеса на планиране", International Scientific Conference ―Defense Technologies (DefTech 2019), Национален военен университет, факултет „Артилерия, ПВО и КИС" Шумен, 2019 г. Електронно издание: ISSN 2367-7902, стр.80

Концепции за оперативния дизайн

Концепциите за дизайн на операциите помагат на командира и щаба да фомулират основните противоречия, природата на предизвикателствата и да изградят възможно най-пълно разбирането на оперативната среда, като анализират стратегическите и оперативните фактори. Оперативните фактори включват време, пространство, сили и информация, и се изобразяват графичното заедно със стратегическите цели и механизмите на взаимодействие, като представят недвусмислено разбиране за ситуацията, намерението на командира и насоките в процеса на планиране. На фигура 2 е представена принципна графична схема на процеса на планиране на операция.



Фигура 2. Дизайн на операцията[5]

Дефинирането на проблема и разработване на единен подход, който насочва планирането и води до оформяне на концепцията на операцията чрез представените елементи на дизайна на операцията е изключително ефективен способ, особенно котаго става въпрос за сложна среда и мисийно командване. Той се състои от следните елементи:

- крайно състояние;
- критерии за преход и прекратяване;
- център на тежеста;
- директен и индиректен подход;
- цели;
- условия за успех;
- действия и ефекти;
- линии на операцията;
- кулминация;
- оперативна пауза;
- последователности и фази.

Всеки един елемент от дизайна на операцията прави концепцията на операцията възможно най-пълна и ясна. Този метод е изключително ефективен за пълното разбиране в рамките на всеобнхватния подход и усъвършенства процеса на планираме.

Заключение

Пълното и широко разбиране на възможно в най-тесния контекст на същноста на конфликта като цяло и в частност кризата, подпомагат процеса на палниране, като позволяват създаването на различни възможности за вземащите решение. Така се очертава, най-общо концепцията за поконкретното разбиране на оперативната среда. По този начин се създават и концептуалните рамки за мислене, които са главната предпоставка за единната и пълноценна рабора на щабния екип.

[5] Allied Joint Doctrine for the Planning of Operations AJP-5, Edition A Version 2, 2019

References

1. Гинев. Д., Изграждане на граждански способности за отбрана на страната, АЛФА ВИЗИЯ, София, 2020 г. ISBN: 978-619-7595-00-0, стр. 14

2. Allied Joint Doctrine for the Planning of Operations AJP-5, Edition A Version 2, 2019;

3. The Operations Process, Army Doctrine Publication, 2019;

4. Георгиев, Валентин "Влиянието на факторите на средата върху процеса на планиране", International Scientific Conference ― Defense Technologies (DefTech 2019), Национален военен университет, факултет „Артилерия, ПВО и КИС" Шумен, 2019 г. Електронно издание: ISSN 2367-7902, стр.80;

5. Георгиев, Валентин "Влиянието на факторите на средата върху процеса на планиране", International Scientific Conference ―Defense Technologies (DefTech 2019), Национален военен университет, факултет „Артилерия, ПВО и КИС" Шумен, 2019 г. Електронно издание: ISSN 2367-7902, стр.73;

6. Comprehensive Operations Planning Directive, 2021.

IMPERATIVES IN THE DECISION-MAKING PROCESS

Danko D. Farazov

***Abstract**: The ability to make a decision is a skill that provides essence of the planning process. Decision making process is complex and multi-layered, and puts the quality of planning to the test. This is the reason that makes decision making a key activity in planning process.*

***Key Words**: Decision, Alternatives, Evaluation, Analysis, Problem.*

ИМПЕРАТИВИ В ПРОЦЕСА НА ВЗЕМАНЕ НА РЕШЕНИЕ

Данко Д. Фаразов

Военна академия „Г. С. Раковски", бул. „Евлоги и Христо Георгиеви" № 82, гр. София
имейл: d.farazov@rndc.bg

Въведение

Вземането на решение е основна и неделима част от управлението. Повечето пъти то се основава на използването на утвърдени правила и практики. Когато, обаче е отнесено към определено сложен проблем и се засягат съществени процеси, вътрешни за организацията и външната среда, тогава е необходимо използването на опит, интуиция и специфични управленски умения. В такива случай, вземането на решение се превръща изключително в творчески процес. В съвременната сложна среда за сигурност този процес е свързан с работата на много специалисти. Организирането на колективната работа на големи групи от хора и структурирането на процеса е изключително предизвикателство пред вземането на решение.

Нива за вземане на решения

Стратегическо ниво – определят основните принципи, критерии и ограничения. Имат дългосрочен характер, трансформират политически ангажименти и намерения, като ги представят в реалната среда и в конкретни аспекти. Очертават рамката на участие и съответните отношения със заобикалящата среда. Свързани са с принципните цели и степента на участие в конфликта. Ясно и недвусмислено обосновават политическите и правни основи на военното участие. Повечето пъти не се извършват в реално време. Сложни са от гледна точка на участието на голям брой от организации, интереси, разглеждат се редица променливи величини и представляват сложна система от процедури на различни нива, като междудържавно, междуинституционално, многонационално и други.

Оперативно ниво – определят начините, участниците и пълния спектър от взаимовръзки и координация. Изпълват със съдържание стратегическите решения. Те са сравнително краткосрочни, тъй като дефрагментират на отделни задачи, етапи, цели и периоди стратегичските. Това ниво обикновенно е структурирано на няколко поднива. Това се налага поради факта, че тук се извършва реалната връзка с принципните постановки и реаната среда, която е много по-сложна от колкото изглежда. Поради голямата сложност на средата за сигурност и високите изисквания при участие на военния компонент при вземането на решение се използва системния подход. Висока-

та сложност изисква голяма подготовка от вземащите решени и в това ниво този процес е изцяло творчески.

Тактическо ниво – определя непосредствения начин на изпълнение. Най-голяма тежест има във фаза 5 - "Изпълнение". Обикновенно на това равнище става натрупване на всички грешки, допусната в предходните две нива. Най-ясно си проличават всички пропуски в плана на операцията. Най-често в процеса на вземане на решение се използва ситуационния подход. Решенията се вземат в реална среда и време. Двата процеса на планиране и на вземане на решение се сливат в едно. Всички пропуски и грешки по правило имат силно пагубно въздействие. Рутината на командния състав е от изключително значение. Използването на изпитани и проверени практики е повече от препоръчително, творческите процеси и импровизациите са крайно нежелани.

Цикъл на вземане на решение (Decision-making cycle)

От момента на констатиране на проблема до момента на вземане на решението и неговото изпълнение е период в рамките, на който са ситуирани редица процеси и се нарича *цикъл на вземане на решение*. Съвкупноста от процеси и процедури в рамките на цикъла дава същноста на процеса за вземане на решение. Схематично цикъла за вземане на решение е представен на фигура 1. В повечето случай представлява итеративна дейност, която на базата на последователни стъпки, води до изграждане на стратегия и реализирането, на която трябва да постигне ефекти в определена посока. Организирането на тези дейности в ясно определени процедури и взаимодействия е ключовата необходимост за бързината и качеството на работата. Този процес се отнася в най-пълна степен за оперативното ниво, тъй като структурната организация и процедурните механизми на работа са различна за всяка една операция. Допълнително утежняващо обстоятелство е многонационалния характер на щабовете. Въпреки общоприетия седем стъпков модел за вземане на решение, ще разгледам само някой основни процеси, които са следните:

- Информационна дейност;
- Определяне на алтернативите за действие;
- Избор на вариант за действие;
- Изпълнение (действие);
- Оценка.

Информационна дейност – отнася се до събиране и анализиране на информация. На основата на старистически процеси, тази дейност е свързана с процеса за управление на знание. Този процес представлява една щирокообхватна дейност свързана със работни структури извън военния обхват и преминаваща през няколно последователни нива, тясно във военните структури докато се затвори пълния информационен процес. Като цяло представлява една основен процес на базата, на който е изградено планирането.

Определяне на алтернативите за действие – представлява процес на проектиране на потенцията на нашите способности на силите върху определени системи от участници с цел да се постигнат необходими благоприятстващи ефекти. Процесът се свежда до генериране на множество от възможни варианти.

Фигура 1. Цикъл за вземане на решение.

Избор на вариант за действие – изборът на вариант за действие е сложен процес, който изисква изключителен опит и познаване средата за постигане на ясна и сравнително достоверна представа за предлаганите от различните варианти, положителни и отрицателни страни. Оценката на различните алтернативи по правило се извършва от допълнителни екипи.

Изпълнение – това е една от най-деликатните дейности, тъй като процеса на изпълнение на операцията може да я доведе до обезмисляне, в резултат на редица грешки и пропуски дори и при наличие на перфектен план на операцията.

Оценка – при този процес се извършва реалното остойностяване всички извършени дейности. Това е важно за да се направи достоверно и недвусмислено разбиране на ситуацията и постигнатите цели. Правилната оценка е от изключително значение за по-наташното участие. Определя и критериите за напредък на операцията и това я прави изключително важна. Изграждането на единно виждане за развитието и оценката на операцията е труден и спорен въпрос. Това е причината да се използват различни нетоди за оценки, които залагат основно на последователно и споделено разбиране на напредъка и прмяната на ситуацията.

Фактори оказващи влияние на процеса на вземане на решение

Групите фактори оказващи влияние са най-различни, но можем да разграничим основно две групи фактори – субективни и обективни.

Субективните фактори са свързани основно с качествата и подготовката на личния състав, но също така и с изградените организационни процеси в щаба и способноста на началника на щаба да управлява процесите в щаба. Индивидуалните личностни подходи в процеса на вземане на решение са от голямо значение и са ключове в сложни ситуации и критични моменти. Те се основават на личностните характеристики на вземащите решение и най-вече командирите. Изграждането на такива кадри е бавен и труденпроцес и поради това те са най-ценния ресурс, когато говорим за оперативно изкуство.ф

В условието на по-сложни регионални кризи и големи контингенти от многонационални съвместни оперативни сили, организацията на процесите и качеството на подготовка на офецерите заема все по-основно място и се превръща в критен фактор за успеха.

Обективните фактори, с които вземащите решение трябва да се съобразяват се отнасят до следното:

- Ограничение по отношение на времето;
- Непълна и ясна (противоречива) информация;
- Ограничени ресурси;

- Спазване на поетите политически ангажименти;
- Спазване на правилата за употреба на сила;
- Риск за цивилни граждани;
- Промяна в политическата обстановка.

Анализа на изброените фактори води до изграждането на сложни зависимости и противоречиви алтернативи за избор. Тази сложност и комплексност на средата в зоната на операцията, поставя на изпитание командирите от всички нива и залага на карта политическия успех на военното участие. Вземането нарешение е труден процес, който освен наличието на опит, интоиция, доказани способности и знание е свързан до голяма степен с изключително много екипна работа и често пъти със спазването на сложни процедури. От тук закономерно издва въпроса свързан с отговорността, който е ключов за тази дейност. В процеса на вземане на решение, важен момент е определянето на ограниченията на оперативната свобода на действие, които се заключават в ограничения свързани с невъзможност за дадена дейност и сдържаност от действия, които не трябва да се извършват. Определяне на необходимите допусканията и изисквания за информация и разузнавателни данни, определя аналитичния характер на процеса и дава възможност да се покажат всички възможни пропуски в информацията, знанията и разузнавателните данни, включително и това, което е от решаващо (критично) значение за последващото развития на планирането. Синхронизираната екипна работа дава основната база на процеса и позволява творческата преценка и дейност на вземащите решение. Това е от изключителна важност в съвременното мисийно комндване в сложна кризисна среда и политическа обстановка.

Заключение

Този процес продължава да бъде едно от най-големите предисвикателста във всяка една операция. Натрупаният опит в годините позволява голяма част от дейностите да се канализират. Непрекъснатото обновяване и допълване на доктриналната и концептуална основа, допълва процеса непрекъснато в условията на променящата се среда за сигурност. Използването на все повече изчислителна техника дори и на най-ниско тактическо ниво улеснява работата в сложни ситуации, когато имаме малко време и много фактори искащи детайлна оценка за въздействието им. Въпреки това постоянно променящата се среда за сигурност и уникалността на всека криза сама по себе си поставя предизвикателства, които непозволяват на този процес да се обособят универсални закономерности и правила. Това налага човешкият интелект, опит и интуиция да са незаменими все още.

References

1. ACO Comprehensive Operations Planning Directive – Interim Version – 3.0. SHAPE, Mons, 2021;
2. Allied Joint Doctrine for The Conduct Of Operations, Edition C Version 1, 2019;
3. MC 319/2 NATO Principles and Policies;
4. Allied Joint Doctrine, AJP-01, Edition E Version 1, 2017;
5. Allied Joint Doctrine for Land Operations Edition A Version 1 March 2016;
6. http://thebanking1.blogspot.bg/2014/11/blog-post.html;
7. http://www.ometeo.net/edu/html/2010104.htm.

CIVIL-MILITARY COOPERATION IS A MAJOR FACTOR IN MODERN MILITARY CONFLICTS

Kaloyan A. Iliev, Veliko P. Petrov

Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, kacho_78@abv.bg , veliko_pp@abv.bg

***Abstract**: After the Second World War and the construction of a new world order, attention was directed to avoiding military conflicts, conducting preventive actions to prevent disorders, crimes, crisis situations and, of course, the protection of human rights. The UN Security Council has the primary responsibility for the maintenance of international peace and international security. The history of the 20th-21st centuries has shown that it is not very easy to maintain peace and tranquility in the world community. Modern military conflicts in Syria, Iraq, Turkey, Congo, Afghanistan, and Ukraine take place in an increasingly complex environment in which, in addition to the military, there are also numerous civilian and humanitarian institutions that together must face the challenges of a wider circle of questions. In certain cases, the military performs tasks that are not exactly "military" in nature, which increases the importance a necessity of civil-military cooperation.*

***Keywords:** military conflicts, crisis situations, protection of human rights international peace, civil-military cooperation*

ГРАЖДАНСКО-ВОЕННОТО СЪТРУДНИЧЕСТВО - ОСНОВЕН ФАКТОР В СЪВРЕМЕННИТЕ ВОЕННИ КОНФЛИКТИ

Калоян А. Илиев, Велико П. Петров

След Втората световна война и изграждането на нов световен ред, вниманието беше насочено към избягване на военни конфликти, провеждане на превантивни действия за предотвратяване на безредици, престъпления, кризисни ситуации и, разбира се, защита на човешките права.

Съветът за сигурност на ООН носи главната отговорност за поддържането на международния мир и международната сигурност.

Историята на XX-XXI век показа, че не е много лесно да се запази мирът и спокойствието в световната общност. Съвременните военни конфликти в Сирия, Ирак, Турция, Конго, Афганистан, и Украйна се провеждат във все по-сложна среда в която освен военните, съществуват и множество цивилни и хуманитарни институции, които заедно трябва да се изправят пред предизвикателствата на по-широк кръг от въпроси.

В определени случаи военните изпълняват задачи, които не са точно „военни" по природа, което увеличава значението и необходимостта от гражданско-военното сътрудничество. Военните сили трябва да бъдат в тясно сътрудничество с цивилния компонент, който включва цялата цивилна среда: местното население, гражданската местност, организациите (правителствени, неправителствени), граждански институции и местните авторитети.

Гражданско-военното сътрудничество (ГВС) представлява отношенията между две страни,

първата страна са военните структури, а втората страна са гражданите и организациите им, като тези отношенията протичат както в мирно, така и във военно време. ГВС предполага взаимодействие, което освен това е основен принцип на военното изкуство и се изразява в съгласуване на действията на войските (силите) по цел, място, време и способи за изпълнение на задачите.

Днес необходимостта от изучаване на такъв феномен като гражданско-военното сътрудничество (CIMIC, ГВС) вече не е под съмнение. Тъй като и при изпълнението на операциите, задачата на военните сили не се състои в постигането на резултати на всяка цена, но изпълнението на мисията, преди всичко, трябва да минава с минимизиране на загубите и осигуряване на защита на местното население, в името на „живота", където очакваният резултат е мир и безопасността на хората.

Целта на ГВС е осигуряването и поддръжката на командирите от всички степени при изпълнение на техните задачи. Отговорност за организацията и ръководството на дейностите по ГВС носи командира на военното формирование.

Предназначението на ГВС е взаимодействие между военните и гражданските участници в рамките на цялостна среда за подкрепа на плана на военния командир. В идеалния случай всички участници следва да работят за една обща цел, но когато това не е възможно, взаимодействието ще гарантира, че дейностите в подкрепа на всеки план са хармонизирани, доколкото е възможно. Това ще сведе до минимум смущенията или неволен конфликт между всички участници. Това взаимодействие може да се състои, но не се ограничава до координация, сътрудничество, взаимна подкрепа, съгласувано съвместно планиране и обмен на информация, покриваща политическия мандат. ГВС включва военните сили на НАТО, управлението и гражданските лица.

Според схващанията на НАТО, ГВС е приложимо за всички видове операции на Алианса. Основни насоки за прилагане на гражданско-военното сътрудничество в операциите на НАТО за постигне на максимален успех за всички страни е изключително важно всички те да разбират напълно как всеки партньор планира и действа. От една страна, военнослужещи на тактическо ниво ще осъществяват задачи по гражданско-военно сътрудничество, като най-общо е описано в AJP-3.4.9 и уточнено в тактическите публикации, като пряко допринася за военните усилия на самия терен. От друга страна, задачи по гражданско-военно сътрудничество ще бъдат извършвани от персонала, който не е пряко свързани с функциите по гражданско-военно сътрудничество.

Като една от целите, поставени от НАТО, за успешното прилагане на всеобхватния подход, се явява подобряването на практическото сътрудничество на НАТО на всички равнища с партньори като ООН, международни, правителствени и неправителствени организации и местни участници в планирането и провеждането на операциите.

Поради възникналата необходимост от все по-широко взаимодействие и сътрудничество, през май 2014 г. е взето решение за промяна на политиката на НАТО за гражданско-военно сътрудничество МС 411/1 и е приета новата политика на НАТО за гражданско-военно сътрудничество и гражданско-военно взаимодействие МС 411/2.

В този документ за пръв път са диференцирани двете понятия „гражданско-военно сътрудничество" (ГВС) и „гражданско-военно взаимодействие" (ГВВ). За разлика от определението за ГВВ, от ГВС се иска съсредоточаване върху военната мисия (по възможност с включване на задачи за сътрудничество с невоенни участници). Тоест, на ГВС е отредено по-ниско място – тактическото ниво. Следователно, чрез прилагане на ГВВ, ГВС може да повиши своята значимост и целта му е най-вече свързана с даването на възможности на командванията на НАТО, да участват в ГВВ.

Въвеждането на ГВВ в рамките на НАТО е насочено към подобряване и стандартизиране на участие в нещо, което по природа винаги е съществувало, а именно връзката между цивилни и военни лица.

Пътят за развитие на гражданско-военното взаимодействие се основава на разбирането, че взаимодействие е ключът към успешното сътрудничество.

В конвенционалните военни операции, провеждани предимно чрез използването на сила за

постигане на оперативните цели, ще се съдържат различни по обхват дейности по гражданско военно взаимодействие в сравнение с операции за стабилизиране или операции за подпомагане при бедствия.

Планирането на военни действия изисква въвеждане на ГВС както всяка друга военна дейност в зоната за отговорност и извън нея. Всички измерения на съвременните военни операции са повлияни от ГВС, като техният фокус е върху гражданската среда. Не всичко в армията е ГВС, но ГВС може да изиграе ключова роля в рамките на приноса на НАТО за прилагане на всеобхватния подход. Именно по тази причина приносът и влиянието на ГВС следва да имат видимо присъствие на всички нива в Алианса в пълния спектър от изпълнявани операции.

Планирането и провеждането на мисии и операции на НАТО изисква да се провеждат обсъждания с различни невоенни участници и в различни сфери (политически, икономически, социални, инфраструктурни и т.н.). Експертите по ГВС и цивилните експерти във военните структури на НАТО следва да поставят акцент върху осигуряването на разбирането им в зоната на операцията и прилагане на това разбиране в планирането, вземането на решения, изпълнението и оценката. Задълбочената оценка, връзката и информирането за решенията на командира са предпоставки за предоставяне на военна помощ на местните власти или други участници.

Стандартните структури, изградени в зависимост от декларираните способности на НАТО и обвързани с набелязаните цели на силите на Алианса, са както следва:

- щабни елементи за ГВС;
- група за ГВС;
- поддържащи формирования за ГВС;
- функционални специалисти.

Органите и силите за ГВС се формират в зависимост от специфичните задачи, които ще изпълняват. Те могат да варират от сили за ГВС, през щабни структури за ГВС, до други специализирани структури за ГВС, създадени под национално или многонационално командване. Допустимо е дори отделни военнослужещи и структури за бойна поддръжка на войските в зоната на операцията да допринасят за ГВС без конкретно обучение и подготовка в тази област.

Щабните елементи за ГВС се определят според нивото и състава. В зависимост от ранга на формированието щабният елемент за ГВС бива: секция, отделение, отдел и т.н. и се нарича S/G/N/J/CJ-9. Според състава си те са национални и многонационални. Структурите на отделите за ГВС ще се различават значително, но като цяло ще се състоят от главен отдел J-9, оперативно отделение, отделение за планиране и отделение за връзка. Основната задача на отдела за ГВС е да подпомага командващия с точни и навременни съвети и оценки съгласно плана за ГВС за операцията, с цел подпомагане и постигане на оперативните целите.

Гражданско-военното сътрудничество се планира, организира и провежда, съобразно:

- социалните, политическите, културните, религиозните, икономическите, хуманитарните фактори и околната среда;
- присъствието на международни, национални и неправителствени организации, техните цели, методи и перспективи, които следва да се съгласуват с тези на Българската армия.

Непосредствената цел на ГВС е установяване и поддържане на сътрудничество на командирите в района за изпълнение на мисията с:

- гражданските власти;
- неправителствени организации и агенции;
- местното население.

Дългосрочната цел на ГВС е съдействие за създаване и поддържане на условия, които да позволят на формированията да постигнат целите на операцията.

Функции на ГВС са:

- Поддръжка на гражданската среда
- Поддръжка на войските

Принципи на военното ръководство на ГВС са:

- Устойчиво управление;
- Концентрация на усилията;
- Всестранно осигуряване;
- Взаимодействие.

Изисквания към материализацията на принципите на ГВС са:

- Законите на страната;
- Общи хуманни ценности;
- Уважение към културата;
- Общи цели на взаимодействието;
- Споделена отговорност;
- Консенсус при вземане на решенията;

Общи задачи на органите и силите, участващи в ГВС са:

- в мирно време – обучение и практическа подготовка, оказване на помощ при природни бедствия и аварии;
- в операции в отговор на криза – управление на гражданското население и ресурсите, координиране на военната помощ, поддръжка на провежданите операции.

Основни насоки и задачи за прилагане на гражданско-военното сътрудничество на структурите на ГВС в БА са:

- координиране и ръководство на дейностите по ГВС в БА.
- разработване на концептуална и доктринална база по ГВС.
- контрол на подготовката на органите и подразделенията за ГВС в БА.
- координиране участието в национални и международни учения и тренировки.
- координиране участието на представители на органите и подразделенията по ГВС от БА в мисии и операции на НАТО и ЕС съвместно с национални, международни и неправителствени организации и агенции.
- разработване на програми за обучение на подразделението за ГВС и другите органи за ГВС.
- Разработване на брифинги, анализи и други документи за подготовка на командния състав по ГВС.
- Оказване на помощ на местната власт и населението при водене на операции в отговор на кризи.
- Изучаване и оценка на обстановката по ГВС.
- Подготовка и развръщане на центрове за ГВС в оперативните райони.
- Оказване на съдействие при доставката на хуманитарна и военна помощ, при защита на културни паметници, възстановяване на гражданска инфраструктура.

Българският опит на структурите отговорни за ГВС са:

- участие в мироопазващите мисии и операции в страните от западната част на балканите, Ирак и Афганистан, които категорично доказаха, че дейностите по ГВС са важно средство в ръцете на командирите на военни формирования от НАТО и ЕС за формиране на добри отношения с местното население и сътрудничество от негова страна за преодоляване на кризата.

ИЗВОДИ:

- Гражданско-военното сътрудничество днес е ново явление на двадесет и първи век, което показва необходимостта и важността на сближаването на гражданския и военния компонент в контекста на сегашните предизвикателства.
- Механизмът за реализиране на системата за ГВС, като ново явление, трябва да се реализира изцяло както на национално, така и на международно ниво.
- Уреждане на кризисни ситуации, както в мирно време (например извънредни ситуации), така и в рамките на международни мисии (мироопазващи операции, операции за подкрепа на мира), показва необходимостта от бързо реагиране на такива ситуации с минимизиране на жертвите на гражданско население, както и на значението и важността на военните и гражданските институции като цяло в структурата на държавното управление, където решаването на такъв въпрос трябва да бъде тясно взаимодействие чрез форма на гражданско-военното сътрудничество (CIMIC).
- В крайна сметка, може да се обобщи, че дейностите по ГВС следва да се провеждат както от персонала за ГВС, така и от всички други военни участници и цивилни експерти в зоната и извън зоната на операцията с цел подпомагане и улесняване на ГВВ както между въоръжените сили и цивилните в зоната на операцията, така и между самите военни на различните командни нива.
- Най-важното е ГВС да бъде напълно интегрирано в учения и експериментите на НАТО, което ще позволи и интегрирането му при провеждане на операции.

References

[1] Иванов В. Гражданско-военното сътрудничество - Първа част. Основи на гражданско-военното сътрудничество.

[2] Иванов В. Гражданско-военното сътрудничество - Втора част. Гражданско - военното сътрудничество в операциите.

[3] Тітко Е.В. Доктринальний підхід визначення цивільно-військових відносин у контексті CIMIC з метою захисту цивільного населення на прикладі праці Семюеля Філліпса Гантінгтона / Е.В. Тітко // Human rights: theory and practice, 23–28 January 2017, edited by M. Dey. – London: IASHE, 2017. – P. 21–25.

[4] AJP-3.1, Allied joint doctrine, for Information operations, 2009.

[5] AJP-3(B), Allied joint doctrine for the conduct of operations, 2011.

[6] AM 86-1-1. ACO CIMIC Tactics, Techniques and Procedures, Supreme Headquarters Allied Powers Europe (SHAPE), Belgium, Jul 2012.

[7] AJP-3.4.9. Allied Joint Doctrine for Civil-Military Cooperation, NATO Standardization Agency (NSA), Feb 2013.

[8] MC 411/2. NATO Military Policy on Civil-Military Cooperation (CIMIC) and civil-military interaction (CMI) North Atlantic Military Committee, May 2014.

DEFINITIONS FOR INFORMATION OPERATIONS, COGNITIVE WARFARE, AND RELATED TERMS

Dobril A. Radoslavov

Defense Policy and Planning Directorate, Ministry of Defense, Sofia, Bulgaria,
d.radoslavov@mod.bg

***Abstract**: The need for a literature and definitions review of the terms related to Information Warfare arises from the increased value of operations under the threshold of war that autocratic societies tend to wage against democracies. The author observes that the ambiguity of these terms allows them to be used vaguely or with various meanings in academic literature and among practitioners. This article aims to establish Cognitive Information Warfare (CIO) as the most relevant term for information operations in the age of increased global great power competition. CIOs are increasingly being used as a tool to impact decision-making through influencing and even weaponizing public opinion. Such clarification of the terms is needed to craft a strategy for countering malign foreign propaganda through Cognitive Information Operations.*

***Keywords**: Information Operations (IO), Information Warfare (IW), Cognitive Information Warfare (CIO)*

Introduction

An important question to ask is why the terms "information warfare" (IW) and "information operations" (IO) are of interest and what synonyms and derivate terms are gravitating around them. This paper aims through a literature review to define Information Operations (IO), Information Warfare (IW), Cognitive Information Warfare (CIO), and related and derivative terms.

There is a need to clarify the expressions mentioned above (IW/IO) before using them in academic papers or in the practice. The ambiguity of these terms allows them to be used vaguely or with various meanings that exist in academic literature and among practitioners. The difference in intended meaning exists not only between various national interpretations but also between sciences and fields of practical implementation. There is a lack of consensus about the meaning of "Information Warfare/Operations" between scholarly sources even within the same nation and in the same scientific field. The ambiguity becomes even more extensive when the terms cross national and science borders. To make things worse, the abbreviation IW is widely used for "Irregular Warfare", which, while related, is a much broader term.

At least two approaches exist to defining Information Warfare. One uses the term very broadly and includes all activities in the information domain and related functional areas. The second, more contemporary and narrow usage of the IW/IO terms, only focuses on the content and the cognitive effect of information. The findings in this paper are listed chronologically to demonstrate how the terms' usage evolved. First, Information is defined in the framework of the interdisciplinary Knowledge Management, then the paper describes more technical definitions, used in computer science, to reach the intended meaning of the terms – the cognitive effect of the information influence.

Information Defined

To be useful, information must be relevant and prompt; hence, not all information has equal value. When present in massive quantities, irrelevant information becomes just data and can cause cognitive overload and prevent us from understanding it and appreciating what part is valuable. Before finding the

proper definition for "Information warfare" and "Information operations", it is critical to define what information is. The task is made more attainable by the evident and widely accepted validity of the interdisciplinary science of Knowledge Management (KM) [7]. Knowledge management is "the management of an environment where people generate tacit knowledge, render it into explicit knowledge, and feed it back to the organization" [1]. Tacit knowledge is personalized know-how difficult to describe, while explicit knowledge can be written, recorded, stored, and transferred to others.

As KM defines it, while data are just facts out of context, Information is a set of data or facts in context or "data that has been given meaning by way of relational connection" [3]. Knowledge is actionable or contextualized Information (tacit or explicit) or "justified true belief" [7], and wisdom is knowledge of what is proper or reasonable [15]. For the paper, this crash course in KM provides a sufficient explanation that "information is data in context". The information must be relevant and prompt to be adequately contextualized and become knowledge that can motivate people and drive their behavior.

Information Warfare – a broad interpretation

We can trace the modern usage of the term "Information war" back to the 1968 book by the Canadian cultural theorist Marshall McLuhan and Quentin Fiore, War and Peace in the Global Village [5]. Decades before the information revolution caused by the Internet, the book predicts the perceptual changes caused by unlimited information delivered by mass media. The authors' view is that progressing communication technologies are making the world smaller and are turning it into a "global village". They predict a decentralized planet without boundaries because the most precious commodity, electronic information, moves worldwide without limits at the speed of electrons. The concept sounds familiar now but was visionary for its time. In the conception of this book, information war refers to using the content of the messages. In a later book, McLuhan even predicts: "World War III is a guerrilla information war with no division between military and civilian participation". The most popular understanding of the term "Information warfare" has come full circle because this early definition was about content; the term broadened, and nowadays, many analysts again are using and advocating a narrower conception.

In his 2001 book Information Warfare: How to Survive Cyber Attacks [4], Michael Erbschloe discusses attack strategies and threats to the information infrastructure and searches for defensive measures. He uses the term "Information warfare" to refer to what now, 20 years later, the literature calls "Cyberwarfare". Such usage is an example and a reminder of how rapidly terminology and semantics change in informational technologies and computer science.

Another example is Daniel Ventre's 2009 book, Information Warfare, which claims to be introducing the term without presuming to solve the question of defining it beyond doubt. The author draws examples from the practice in the United States, India, China, Russia, Singapore, and Japan. He employs the term to refer to "a range of operations carried out in the information world" [13], meaning the digital domain. The usage of IW in both books is either broader or utterly different from its predominant contemporary usage, thus creating ambiguity that requires clarification.

A 2013 RAND Corporation report states: "Debate over the meaning and even significance of the term information warfare extends back at least 15 years" [11] (i.e., since 1998). The authors define IW as "conflict between two or more groups in the information environment", which is somehow useful but again too vague. Does it involve only the content or a struggle to destroy or silence the opponent's technological capabilities? The authors admit the controversy but without focusing on the content itself: "The basic point of contention seems to be the scope of information warfare: whether it is limited to: [a] conducting or defending against electronic attacks on computers and related information systems or [b] whether it also includes the whole spectrum of possibilities for using information effectively in warfare and denying enemies the same capability".

US Joint Publication 3-13, Information Operations defines the term (abbreviated IO) as: "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and poten-

tial adversaries while protecting our own" [6]. For the present research, this definition is also too broad. It includes all activities and various doctrinally defined functional areas such as Electronic Warfare (EW), Computer network operations (CNO), Network Operations, Electromagnetic Spectrum Operations (EMSO), Information Operations (IO), Signals Intelligence (SIGINT), Military Information support operations (formerly PSYOP), Public Affairs Operations, Knowledge Management, etc. In contrast, this paper is primarily interested in the cognitive effects of information and disinformation and how they change people's perspectives.

Practical and narrow sense usage

Over time the understanding and meaning of the terms moved away from the broad categorization outlined above, which included all electromagnetic or cyber domain interactions and activities. Some academic sources provide a classification of information disorder types used as a tool in information operations. Many practitioners also offer applicable definitions and characterizations of related terms. The terminology evolves frequently, and this paper presents the most relevant definitions and lexicon for crafting a strategy for countering malign foreign Cognitive Information Warfare. One issue with American sources is that they predominantly look at IO as a primarily military endeavor. Such is the observation of a Congressional research paper from 2018. "While IO in the United States tends to be seen as a purely military activity, other countries and terrorist organizations have robust information warfare strategies and use a whole-of-government or whole-of-society approach to information operations" [2].

To prove the point, even the RAND Corporation researchers focus on operations with Information, defining them as influence operations designed for the "collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent". The term "Information disorder" refers to the level to which an individual is willing and actively engaging in spreading falsehoods. In a world over-connected by the Internet, search portals, and social media, everyone can become a creator or amplifier of information. "Disorder" is when a person develops or spreads incorrect information with malign intent. The Council of Europe's report from 2014 discusses types of information disorder and lists them by falseness and intent to harm:

- Misinformation – unintentional mistakes or when falsehood is taken seriously.
- Disinformation – fabricated or deliberately manipulated content. Intentionally created conspiracy theories.
- Malinformation – deliberate publication of private information other than such of public interest. Intentional change of context, date, or time of genuine content.

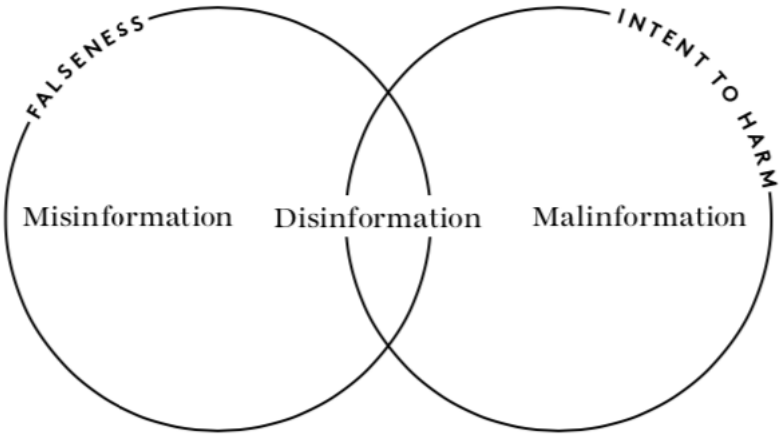


Figure 1: Types of Information Disorder
Source: Wardle, C. & Derakshan, H. [14]

This classification interprets the information defined by Knowledge Management – as truth in context, focusing on the messages, not on the technology built to store, carry, and transmit them.

Facebook (currently Meta) is one of the main targets for accusations of amplifying and allowing falsehoods to spread. The company is attempting to grasp and deal with the issue. In a report from 2017, Facebook defines "Information operations" as: "actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome. These operations can use a combination of methods, such as false news, disinformation, or networks of fake accounts aimed at manipulating public opinion (we refer to these as 'false amplifiers')" [9].

Cognitive Information Warfare

In the 21st century, information increasingly reaches peoples' minds through adaptive media – one that recognizes their preferences and can adapt to retain their attention, thus exploring and amplifying biases to form their understanding of reality. This transformation in social and cognitive matters did not happen overnight but was gradually and incrementally made possible by technological innovations like the Internet and social media.

A NATO Review paper describes Cognitive Warfare as the type of warfare in which "the human mind becomes the battlefield". The article defines it as "the weaponization of public opinion by an external entity, for the purpose of influencing public and/or governmental policy or for the purpose of destabilizing governmental actions and/or institutions" [8]. The objective of Cognitive Warfare is to alter what and how people think and to influence their behavior by shaping and influencing individual and collective beliefs, motivations, and ultimately actions.

Cognitive warfare is a combined arms approach of several warfare disciplines. Cyberwarfare deals with the means to deliver messages to the target through technological capabilities and prevent others from doing it. Information Warfare aims to control the targeted individual or population's information. It is important to remember that information can be conveyed through words, images, and actions, including kinetic means. Psychological warfare's goal is to control and manipulate the content of verbal, graphic, and other messages to influence the targets' feelings and beliefs. Altogether, these types of warfare become a means to an end in Cognitive Information Operations (CIO).

Conclusion

Considering the lack of universally agreed definitions for "information warfare" and "information operations", this article advocates referring to their narrow meanings and emphasizing the content and its effect rather than the media or methods for message delivery. In an attempt to organize cognitive defense the focus needs to stay on the cognitive effect of the information campaigns and how they influence the audience's sentiments, way of thinking, and behavior. Consequently, societies, organizations, and governments shift their attitudes and policies. Cognitive Information Operations (CIO), in this sense, are used not only against foes but also to influence sympathetic and impartial populations, including to counter the adversary's effort in this and other domains.

References

1. Brackett, M. H. (2014). *Data Resource Data : A Comprehensive Data Resource Understanding*. Bradley Beach, NJ: Technics Publications. Retrieved from https://www.dataversity.net/the-data-information-knowledge-cycle/
2. Congressional Research Service. (2018, March 5). *Information Warfare: Issues for Congress*, R45142. Retrieved from

https://www.everycrsreport.com/files/20180305_R45142_c92c6be5763f84c05aee8a79ebe1727814d8da8d.pdf
3. Crockett, L. (1999). *Fundamental issues in honors teaching: data, information, knowledge and wisdom on the wired campus*, (10.10.1999).
4. Erbschloe, M. (2001). *Information Warfare: How to Survive Cyber Attacks*. Osborne/McGraw-Hill. Retrieved from https://search-ebscohost-com.nduezproxy.idm.oclc.org/login.aspx?direct=true&AuthType=ip,url,uid&db=cat04199a&AN=ndu.200610&site=eds-live&scope=site
5. Fiore, Q. & McLuhan, M. (1968). *War and Peace in the Global Village*. Bantam Books. New York.
6. *Joint Publication 3-13, Information Operations, Incorporating Change 1, 20 November 2014* (Approved for incorporation into JP 1-02 with JP 3-13 as the source JP.) (2012).
7. Nonaka, I. (1994). *A Dynamic Theory of Organizational Knowledge Creation*. Organization Science, 5(1), 14–37. http://www.jstor.org/stable/2635068
8. NATO Review. (2021, May 20). *Countering Cognitive Warfare: Awareness and Resilience*. Johns Hopkins University & Imperial College London. Retrieved from https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html
9. Nuland, W., Stamos, A., Weedon, J. (2017). *Information Operations and Facebook.* Retrieved from https://about.fb.com/wp-content/uploads/2017/04/facebook-and-information-operations-v1.pdf
10. nytimes.com. (2018, November 12). *Operation InfeKtion: How Russia Perfected the Art of War*. Retrieved from https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html
11. Porche, I., Paul, Ch. & Center, A. (2013). *Redefining Information Warfare Boundaries for an Army in a Wireless World*. Rand Corporation Monograph Series. Santa Monica, CA: RAND Corporation. Retrieved from https://search-ebscohost-com.nduezproxy.idm.oclc.org/login.aspx?direct=true&AuthType=ip,url,uid&db=nlebk&AN=608705&site=eds-live&scope=site
12. RAND, Topics, Information Operations. Retrieved from https://www.rand.org/topics/information-operations.html
13. Ventre, D. (2009). *Information Warfare*, John Wiley & Sons, Incorporated, ProQuest Ebook Central. Retrieved from https://ebookcentral-proquest-com.nduezproxy.idm.oclc.org/lib/nationaldefense-ebooks/detail.action?docID=1106528.
14. Wardle, C. & Derakshan, H. (2017, October). *Information Disorder. Toward an interdisciplinary framework for research and policymaking,* Council of Europe. Retrieved from http://tverezo.info/wp-content/uploads/2017/11/PREMS-162317-GBR-2018-Report-desinformation-A4-BAT.pdf
15. *Wisdom* (noun (1)). In Merriam-Webster's online dictionary (11th ed.). Retrieved from: https://www.merriam-webster.com/dictionary/wisdom

WEAPONS, TECHNOLOGIES, LOGISTICS

BURNING CHARACTERIZATION OF HETEROGENEOUS PROPELLANT AT HIGH PRESSURES

Florin-Marian Dîrloman*, Traian Rotariu*, Adrian-Nicolae Rotariu*, Gabriel-Flavius Noja, Mihai-Ionuț Ungureanu*, Daniel-Neculai Zvîncu*, Alexandra-Ioana Dan***

**Military Technical Academy "Ferdinand I" 39-49 Av. George Cosbuc, Bucharest, Romania*
florin.dirloman@mta.ro, traian.rotariu@mta.ro, adrian.rotariu@mta.ro, mihai.ungureanu@mta.ro, daniel.zvincu@mta.ro, ioana.dan@mta.ro
*** Military Equipment and Technologies Research Agency, 16 Aeroportului Street, Clinceni, 077025 Ilfov, Romania, gnoja@acttm.ro*

***Abstract**: This paper describes the experiments performed for the investigation of the burning characteristics of a 'green' composite rocket propellant. For this purpose, a heterogeneous mixture comprising: phase-stabilized ammonium nitrate and ammonium perchlorate as oxidizers, aluminum as metallic fuel and polyurethane matrix as binder, was subject to experimental testing consisting in burning investigations in a closed vessel system. The collected data will be utilized to characterize the burning behavior of this type of energetic mixture in a subscale rocket motor.*

***Keywords**: internal ballistics, closed vessel, composite rocket propellant, burning rate*

1. Introduction

Solid rocket composite propellant is referred to a class of energetic heterogeneous mixture, which is mainly composed from a crystalline material (oxidizer), a metallic powder (fuel) and a polymeric matrix (binder) [1,2]. The main physico-chemical transformation of these energetic formulations is represented by controlled combustion, process in which the chemical energy is converted into thermal energy of gaseous reaction products resulted, and afterwards into kinetic energy, depending on the special structural mechanical configuration of the composite [2]. The combustion phenomenon can be predicted by creating a burning law, which can be revised by enabling the propellant to burn in parallel layers between specific boundaries [2,3].

In order to design and develop a launching system, the experimental firing trials are mandatory for a thorough ballistic characterization. Thus, the closed vessel tests are conducted to determine the burning rate law. The thermodynamic processes of internal ballistics represent a series of extremely complex phenomena, which involve the initiation and combustion of the propellant, the generation of combustion gaseous products at very high temperatures, the transformation of the caloric energy of these gases into kinetic energy. The above-mentioned processes are interdependent and occur simultaneously [4-6].

A key step in computing internal ballistic processes is identifying the characteristics of the burning mechanism. Various equations are used to estimate the values of these parameters in conjunction with experimental pressure-time patterns. When performing tests in a closed vessel system, the data collected by piezoelectric pressure transducers is converted and analyzed to predict the pressure variation of the system [4-6].

Interior ballistics focuses on the theoretical and experimental determination of thermochemical parameters that directly influence the combustion of propellants into the motor chamber as well as the design of combustion calculation models. The main characteristics that can be achieved by firings in closed vessel are: maximum pressure value, propellant force, co-volume, pressure exponential coefficient and the progressivity [6-8]. Given the lack of data in the literature on this topic, this study aims to provide some additional information on the burning characteristic of "green" rocket propellants. Thus, this paper describes the experimental investigations that were carried out in a closed vessel system as well as the strategy used to calculate the values of the relevant parameters.

Materials and methods

The technical details of the investigated type of composite rocket propellant, the ballistic equipment employed, and the characterization process are provided in the sections that follow.

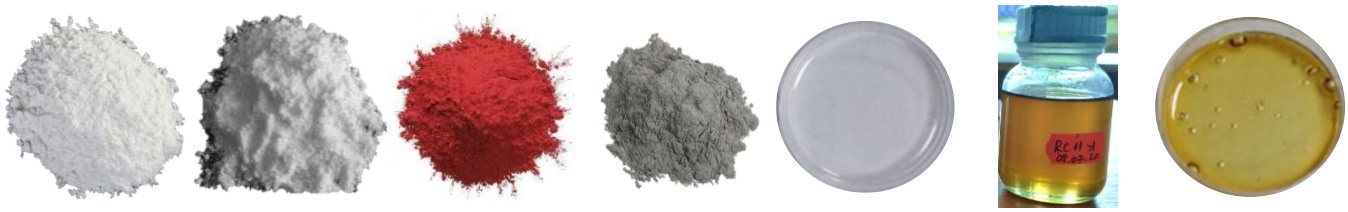
Materials

The following materials were used in the development of the composite rocket propellant: a polyester-polyol **RP1** obtained from PET degradation [9], Setathane D1160 (**SET**, hydroxyl content – 5.4%, Allnex), diphenylmethane-4,4′-diisocyanate (**MDI**, -NCO content – 31.5%, Covestro), phase-stabilized ammonium nitrate with potassium nitrate (**PSAN**) and ammonium perchlorate (**AP**) were vacuum dried prior to use [10]. The metallic fuel employed for these energetic formulations was aluminum (Al), while iron oxide (Fe_2O_3) was used as catalyst.

Methods

2.2.1 Propellant formulation manufacture

The chemical composition and the distribution of the components of the heterogeneous energetic formulation designed for rocket propellants have multiple effects on their performance, stability and sensitivity characteristics. To obtain a uniform distribution of the solid components of the energetic mixture, it is necessary to use dry components with appropriate particle sizes. Thus, the first step in the development of the "green" energetic formulation, intended for use as rocket propellant, was prepping the raw materials. It is well known that AP, PSAN and the components of the binder (polyols and isocyanates) are hygroscopic, therefore these formulations should not contain any water, or at least their water content should be kept under a reasonable level. Consequently, these components must be dried prior being mixed. Drying was carried out in a vacuum oven at 60°C for 48 hours. In addition to being essential for achieving propellant uniformity, the granulometrically dimensions of the constituents also have a significant impact on the burning rate. In order to obtain the maximal burning performances, the oxidants were dried, mashed, and granulometrically separated, and only the fraction containing solid particles with dimensions of 50 and 200 μm were afterwards added to the mixture. The two oxidizers were mixed with the metallic fuel (Al) and catalyst (Fe_2O_3) until they were evenly spread between each other. The polymeric binder employed for these energetic formulations was obtained by reacting a polyisocyanate (MDI) with a mixture consisting of commercial polyol SET and polyol synthesized from the degradation of PET post-consumer waste, RP1. The blend of polyols was firstly thoroughly mixed with the solid components. The addition of aromatic isocyanate MDI was the final step in the solid propellant manufacture process. Figure 1 depicts the aspect of the materials involved in the manufacture process, while Table 1 shows the composition of the energetic formulation herein reported.



PSAN **AP** **Fe_2O_3** **Al** **SET** **RP1** **MDI**

Figure 1: The compounds used for the manufacture of "green" rocket propellants

Table 1. The composition of the rocket propellant composite

Sample	Components [wt.%]							Density [g/cm³]
	Binder			Oxidizer		Fe_2O_3	Al	
	15			72				
	SET	RP1	MDI	AN	AP			
SRM_1	19.3	34.9	45.8	60	40	1	12	1.52

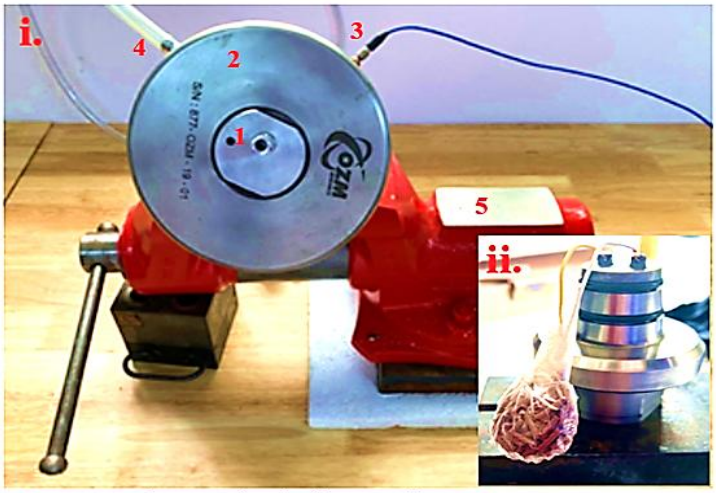
For the experimental tests conducted into the closed vessel, the rocket composite mixture was extruded into small cylindrical configuration with a diameter of 1.71mm and a length of approximately 7 mm, as presented in Figure 2.

cylindrical configuration **diameter and length measure**

Figure 2: The configuration and the dimensions of the propellant samples

2.2.2. Rocket propellant characterization

The procedure consists in measuring the pressure variation over time, established by the gases resulting from the decomposition of the propellant amount in the combustion chamber. Thus, to be able to determinate the ballistic characteristics, the pressure–time profiles $p(t)$, resulted by the combustion of the tested propellant were measured by using a closed vessel, with an volume of the inner chamber of 40 cm^3. The pressure data was obtained by a piezoelectric transducer, with a frequency of response of 25 kHz, which allows measurement with a maximum error of ±0.1 connected to a PICOSCOPE series 6000 oscilloscope. The propellant charge was ignited by using powdered composite mixture based on ammonium perchlorate (71%), aluminum (14%) and polyurethane (15%) and a MB2-N electrical igniter. The experimental investigations were conducted at ambient temperature. The structural configuration of the closed vessel and the propellant amount are presented in Figure 3.



1 - locker with electrical ignition terminals; 2 - closed vessel cap;
3 - pressure transducer; 4 - gas exhaust valve; 5 - fastening stand.

Figure 3: Structural system configuration
(i. closed vessel system; ii. tested sample)

Results and discussions

Taking into account the inner volume of the closed vessel, the experimental tests were conducted for two loading densities of $\Delta_1 = 100\ kg/m^3$ and $\Delta_2 = 150\ kg/m^3$. The data acquired during the experimental investigation are plotted in Figure 4.

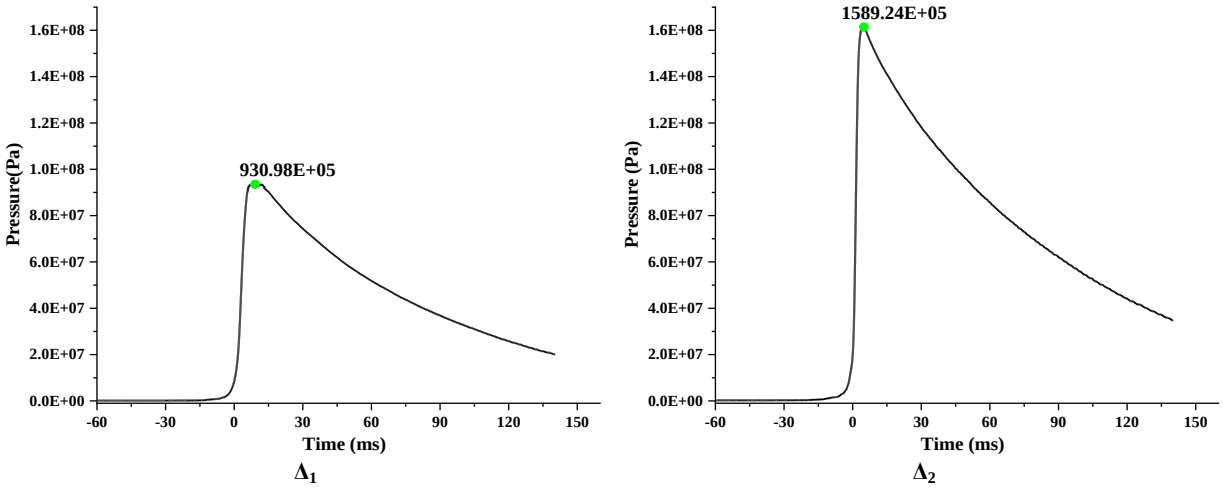


Figure 4: The p(t) profiles for the two loading densities

In this instance, it appears that loading density has an impact on the pressure values and burning time of the composite rocket mixture. As a consequence, the lowest loading density presents the lowest pressure value and the longest burn time. The higher value of pressure leads to a higher value of the burning rate of propellant. Through experimental tests in the manometric bomb, Noble and Abel established the dependence of the maximum pressure on the loading density, expressed by the following equation [4, 7]:

$$p_{max} = \frac{f\Delta}{1 - \alpha\Delta} \tag{1}$$

where:
Δ - loading density, [kg/m^3]; **f** - propellant force**,** [J/kg] **α** - co-volume [m^3/kg].

Thus, based on the previous equation and the maximum pressure values for the two charge densities, the coefficients of interest in the gas equation of state, such as the propellant force (f) and co-volume (α), can be determined using Equations (2) and (3).

$$\alpha = \frac{\Delta_1 p_{max2} - \Delta_2 p_{max1}}{\Delta_1 \Delta_2 (p_{max2} - p_{max1})} \tag{2}$$

$$f = \frac{P_{max2}}{\Delta_2} \cdot \ 1 - \alpha \cdot \Delta_2 \tag{3}$$

For the analyzed mixture the calculated values for the propellant force and co-volume: α = 0.002 m^3/kg and f = 6.867•10^5 J/kg. The fraction of burned propellants (Ψ(t)), can be calculated with Equation (4), as function of loading density (Δ), propellant density (δ), pressure variation (p(t)), force (f) and co-volume (α).

Once the (t) is calculated, by adjusting the equation (4), the formula for the coefficient of the pressure exponent can be express by equation (5). Figure 5 depicts the (t) and (Ψ) profiles.

$$\psi(t) = \frac{\frac{1}{\Delta} - \frac{1}{\delta}}{\frac{f}{p(t)} + \alpha - \frac{1}{\delta}} \tag{4}$$

$$\upsilon = \frac{ln \left(\frac{d\Psi}{dt}\right)_{\Delta_2} - ln \left(\frac{d\Psi}{dt}\right)_{\Delta_2}}{ln\ p_{\Delta_2} - ln\ p_{\Delta_3}} \tag{5}$$

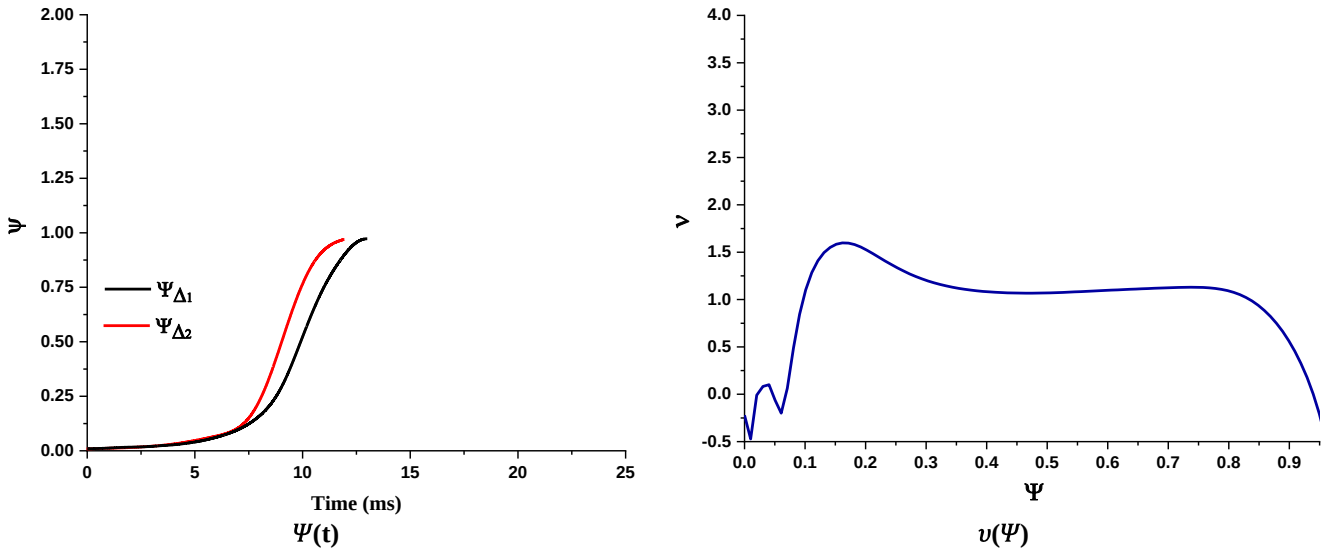


Figure 5: The (t) and (Ψ) profiles for the analyzed sample

From the calculated data presented in Figure 5, the average value of exponential burning coefficient is around 1.12. A significant variation from this value can be observed in the ignition stage of the composition, when the pressure values are low because this process is slower than that of a gun powder propellant.

The burn rate characteristics were determined without any restriction to the evolution of the burning surface. Based on the experimental data, the variation coefficient of progressivity as function of the fraction, σ(Ψ), can be express as Equation (6). The progressivity profiles for the two loading densities are depicted in Figure 6.

$$\sigma\ \psi\ = \frac{d\psi}{dt} \cdot \frac{\Lambda_0}{S_0} \cdot \frac{1}{A \cdot p^{\upsilon}} \tag{6}$$

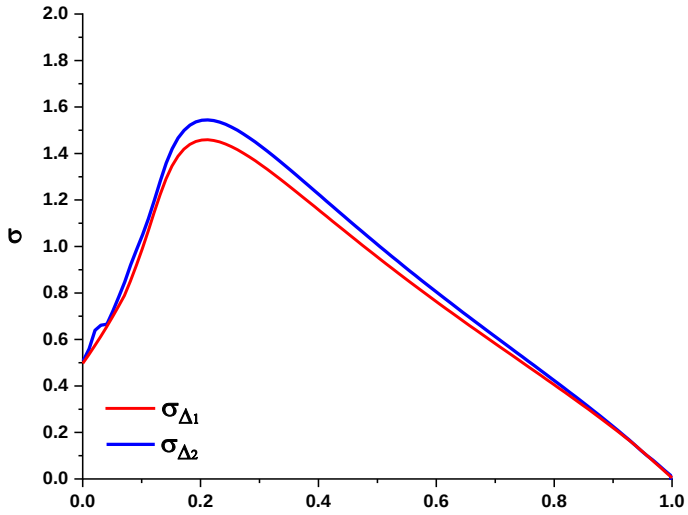


Figure 6: The σ(Ψ) profiles for the two loading densities

The propellant is high progressive for fraction values in interval 0 to 0.22. At higher values of the fraction, the progressiveness coefficient starts to decrease slowly.

Conclusions and perspectives

Establishing the ballistic characteristics of solid composite propellants is the first step before introducing these energetic mixtures into the rocket launch system. For this reason, a heterogeneous solid mixture based on PSAN, AP, Al, Fe_2O_3 and polyurethanic binder, developed from the polyester-polyols derived from PET degradation, was subjected to a series of experimental static combustion on a closed vessel system to determine characteristics of burning.

Based on the obtained data, it was proven that the combustion mechanism is directly influenced by the loading density of the closed vessel. Another factor that influences the values of the combustion parameters and which was not took into consideration was the heat dissipation in the inner chamber wall. Thus, this study provides the perfect background for further studies in the future for this type of energetic mixtures.

Acknowledgments

This work was funded by the Romanian Ministry of Education and Scientific Research (UEFISCDI), project number PN-III-P2-2.1-PTE2021-0211- ctr. no. 75PTE/2022 and PN-III-P2-2.1-PTE-2021-0514 - ctr. no. 80PTE/2022.

References

1. Agrawal, J.P. (2010). *High Energy Materials: Propellants, Explosives and Pyrotechnics*, pages 209–316, Weinheim, Germany: John Wiley & Sons.
2. Kubota, N. (2015), *Propellants and Explosives: Thermochemical Aspects of Combustion* pages 69–110, Weinheim, Germany: John Wiley & Sons.

3. Rotariu, A. N., Matache, L., Bucur, F., Cîrmaci-Matei, M. V., Mărmureanu, M. & Trană, E. (2020), Implementation of a gumbel distribution function in interior ballistic calculations for deterred propellants, *U.P.B. Sci. Bull., Series B*, vol. 82 (1).
4. Carlucci, D.E., Jacobson S.S. (2008). *Ballistics. In Theory and Design of Guns and Ammunition*, USA: CRC Press.
5. STANAG 4115: *Definition and Determination of Ballistic Properties of Gun Propellants*, 2nd ed. Military Agency for Standardization: Brussels, Belgium, 1997.
6. Corner, J. (1950). *Theory of the Interior Ballistics of Guns*, New York: John Wiley.
7. Titică, V. (1993). *Balistica interioară a gurilor de foc*, Vol. 1, Bucureş ti, Romania: Editura Academiei Tehnice Militare.
8. Serebryakov M. E. (1972). *Interior Ballistics of Tube Weapons and Solid Fuel Rockets*, Moscow: State Scientific and Technical Publishing House Oborongiz.
9. Dîrloman, F.M.; Toader, G.; Rotariu, T.; Ţigănescu, T.V.; Ginghină, R.E.; Petre, R.; Alexe, F.; Ungureanu, M.I.; Rusen, E.; Diacon, A.; Ghebaur, A.; Duldner, M.; Coman, A.E.; Ţincu, R. Novel Polyurethanes Based on Recycled Polyethylene Terephthalate: Synthesis, Characterization, and Formulation of Binders for Environmentally Responsible Rocket Propellants. *Polymers* **2021**, 13, 3828. https://doi.org/10.3390/polym13213828
10. Dîrloman, F.M.; Rotariu, T.; Ţigănescu, T.V.; Toader, G.; Zecheru, T.; Iordache, T.V. Phase stabilized ammonium nitrate for future green rocket propellants. *UPB Sci. Bull.* **2021**, *83*, 87–100.

ASSESMENT OF A NEW THERMOMARIC SOLID COMPOSITION USED IN EFP-TB TANDEM AMMUNITION

Liviu C. Matache, Andrada M. Runceanu, Adrian N. Rotariu, Florin M. Dirloman, Răzvan M. Mircioagă, Cristian Moldoveanu, Pamfil Șomoiag

Faculty of Integrated Systems of Armaments, Engineering and Mechatronics, Military Technical Academy „Ferdinand I", Bucharest, Romania, andrada.runceanu@mta.ro

***Abstract**: Thermobaric munitions represent one of the non-conventional munitions that are designed to produce heat and pressure effects. They may also be found in specialty literature as "fuel-air explosives" or „aerosol bomb". Due to its proprieties and characteristics thermobaric ammunition is very effective in closed or semi-closed spaces.*

In this paper we propose an evaluation of a new solid thermobaric composition, based on metal powders, such as aluminum (Al), magnesium (Mg), a high explosive such as hexogen (RDX) and an organic binder, which has the role of strengthening the thermobaric composition and decrease the explosive sensitivity to mechanical stimuli. In addition, a comparison between overpressures and impulses was made in all cases.

***Keywords**: thermobaric, metallic powders, pressure of explosion, hexogen, composite*

Introduction

The thermobaric weapons are classified in the category of volumetric weapons. Target destruction is mainly achieved by the shock wave of thermobaric explosives.[1][2] The volume of the explosion, in the case of thermobaric explosives, does not have the sole purpose of maximizing the pressure, unlike secondary, conventional explosives, such as trinitrotoluene (TNT) which have a lethal effect based on the maximum value of overpressure that produces wounds and injuries. In the case of thermobaric ammunition the impulse has a greater importance. [3]

In general, the thermobaric explosives (TBX) and enhanced blast explosives (EBX) are defined and categorized as liquid and solid mixtures and advanced compositions including layer charges. In this concept thermobaric explosive (TBX) consists of a central charge (called the core), which is a high explosive, and an external secondary charge (fuel-rich formulation) [4][5]. Shock wave produced by thermobaric charge detonation has a longer positive phase and a bigger magnitude of impulse than a classical condensed explosive, even the maximum peek pressure is lower, as you can see in Figure 1.

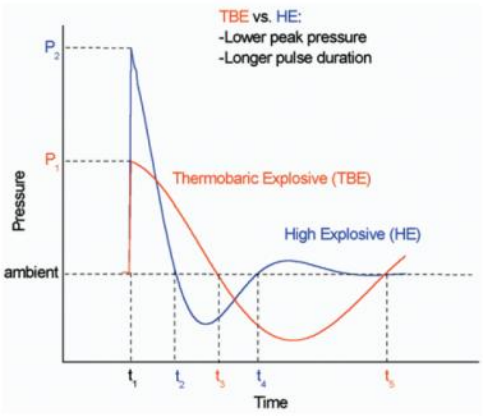


Figure 1: Comparation between thermobaric and condensed explosives [4][6]

Tandem charge it is a concept of two or more explosive charges that detonate in a controlled manner in order to enhanced the destructive effect. Usually tandem ammunition are designed to fight against reactive armour, but can be used against non-explosive reactive armour as well.

As part of a research project, ATM"FI" specialists designed and produced a tandem ammunition consisting of two stages: one EFP (Explosively Formed Penetrator) and one TB (thermobaric), as can be seen in Figure 2.

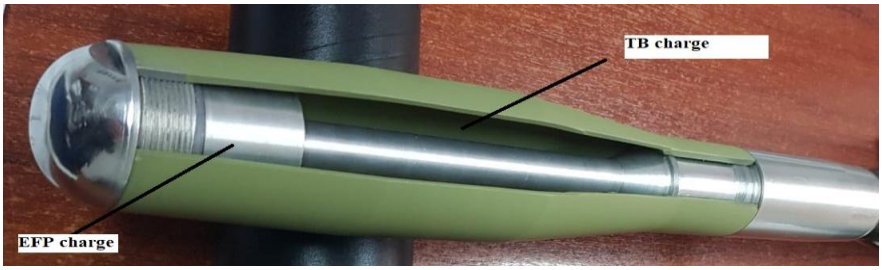


Figure 2: EFP-TB Tandem charge configuration

The internal design of this ammunition presents an innovative character and combines the two stages EFP and TB in order to maximaze the effect on the target, by piercing it and the deflagration of the thermobaric composition both outside and inside the target (fighting vehicle, houses, etc.).

For this configuration we designed and synthesized a solid thermobaric mixture, which was evaluated through experimental tests in the firing range, as shown below.

1. Thermobaric mixture synthesis

Composition design

Two types of thermobaric compositions were designed:

a) 10% binder; 15% RDX; 20% Mg; 55% Al
b) 10% binder; 15% RDX; 35% Mg; 40% Al

The binder, in both cases, consists of MDI and SET in a mass ratio of 0.7 to 1.

The amount of synthesized composition was calculated for an average density of 1.4 g/cm3, a height of h = 120 mm, an outer diameter of D = 70 mm and an inner diameter of d = 17 mm.

An excess of 5% was used for each component in order to compensate for possible losses.

1.2. Mixture synthesis

Three blocks were made for each type of composition. They are numbered from 1 to 6 (TBX1, TBX2, TBX3, TBX4, TBX5, TBX6), the first 3 containing 55% Al and the last 3 40% Al.

The preparation of the composition began by weighing and mixing magnesium with aluminum until a homogeneous composition is obtained, as can be seen in Figure 3.

Figure 3: Mixing magnesium with aluminum

The next step was to weigh and add the phlegmatized hexogen, as shown in Figure 4, to be mixed with the previously homogenized substances (Al and Mg).

Figure 4: Mixing RDX with homogenized substances (Mg and Al)

Manual mixing was done until the composition was completely homogenized, the binder was added afterwards, as shown in Figure 5. To avoid conglomerates, mixing has been done slowly, attentive during a longer period of time.

Figure 5: Mixing the binder

The final step consisted in loading the mixture and pressing it into the mold. This process is presented in the following images.

1.3. Block composition pressing

To obtain the final shape, the compositions were loaded into molds with a diameter of D = 70 mm and by using a 17 mm rod, the central channel was made. The pressing was done with the help of a wooden central perforated piston, as can be seen in Figure 6 and Figure 7.

Figure 6 Încărcarea compoziţiei

The final configuration was the result of several successive pressings in order to obtain a high density as well as to avoid large density variations throughout the composition.

Figure 7 Presarea compoziţiei

The density obtained are presented in the table below.

Tabel 1: The geometric and gravimetric characteristics of the composition

	Masa [g]	Înălţ imea [mm]	**Diametrul [mm]**	**diametrul int [mm]**	**Volumul [cm3]**	**Densitatea [g/cm3]**
TBX1	550	98	**71.4**	**17.500**	**368.626**	**1.492**
TBX2	572	100	**71.4**	**17.500**	**376.339**	**1.520**
TBX3	557	105	**71.4**	**17.500**	**395.157**	**1.410**
TBX4	578	114	**71.4**	**17.500**	**429.028**	**1.347**
TBX5	566	114	**71.4**	**17.500**	**429.028**	**1.319**
TBX6	551	113.3	**71.4**	**17.500**	**426.393**	**1.292**

Block composition testing

Equipment used

The following equipment was used to determine the fireball size and pressure variation with time:

- High speed camera FASTCAM SA-Z – it allowed recording data in natural light conditions up to 50,000 fps;
- Laptop – for storing and analyzing the data provided by the high speed camera;
- Pressure sensors type PCB 102B06;
- Modul for aquisition data and signal conditioner;

- Power generator;

Pressure transducers were mounted "side on" to record static pressure. The location distance of the transducers was 1 m, 2 m and 3 m from the central axis of the block, as can be seen in Figure 8.

Figure 8: Disposing of pressure transducers

Figure 9: Disposing of high speed camera

Ignition of thermobaric compositions was made using an electric blasting cap inserted in central explosive charge (RDX flegmatizat).

Obtained results

The evolution of the fireball produced by the 6 thermobaric compositions is presented in summary in Table 2.

Table 2: Evolution of fireball of the 6 thermobaric compositions

Time (ms) / Composition	0	1.12	22.8
TBX1			
TBX2			
TBX3			
TBX4			
TBX5			
TBX6			

Fireball duration data for the 6 compositions has been centralized in the table below.

Table 3: Fireball duration of compositions

Composition	TBX1	TBX2	TBX3	TBX4	TBX5	TBX6
Firebal duration(ms)	176.68	198.39	231.24	227.89	228.11	231.89

The average duration for the composition containing 55% Al is 202.10 ms, and for the one containing 40% Al is 229.30 ms.

It can be seen that after firing, the metallic fuels failed to oxidize completely, especially aluminum which needs very high temperature.

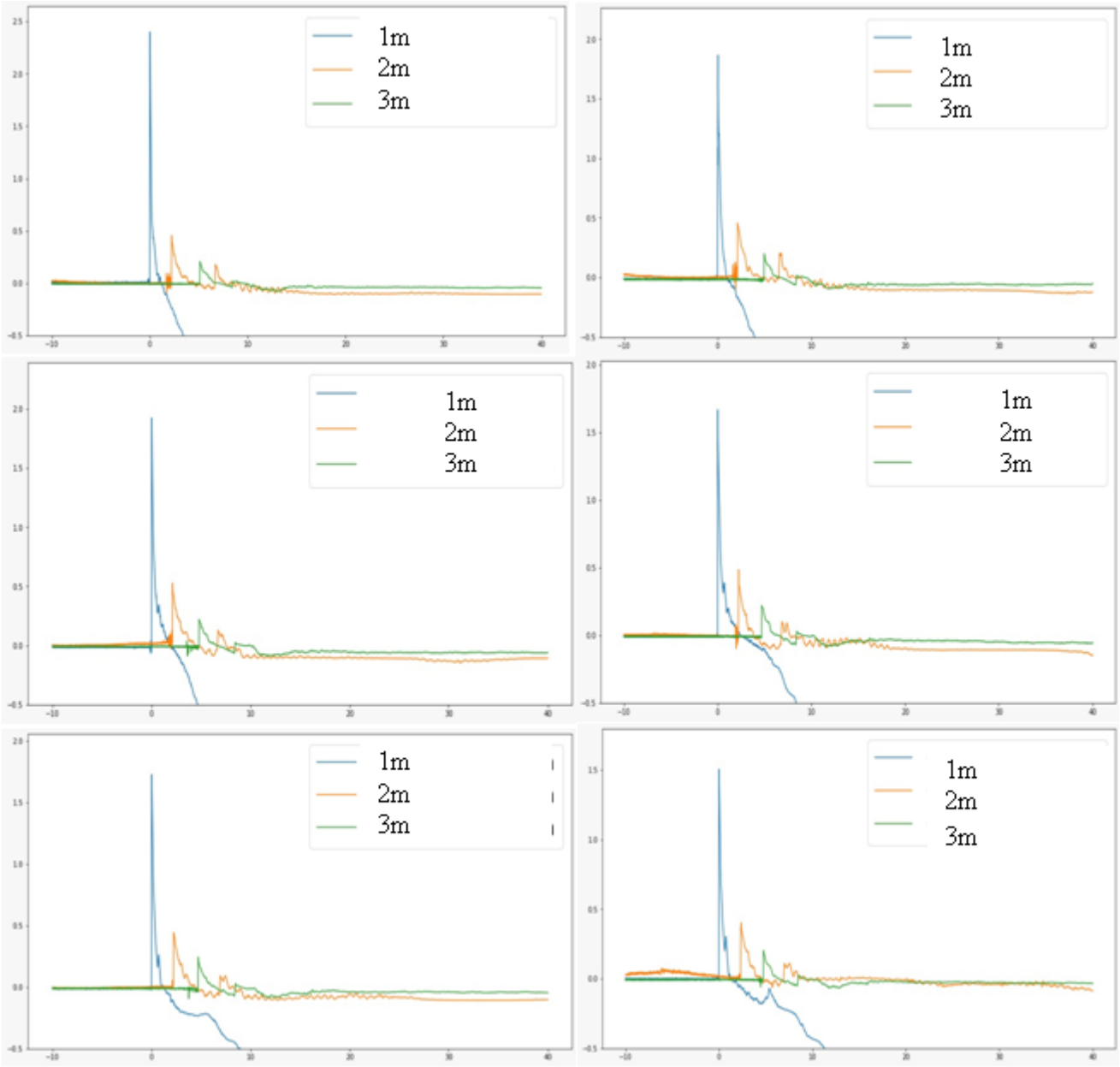


Figure 10: Pressure vs. time (time [s] pressure [bar])

The recorded pressures variation over time are shown in the figures above. At the same time, based on the time variation graph, the impulses were calculated for each individual case using a program written in Python 3.10.5. The data is summarized in Table 4.

Table 4: The calculated impulses for the 6 compositions

	Impuls la 1m[Pa*s]	**Impuls la 2 m[Pa*s]**	**Impuls la 3 m[Pa*s]**
TBX1	57,187	40,405	13,043
TBX2	50,495	40,597	10,980
TBX3	55,391	53,190	14,345
TBX4	68,944	42,753	13,772
TBX5	58,523	37,988	13,394
TBX6	59,033	33,721	13,498

Conclusions

After performing the tests, it was observed that the variation of the amount of magnesium and aluminum does not significantly influence the dimensions and duration of the fireball, but adding more magnesium increases the combustion efficiency of aluminum, obtaining a greater impulse for the compositions containing 35% Mg, as can be seen in Table 4. The maximum impulse is obtained in the case of the TBX4 composition, while the maximum pressure is obtained for the TBX 1 composition.

Acknowledgments

This work was supported by a grant of the Romanian Ministry of Education and Research, CCCDI - UEFISCDI, project number 84PTE/2022, within PNCDI III.

References

1. Michael, N. (1998) *A visual model for blast Wawes and fracture*. Master's thesis. Toronto. The Department of Information Technology.
2. https://www.globalsecurity.org/military/systems/munitions/thermobaric.htm
3. https://www.globalsecurity.org/military/systems/munitions/explosives.htm
4. Anna E. Wildegger-Gaissmaier (2004) *Aspects of the thermobaric weaponry*. ADF Health, Vol. 4.
5. Ungureanu, M. I., Matache, L. C., Rotariu, T., Barbu, C., Dîrloman, F. M., (2021), High blast explosive composition for annular thermobaric ammunitions, *UPB Scientific Bulletin, Series B: Chemistry and Materials Science* **83,** 3, 263-272.
6. Iorga, O. G., Munteanu, M., Ț igănescu, T. V., Epure G., (2018), Experimental and theoretical aspects regarding design and testing of thermobaric munitions for recoilless armament systems, *International Conference KNOWLEDGE-BASED ORGANIZATION*, XXIV, 3, 107-117.

THE CONCEPTION OF A NON-STANDARDIZED TEST FOR ASSESSING THE EFFICIENCY OF THE INNER LAYER OF THE BALLISTIC HELMETS

Rotariu Adrian-Nicolae[1], Cirmaci-Matei Marius-Valeriu[1], Bucur Florina[1], Matache Liviu[1], Pulpea Bogdan[1], Florin Dirloman[1], Adrian Malciu[2], Sava Alin[1]

[1]Military Technical Academy
Av. George Cosbuc 39-49, Bucharest, Romania

[2]Military Equipment and Technologies Research Agency
Str., Aeroportului 16, Clinceni, Romania

Abstract**:** *From a military point of view, testing standards have been established for the verification of ballistic helmets. However, the issue of how their components fulfill their mission, such as shock absorption pads, is still open. The article presents the concept of a non-standardized test, in which acceleration and pressure sensors and high speed camera are used, which highlights the efficiency of such layers by comparison with reference tests.*

Keywords*: impact test, ballistic helmet, shock absorbent*

1. Introduction

The current models of ballistic helmets used mainly composite materials in their construction and are designed to protect the military personnel against penetration by small calibre projectile or shrapnel. The impact resistance of such equipments is already standardised, both from the point of view of threats and admission criteria, as well as work procedures [1, 2].

However, over time, various non-standardized tests have been performed on such helmets on ballistic range or with impact machines [3-6]. Such research is required due to the fact that even in the absence of a penetration, the deformation of the composite structure during an impact may result in severe head injuries or less obvious traumatic brain injuries [7]. Therefore, a deformable inner layer, able to absorb energy and to mitigate the intensity of accelerations is mandatory.

In line with the previously presented considerations, the present paper discusses the issue of developing a dynamic test in which a compressed air cannon is used to impact a head surrogate equipped with such ballistic helmets, in order to assess the efficiency of the inner layer of the ballistic helmets.

2. Test concept

Currently in ballistic testing of military helmets there are standards and methods that treat differently the mechanical response of the head-neck assembly impacted by a low-mass, high-velocity projectile. On the one hand there are head surrogates that can slide together with a seating base in a direction parallel to the direction of projectile trajectory [1]. A second variant of head surrogates or human/ animal skulls are mounted on a fixed support, but which includes an elastic sub-assembly that reproduces the flexibility characteristic of the human neck [3, 6]. Also, the interpretation of the test results differs de-

pending on the approach taken The analysis tools include the classic witness plate or ballistic plastiline, but also sensors such as accelerometers, strain gauges or pressure and force transducers [3, 6].

Obviously, the test variants in which real tissues are used, coupled with extensive accessories (accelerometers, pressure sensors, strain gages), have prohibitive costs but offer much more information regarding the effects of the impact on the helmet wearer. Bearing in mind the objective of this research program, a compromise between the cost and the complexity of the test was sought.

In this sense, first of all we have opted for compressed air cannon, instead of shooting with real ammunition in military range. Such an installation generates much lower speeds but allows the use of large projectiles that can be equipped with accelerometers. Regarding the impact energy or the impact impulse, they can be matched with those specific to the bullet impact, but never both at the same time. Also, such projectiles can be provided with different geometric impact profiles: flat, spherical, conical or even ogival. Fig. 1 shows the conceptual elements of the pneumatic installation, like the existence of a protected cable inside of the barrel used to connect the projectile accelerometer (model 350C03) to the data acquisition system.

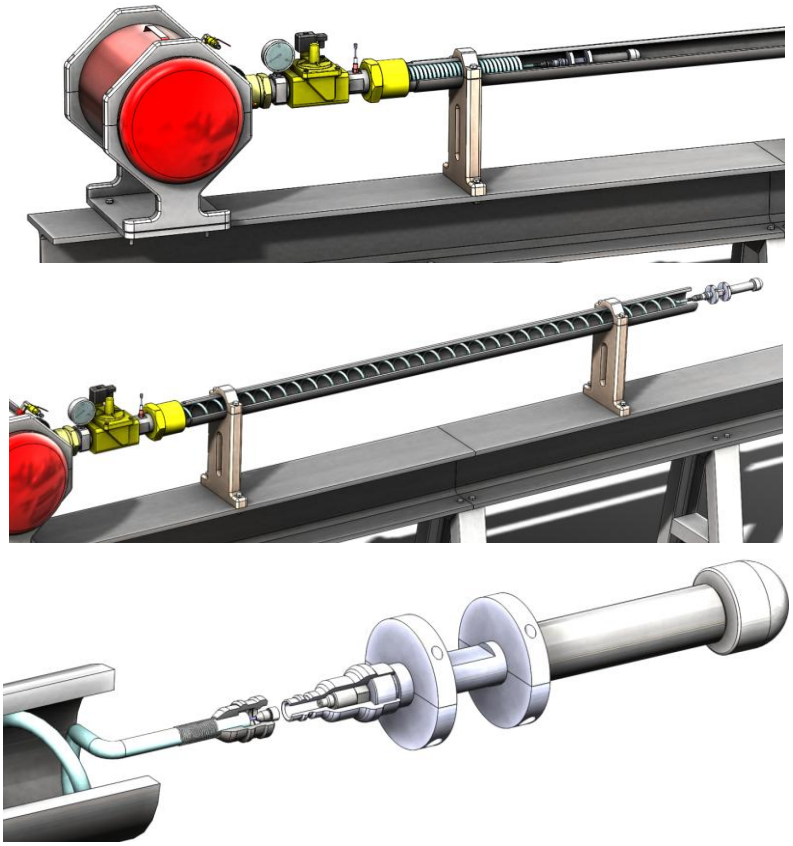


Fig. 1 Compressed air cannon with the projectile in initial position (up), out of the barrel (middle) and the detail of accelerometer connection (down)

For the target, it was decided to use a plastic skull mold, available on the market, with an empty cranial box, which can be loaded with brain-specific soft tissue stimulating material. A subassembly containing a pressure transducer (model PCB 102B15), oriented with the sensitive surface upwards, was mounted inside the cranial box as in fig. 2. The head surrogate was mounted on a fixed support, but which includes an elastic element (helicoidally spring) to take into consideration the flexibility of the human neck.

The ballistic gelatine used to fill the cranial cavity was manufactured according to the procedure provided by the manufacturer at a concentration of 10%. After heating to 39 °C the gelatine was poured through a channel made in the upper part of the skull, see Fig. 3.

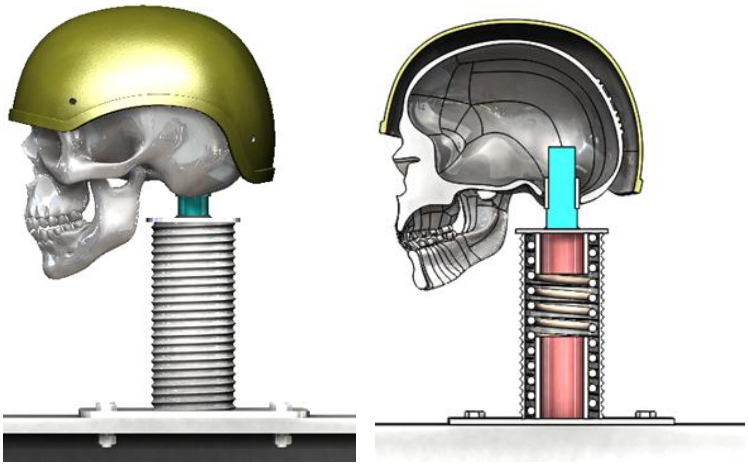


Fig. 2 Head surrogate concept with an elastic element

Fig. 3. The head surrogate preparation

3. Assessment of shock absorber layer functionality through proposed test

In order to evaluate the potential of the proposed test, were carried out tests with the ballistic helmet made of Kevlar, a model produced by STIMPEX S.A. The design of the testing stand allows arranging the surrogate in four different positions, as can be seen in Fig. 4: frontal impact, left impact, right impact and rear impact. Two types of helmets were used: helmets provided inside with polymeric foam type shock absorber elements and helmets in which these elements were removed (reference tests).

The tests were carried out with 0.4 kg projectiles with a flat head of 27 mm diameter. Using this impact head allows the same helmet to be used in multiple tests involving impact from the same direction. It was aimed to achieve an impact velocity of 14 m/s, the velocity that ensured an impact impulse twice the impulse obtained at the bullet impact for a 7.62x25 mm ammunition fired by the Tokarev TT handgun.

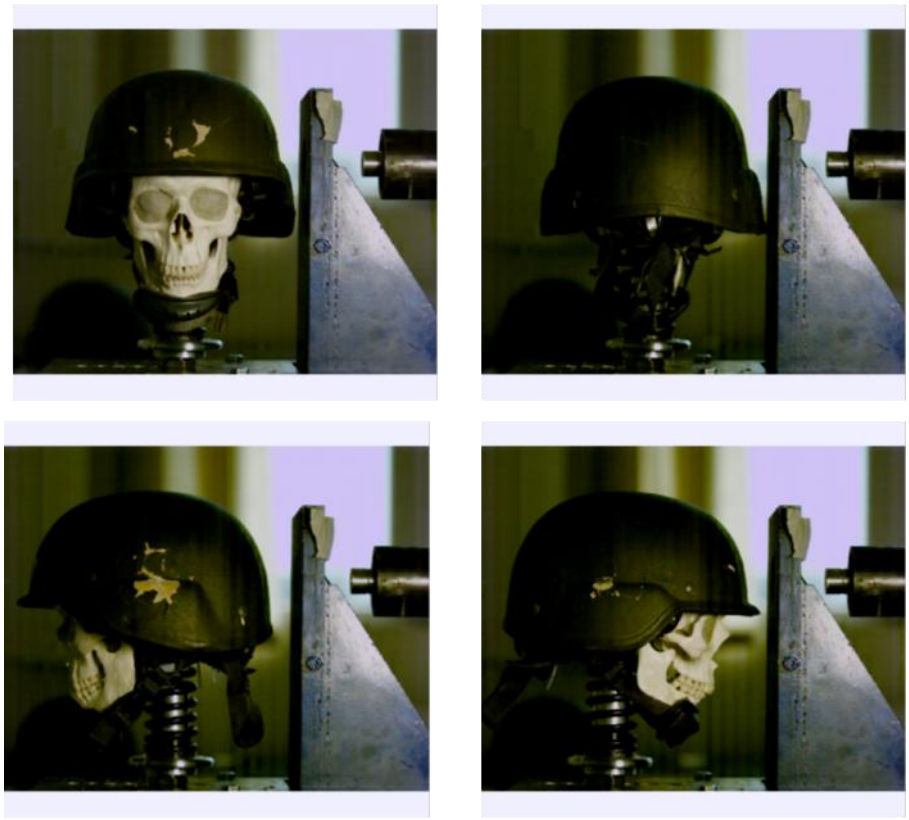


Fig. 4. The test surrogate positions

A PICOSCOPE series 6000 oscilloscope was used to acquire the data transmitted by the sensors. As an example, data acquired for frontal and rear impact tests are plotted in fig 5 and 6. In addition, in order to measure the impact velocity and to document the impact process, like in fig. 7, the tests were filmed with a high speed camera PHOTRON FASTCAM SA3 model 120K-C2, with 25000 frames per second.

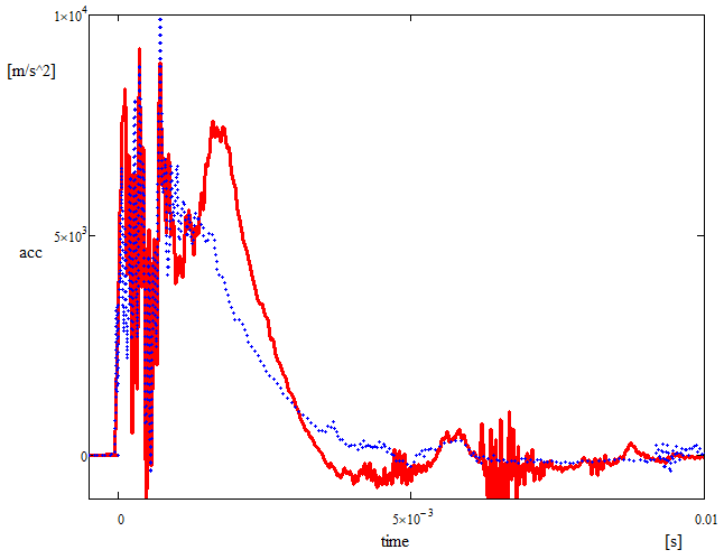


Fig. 5. The comparison of measured accelerations for frontal impact tests

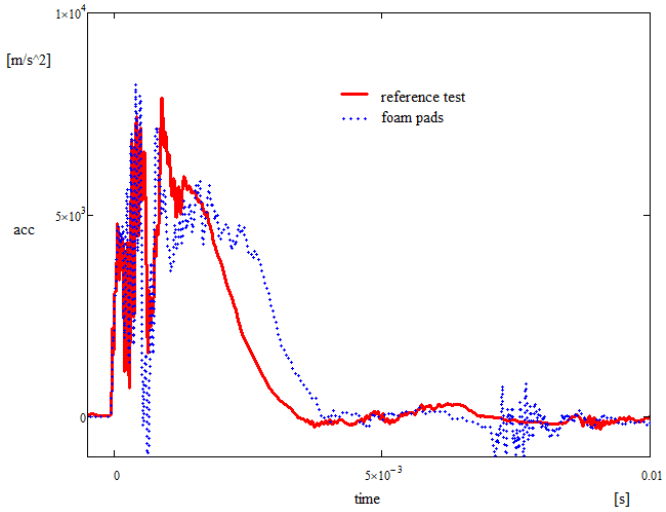


Fig. 6. The comparison of measured accelerations for posterior impact tests

Fig. 7. The images sequence for the lateral impact at a frequency of 250 fps, arranged in Z

The signals measured by the sensors placed on the projectile and inside the surrogate clearly show differences between the tests in which shock absorbing pads were used and those in which they were absent. The shocks are less intense and extend over a longer period of time than in reference tests, a situation that indicates that the pads work according to their intended purpose.

As for the analysis of the images, it clearly showed that there is a delay between the moment when the helmet is hit and the moment when the surrogate starts to move. It is also clearly visible on the footage that during the phenomenon the helmet suffers considerable deformations, but only in the elastic region, as long as at the end of the test the structure of the helmet did not suffer modifications.

4. Conclusions

Based on previous considerations, the following conclusions can be drawn:

- The non-standardized proposed test is able to highlight the functionality of the shock absorption elements through comparison with reference tests;
- The concept may be used in order to differentiate the various solutions depending on the measured efficiency;
- The potential of the test set-up may be increased through additional video analysis of the surrogate movements.

Acknowledgment

This work was supported by a grant of the Romanian Ministry of Education and Research, CCCDI - UEFISCDI, project number 44PTE/2020, within PNCDI III.

References

1. National Institute of Justice, NIJ STANDARD 0106.01 FOR BALLISTIC HELMETS, 1981;
2. USA DoD, AR/PD 10-02: HELMET, ADVANCED COMBAT (ACH), 2011;
3. C. J. Freitas, J. T. Mathis, N. Scott, R. P. Bigger, J. MacKiewicz, Dynamic Response Due to Behind Helmet Blunt Trauma Measured with a Human Head Surrogate, International Journal of Medical Sciences, 2014; 11(5):409-425;
4. K. Jamroziak, M. Bajkowski, M. Bocian, S. Polak, M. Magier, M. Kosobudzki, R. Stepien, Ballistic Head Protection in the Light of Injury Criteria in the Case of the Wz.93 Combat Helmet, Applied Sciences, 2019, vol. 9, no. 13, 2702. https://doi.org/10.3390/app9132702
5. J.-C. Sarron 1 , M. Dannawi, A. Faure, J.-P. Caillou, J. Da Cunha, R. Robert, Dynamic effects of a 9 mm missile on cadaveric skull protected by aramid, polyethylene or aluminum plate: an experimental study, J Trauma, 2004, 57(2):236-42;. doi: 10.1097/01.ta.0000133575.48065.3f;
6. H. Liu, J. Kang, J. Chen, G. Li, X. Li, J. Wang, Intracranial pressure response to non-penetrating ballistic impact: an experimental study using a pig physical head model and live pigs**,** Int J Med Sci, 2012; 9(8):655-64, doi: 10.7150/ijms.5004;
7. E. G. Blackman, M. E. Hale, S. H. Lisanby, Improving TBI Protection Measures and Standards for Combat Helmets, 2011;

THEORETICAL ASSESMENT OF OPTIMAL MULTIPLE ROCKETS LAUNCHING FOR LAROM PLATFORM

Neculai-Daniel Zvîncu, Pamfil Șomoiag, Cristian-Emil Moldoveanu, Florin-Marian Dîrloman, Costin-Dumitru Berechet

Faculty of Integrated Armament Systems, Military Engineering and Mechatronics, Military Technical Academy „Ferdinand I", Bucharest, ROMANIA, daniel.zvincu@mta.ro

Abstract: *The LAROM is a Romanian mobile multiple unguided rockets launcher that can operate with the standard 122 mm rockets, as well as with the more advanced 160 mm rocket, having a strike range between 20 and 45 km.*

In their previous research, the authors calculated, for the scenario of two rockets launched, the minimum forces, moments and oscillations, determining the optimal time required between the launches. The assessment took into consideration the induced forces on the launch facility (tipping part, chassis).

The main objective of this paper to assess the optimal time and launching order for multiple GRAD rockets, considering theoretical determinations.

Keywords*: LAROM, MLRS, ILANPRN, unguided rocket, optimal launching.*

Introduction

LAROM is a MLRS (multiple launch rocket systems) jointly developed by Aerostar (Romania) and Israel Military Industries (IMI), configured with either GRAD 122 mm or IMI's LAR 160 mm unguided rockets. The vehicle has two launch pod containers. Depending on calibre, each container holds 13 or 20 rockets. The LAROM is based on a Roman DAC-25.360 6x6 military truck. The vehicle is reloaded by supporting ammunition resupply truck [1].

Figure 1: LAROM with IMI's LAR 160 mm launch pod containers

GRAD MLRS were first developed in the early 1960's. **These** systems are still having a role on today's battlefields, despite the intent of users to develop modern, similar capabilities or replace them with guided rockets of different calibre [2, 3, 4].

Figure 2: 122 mm GRAD rocket

Continuing the previous research, the authors have advanced towards a theoretical evaluation of multiple GRAD rockets being launched from LAROM platform [5]. The purpose is not only to determine the optimal time between launchings, but also to establish the best launching order. For this purpose, the Matlab application ILANPRN is used. The algorithm is described next in the following subchapters.

1. Mathematical model for LAROM launcher firings

The movement of the launcher-rocket system is determined if the position variables s, φ_y, φ_z, z_s, γ_x,γ_y are known. All variables of the launching platform are determined in relation to the $O_T X_T Y_T Z_T$ earth fixed reference system.

In order to determine the oscillations of the launching platform during firings, the oscillating system can be assimilated with a set of rigid or elastic bodies connected by elastic elements. The main components of the system are:

- the rockets that are currently on the launcher, including the one being launched;
- the launcher pod with the cradle;
- the chassis of the vehicle on which the pod base is placed with the pivoting support.

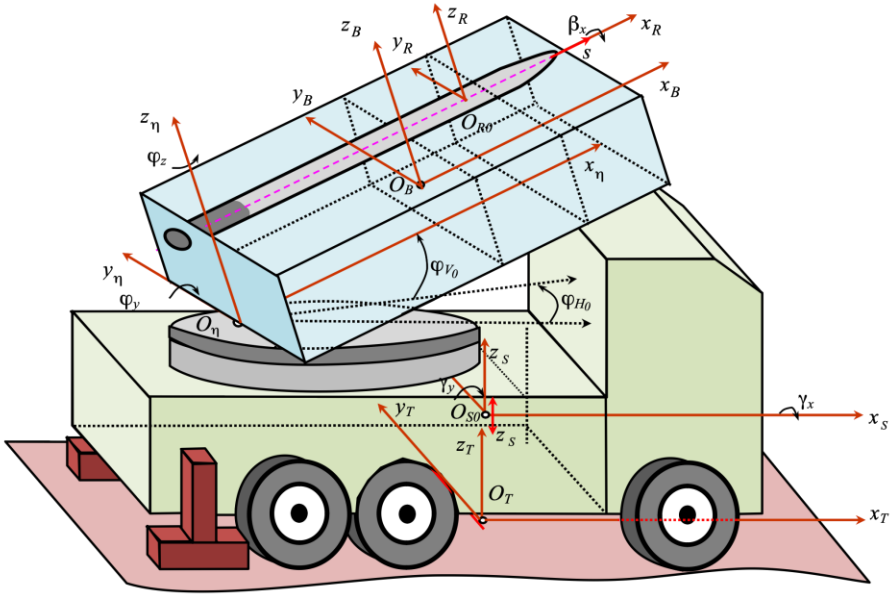


Figure 3: LAROM launcher

The geometric and mass parameters of the launcher platform were defined in previous authors' research [5, 6].

The algorithm for calculating the launch oscillations is the following (figure 4):

Ist approximation

- the position variables s, φ_y, φ_z, z_s, γ_x, γ_y and the binding forces and momentum F_{Rb_x}, F_{Rb_y}, F_{Rb_z}, M_{Rb_x}, M_{Rb_y}, M_{Rb_z}, R_{Π_x}, R_{Π_y}, R_{Π_z}, M_{η_x}, M_{η_y}, M_{η_z} are initiated with the zero value;
- the calculation is performed for the fired unguided missile, s (the movement in the launching tube) being determined;

For the other missiles in the containers, as well as for the launched missile, the binding forces and momentum transmitted to the tipping platform are determined, being applied in the center of mass of the tipping part (F_{Rb_x}, F_{Rb_y}, F_{Rb_z}, M_{Rb_x}, M_{Rb_y}, M_{Rb_z}).

- the numerical determinations are performed at the level of the tipping part, using data from the previous steps, in order to determine , φ_y, φ_z, R_{Π_x}, R_{Π_y}, R_{Π_z}, M_{η_x}, M_{η_y}, M_{η_z};

- the chassis calculation is performed based on previous determined data in order to determine the z_s, γ_x and γ_y variables

IInd approximation

The position variables s, φ_y, φ_z, z_s, γ_x, γ_y are considered known from the first approximation. The obtained results are compared with those of the previous approximation, in order to verify the convergence of the algorithm. In order to obtain a satisfactory convergence of the results, it is necessary to go through at least 3 iterations [5, 6, 7, 8].

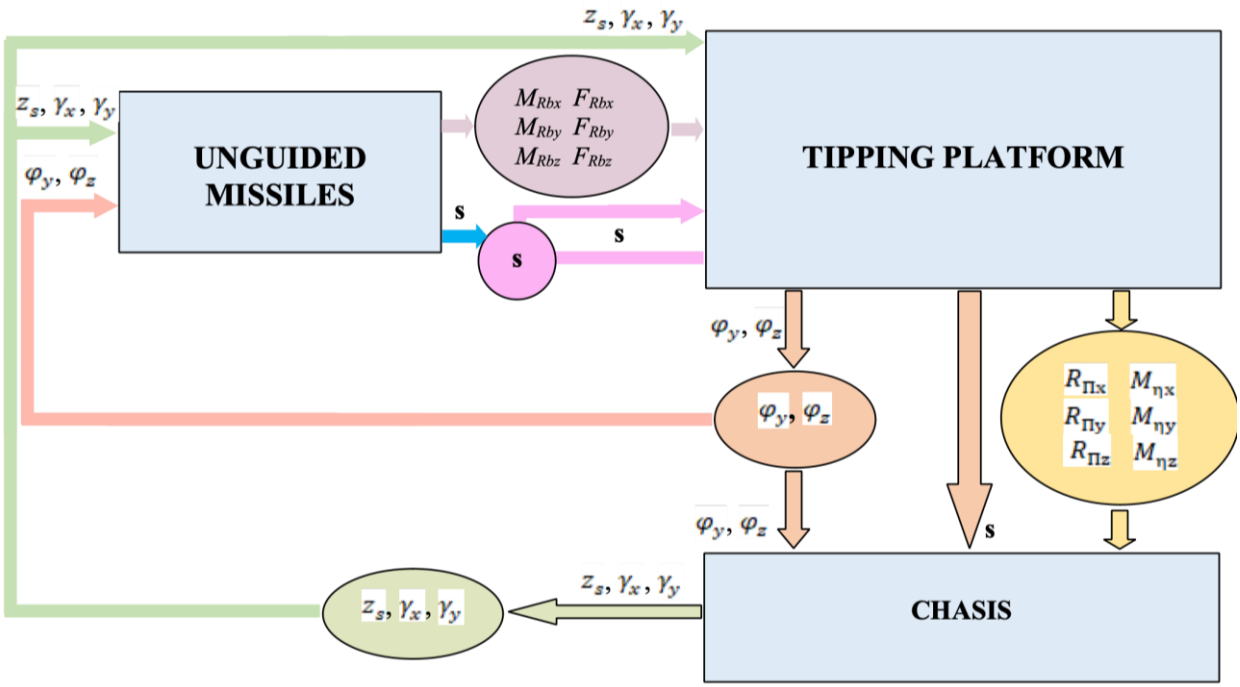


Figure 4: LAROM launcher parameters for MATLAB program

The equation system solved in the previous approximation has the following form:

$$
\begin{aligned}
s &= v_R \\
\varphi_y &= \omega_{\varphi_y} \\
\varphi_z &= \omega_{\varphi_z} \\
z_s &= v_{z_s} \\
\gamma_x &= \omega_{\gamma_x} \\
\gamma_y &= \omega_{\gamma_y} \\
v_R &= F_{v_R}(v_R, \omega_{\varphi_y}, \omega_{\varphi_z}, v_{z_S}, \omega_{\gamma_x}, \omega_{\gamma_y}) \\
\omega_{\varphi_y} &= F_{\omega_{\varphi_z}}(v_R, \omega_{\varphi_y}, \omega_{\varphi_z}, v_{z_S}, \omega_{\gamma_x}, \omega_{\gamma_y}) \\
\omega_{\varphi_z} &= F_{\omega_{\varphi_z}}(v_R, \omega_{\varphi_y}, \omega_{\varphi_z}, v_{z_S}, \omega_{\gamma_x}, \omega_{\gamma_y}) \\
v_{z_S} &= F_{v_{z_S}}(v_R, \omega_{\varphi_y}, \omega_{\varphi_z}, v_{z_S}, \omega_{\gamma_x}, \omega_{\gamma_y}) \\
\omega_{\gamma_x} &= F_{\omega_{\gamma_x}}(v_R, \omega_{\varphi_y}, \omega_{\varphi_z}, v_{z_S}, \omega_{\gamma_x}, \omega_{\gamma_y}) \\
\omega_{\gamma_y} &= F_{\omega_{\gamma_z}}(v_R, \omega_{\varphi_y}, \omega_{\varphi_z}, v_{z_S}, \omega_{\gamma_x}, \omega_{\gamma_y})
\end{aligned}
\qquad 1.1
$$

The approximations are performed in MATLAB using the ode45 solver based on the fourth and fifth order Runge - Kutta methods and algorithms. These methods use a weighted average of the estimated values of the derivatives in the area of interest so as to calculate a value y_{i+1}, having known the value y_i. Thus, if we consider a function $f\ x,y\ = \frac{dy}{dx}$ with initial conditions $y_I = y(0)$, using the Runge - Kutta method, y_{i+1} is determined with the relation:

$$y_{i+1} = y_i + \frac{h}{6}(k_1 + 2 \cdot k_2 + 2 \cdot k_3 + k_4) \quad 1.2$$

where

- $k_1 = f(x_i, y_i)$ is the value of y' for x_i,
- $k_2 = f(x_i + \frac{h}{2}, y_i + \frac{h}{2} \cdot k_1)$ is the value of y' for $x_i + \frac{h}{2}$,
- $k_3 = f(x_i + \frac{h}{2}, y_i + \frac{h}{2} \cdot k_2)$ is the second estimated value of y' for $x_i + \frac{h}{2}$,
- $k_4 = f(x_i + h, y_i + h \cdot k_3)$ is the estimated value of y' for x_{i+1}.

Initial data for the optimal time between launchings determinations:

- initial horizontal firing angle, $\varphi_{H_0} = 45^{\circ}$;
- initial vertical firing angle, $\varphi_{V_0} = 45^{\circ}$;
- number of unguided missiles considered = 4.

2. Optimal launching order determinations

Specific missions or training exercises require a specific number of rockets to be launched and not a full salvo. For this specific type of firings, we are presenting the solution for determining the optimal launching order. We have considered the cases of four rockets per container to be launched. The location of each rocket can be visualised in figure 5. A time step of 0.25 seconds between launchings was also taken into account.

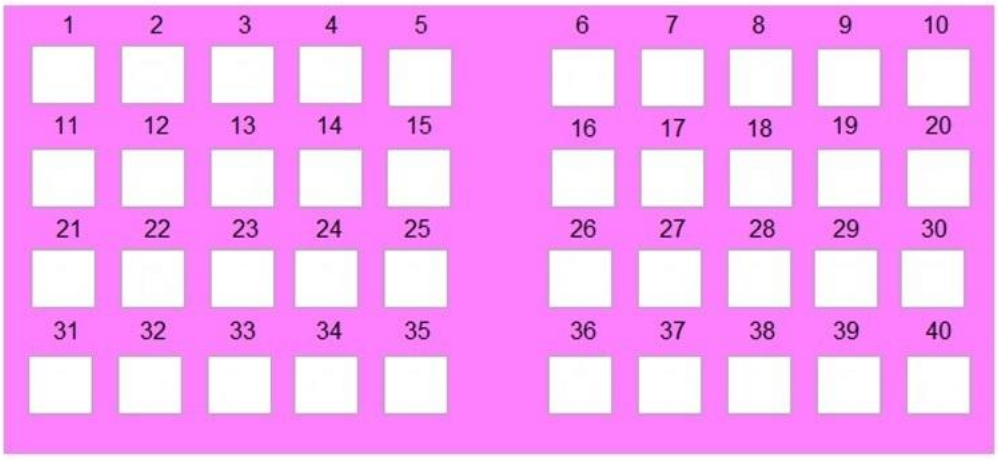


Figure 5: Rocket distribution on pod containers

The amplitude and the impulse of the oscillatory movements of the firing platform were calculated. The formulas used for amplitudes and impulses determination are the following:

$$I_\tau = \int_0^t \tau\ dt \quad 2.1$$

$$A_\delta = \int_0^t \delta \, dt$$

The equivalent values for the total amplitude and impulse of the oscillatory movements of the platform are determined using the formulas:

$$A_{tot} = \sqrt{A_{\varphi y}^2 + A_{\varphi z}^2 + A_{gx}^2 + A_{gy}^2 + A_{\varphi y}^2 + A_{zs}^2} \qquad 2.2$$

$$I_{tot} = \sqrt{I_{\varphi y}^2 + I_{\varphi z}^2 + I_{gx}^2 + I_{gy}^2 + I_{\varphi y}^2 + I_{zs}^2}$$

The scenarios considered involved firing from two fixed positions symmetrically opposed (rocket from position **3** followed by the one from position **38**) coupled with two launchings from variable positions. A total of twenty cases were calculated, as presented in table 1. Considering either the total amplitude of the oscillation or the total impulse of the oscillation, one obtains different results for the best and worst case scenario.

Table 1: Values obtained for the cases considered

Case	Rocket launch order	Total amplitude of the oscillation [mm]	Total impulse of the oscillation [N*s]
1	**3-38-25-16**	43.7273	34.1984
2	**3-38-24-17**	43.6767	33.9763
3	**3-38-23-18**	43.68	33.9489
4	**3-38-22-19**	43.8872	33.8696
5	**3-38-21-20**	43.6754	33.998
6	**3-38-35-6**	43.5118	34.0475
7	**3-38-34-7**	44.3886	34.2092
8	**3-38-33-8**	44.3882	34.2017
9	**3-38-32-9**	43.6664	34.1309
10	**3-38-31-10**	43.669	34.0862
11	**3-38-16-25**	43.7136	33.701
12	**3-38-17-24**	43.7484	33.4535
13	**3-38-18-23**	43.7309	33.5891
14	**3-38-19-22**	43.894	33.7204
15	**3-38-20-21**	43.7061	33.8192
16	**3-38-6-35**	43.5645	33.4898
17	**3-38-7-34**	44.4432	33.687
18	**3-38-8-33**	44.4549	33.65

Case	Rocket launch order	Total amplitude of the oscillation [mm]	Total impulse of the oscillation [N*s]
19	**3-38-9-32**	43.7278	33.5741
20	**3-38-10-31**	43.7322	33.5651

Legend:

Best case scenario **Worst case scenario**

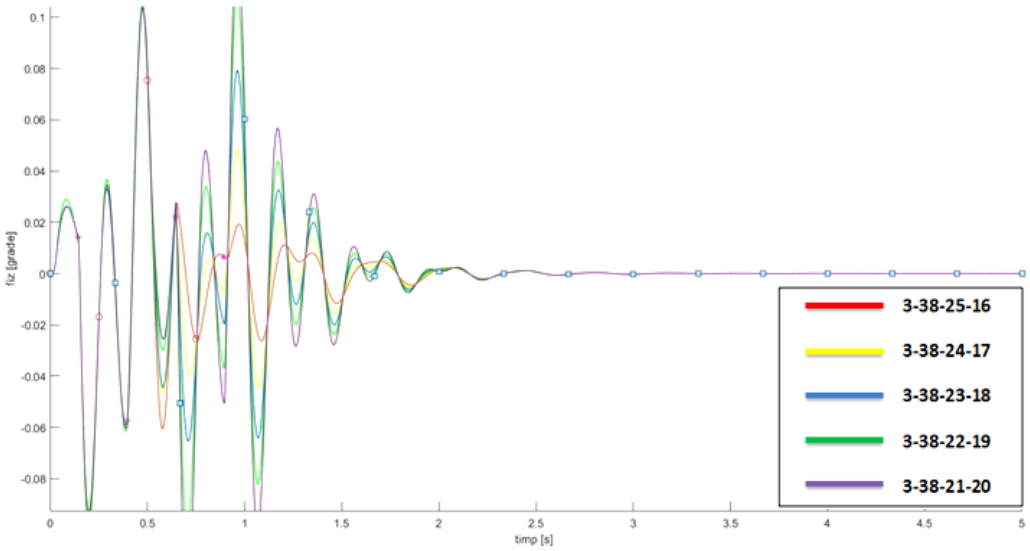


Figure 6: Oscillations during the rotation movement of the platform on Z axis

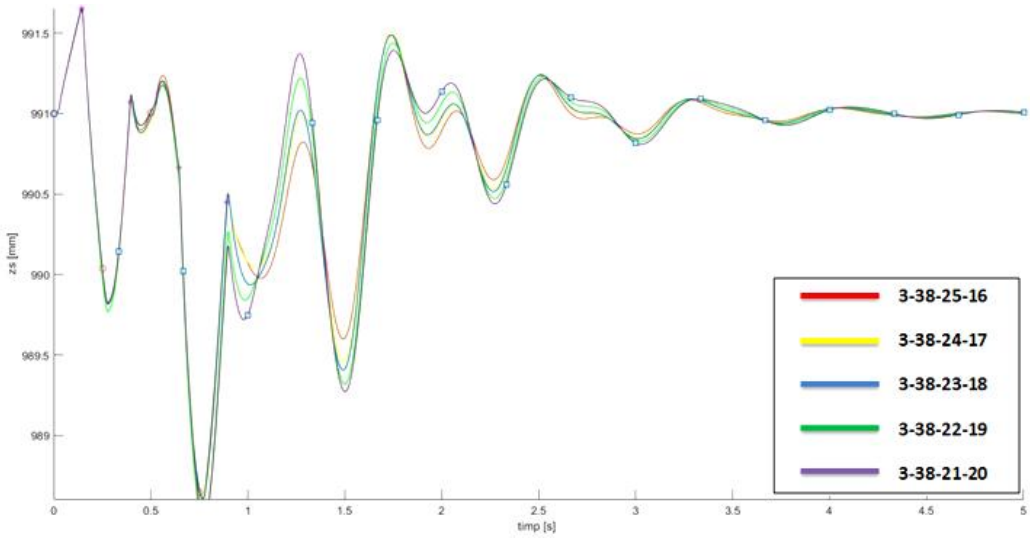


Figure 7: Oscillations created during the translational movement of the chassis on Z axis

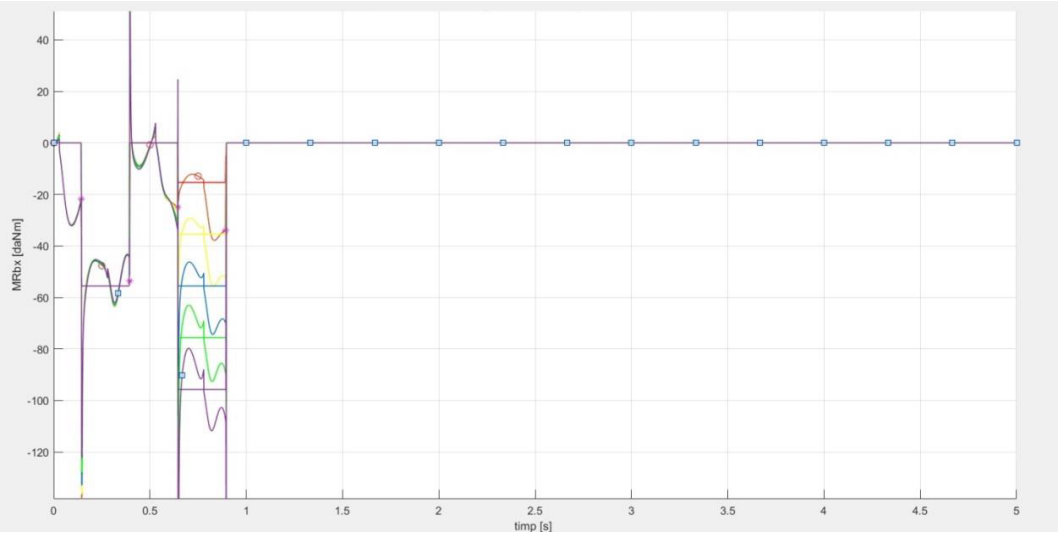


Figure 8: Momentum transmitted from the rocket to the platform on X axis

Figures 6 and 7 describe the oscillatory evolution of the chassis during the rotational and translational movement on the axis of interest. Same procedure can be applied to extract oscillatory evolution graphs for the tipping platform, using the features from Matlab ILANPRN program.

3. Optimal time between launchings determinations

Determining the optimal time between launchings requires to evaluate the oscillations determined by the rotations of the tipping part and the chassis of the firing platform when the last unguided GRAD rocket is launched. The rocket launch order was selected the one for which the total impulse calculated was the minimum in the previous subchapter (**3-38-17-24)**.

The numerical determinations were conducted for the following time intervals between each rocket launched:

- case I – 0.2 seconds;
- case II – 0.4 seconds;
- case III – 0.6 seconds;
- case IV – 0.8 seconds.

We evaluate the optimal time between launchings by comparing the movement of a material point located on the chassis of the platform considering the time intervals selected.

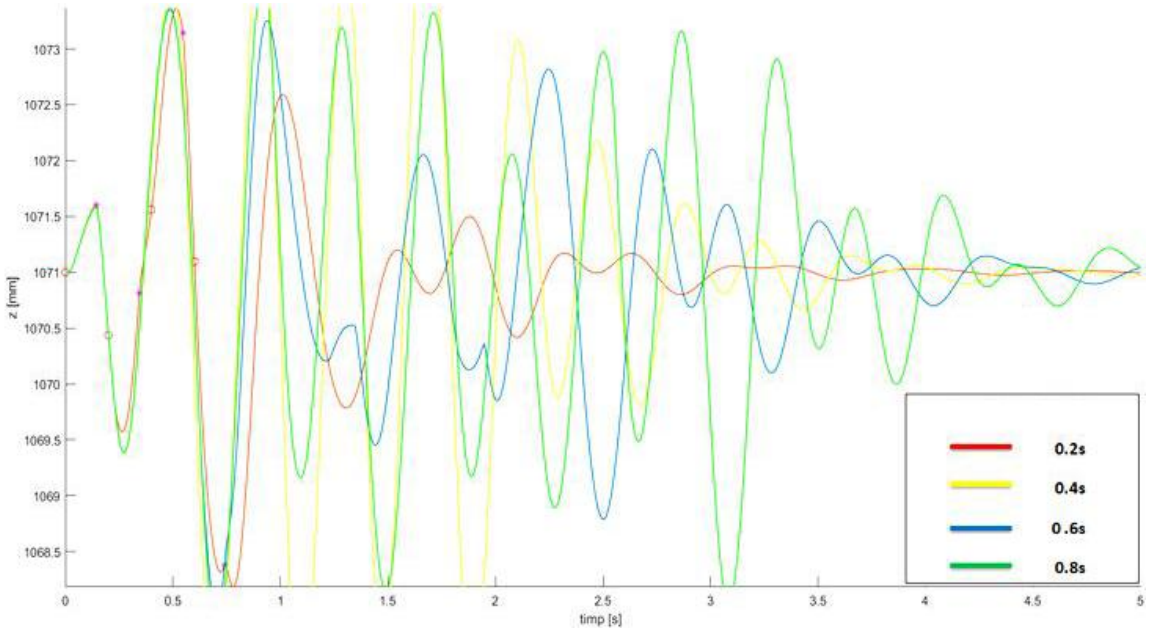


Figure 9: Movement of a material point located on the chassis, considering different times of launching

In figure 9 it can be observed that for a time step of 0.2 seconds, the movement is amortised the earliest and the amplitude of the oscillations is the lowest, therefore this is the best case scenario for the given options. With time intervals of 0.8 and 0.6 seconds between the rockets launchings, the stress induced to the launching platform is at the highest value.

Acknowledgments

Numerical determinations were conducted using the MATLAB program in order to evaluate the effects of firing unguided rockets when considering different launchings order and time intervals between launchings. It is considered the influence of the oscillatory movements given by the rotation angles of the tipping part and chassis along the x/y axis and the linear oscillation of the chassis along the z axis when the second unguided missile is launched.

The best and worst case scenarios in terms of the stress induced to the launching platform are presented, considering the launch of four unguided GRAD rockets from different launch pod positions.

References

1. Stroea, A.; Băjenaru, Ghe. – *Romanian artillery in data and images*, Technical-Editorial Center of the Army Publishing House, Bucharest, 2010;
2. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-july-22
3. https://www.newsweek.com/russia-reportedly-blasts-ukrainian-targets-bm-21-grad-rocket-launcher-1713192
4. https://www.hrw.org/news/2020/12/11/armenia-unlawful-rocket-missile-strikes-azerbaijan
5. https://www.aadcf.nvu.bg/scientific_events/dtf2021/wtl/5%20Zv%C3%AEncu.pdf
6. Şomoiag, P. – *Weapons Systems. Dinamics of self-propelled launching systems*, Military Technical Academy Publishing House, Bucharest, 2007;
7. McCoy, R. L. – Modern Exterior Ballistics, Schiffer Publishing Ltd., 1999;
8. Şomoiag, P.; Sava, A.C.; Moldoveanu, C.E.; Iancu, I. - Weapons systems. The firing action on missile launching systems, Military Technical Academy Publishing House, Bucharest, 2012.

PERSONNEL BALLISTIC PROTECTION USING COMPOSITE MATERIALS

Diana-Carmen Dumitraș

Military Equipment and Technologies Research Agency, Center for Navy Scientific Research and Innovation, Constanta, Romania, dianacarmen.dumitras@gmail.com

Abstract: *Composite fibers are a perfect compromise between advanced protection provided to the military personnel and a relatively low weigh. Given the many advantages the use of composite materials such as Kevlar, Twaron and Dyneema fibers in ballistic applications, the new trends are increasingly moving towards replacing classically used materials with these materials. In the following paper will be presented the main advantages of using composite materials within the individual ballistic protection, making a theoretical study of the properties and protection mechanisms that intervene in the case of dangers associated with armed struggle, and by using empirical and experimental methods, the response of protection materials to penetration will be calculated and compared.*

Key words: *Failure mechanisms, Penetration, Material properties, Shear strength, Penetration Velocity, Energy absorption.*

Introduction

The continuous evolution within the ammunition industry has implicitly led to the evolution of technologies used in the framework of ballistic (individual) protection. There are two fundamental categories of ballistic protection: passive and reactive, the first relying on stopping the threat only using properties of the materials that make up the means of protection, and the second on generating a kinetic response in the material of the means of protection [2].

A difficult task when it comes to designing the different configurations that ensure the protection of personnel and military technique, is the analysis of the real or perceived threat. This type of information is able to generate relatively accurate data, related to the possible phenomenon that occur during the impacting of a threat.

The possible threats that may appear in the battle are foreseen and classified under national and international standards [6,7], being divided into risk classes and threat levels, in the case of individual protection against military personnel, of which [3] are part:

- Ammunition for small arms (calibers ranging from 5.56 mm to 14.5 mm);
- High-speed fragments;
- Threat of stabbing.

A solution that might meet the requirements of the ballistic protection field, personnel protection especially, is composite materials. They are used within the protection structures by processing in different forms: fibrous composites, materials made of composite matrix or sandwich/layered plates. [4]

This work aims to carry out a theoretical study on the mechanisms of penetration, as well as on some aspects related to terminal ballistics in the case of composite materials used for individual ballistic protection. The study will present the main composite materials used in ballistic protection, followed by the evaluation of the response they have to the action of different types of threats, compared to classical materials.

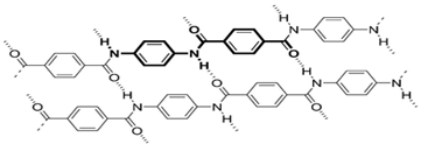
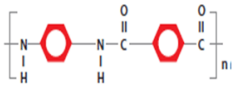
I. Composite material

In recent years, has been observed an interest in light armor and the development of new technologies for making them. Compared to hard armor, the protection made with light materials offer much more flexibility, which is preferred by the personnel on the battlefield [1] . One of the recent trends when it comes to means of ballistic protection, is the use of composite materials such as carbon nanotubes and other nano-materials

Composite materials are generally made of a matrix material and a type reinforcement. Usually they are used in ballistic applications with reasonable failure rates (~ 3%-6%), therefore presenting excellent energy absorption properties. [2,3] Most of the composite materials used have a fibrous structure, and although they are mainly used in the manufacture of bulletproof vests and other types of personnel protection, and due to their properties amour designer started the incorporation of composites into the protection of the technique as well. The materials composite with a special interest are:

- Kevlar fibers
- Dyneema fibers
- Twaron fibers

Table 1 Molecular structure of the main types of fibers used in ballistic protection [4]

Fiber	Structure
Kevlar	
Dyneema	$[-CH_2-CH_2-]_n$
Twaron	

The resistance to actions phenomenon such as penetration depends on a number of different parameters, but the possibility of determining a variable that can be altered to provide increased protection is limited. However, there are parameters such as the specific energy absorption capacity of the fibers and the speed of sonic or elastic fibers waves that significantly influence the protection offered by the material. [2,3] The speed of elastic waves is of particular importance, allowing the delocalization of the stresses from the point of impact, thus implicitly the specific absorption of energy of the fiber. [2,3]

The properties of some of these composite materials and some materials typically used in ballistic protection are presented in table 2 and will further be used to differentiate between their efficiency in ensuring the best protection when we will discuss the mathematical method that describe the way the properties of a material influence the protection they provide:

Table 2 Properties of different materials used in ballistic applications

	Type of fiber	Kevlar 29	Kevlar 49	Standard Twaron	High tenacity Twaron	Dyneema SK76	MIL-12560	AA 2024
Pro	Density (kg/m3)	1,440	1,440	1250	1440-1450	97	7830	2765
	Tensile strength (MPa)	3000	2900	2400-2500	3400-3600	3700	1207	400–430

	Type of fiber	Kevlar 29	Kevlar 49	Standard Twaron	High tenacity Twaron	Dyneema SK76	MIL-12560	AA 2024
properties	Traction mode (GPa)	74	105	60-80	85-95	116	1207	400–430
	Elongation to Break (%)	3.5	2.5	3.0-4.4	3.3-4.0	3.8	12	10–15
	Shear strength (MPa)	2758	3990	-	-	3619	618	281
	Compressive shear strength τ_S (MPa)	1169	3990	3600	3600	462	618	281

II. Methods for determining the protection offered by a material

An important step in choosing materials for armors, is to understand their penetration mechanisms. The penetration subjects the material to a complex state of stress that will lead to material failure, which can occur in the form of the failure mechanisms depicted in the figure 1. Penetration processes are affected by the material properties of the penetrator and target, the speed of impact and the input geometry of the projectile(s).

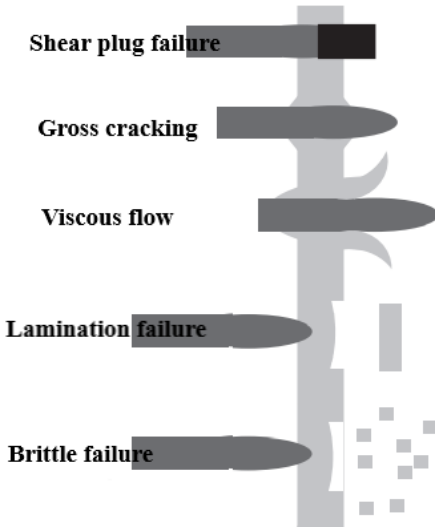


Figure 1 Different failure mechanisms of a material [3]

The decision concerning the material the makes up the protection equipment for personnel, entails predicting as accurately as possible the behavior of the material when subjected to the loads that occur during an impact with a threat, and for that there are two general methods that can predict the material behavior and the properties that the material has to have in order to resist the loads they are subjected to appear.

One method uses a mathematical model of a penetration, which is described by the following equation, which results from conservation of kinetic energy [2]:

$$\frac{m \cdot {v_0}^2}{d^3} = c \cdot [\frac{h}{d}]^n \quad (1)$$

Where: d-diameter of a cylindrical body penetrating a plate; m - is the mass of the cylinder, h- the thickness of the plate the cylinder strikes, and v_0 - is its impact velocity; and c, n are empirically derived constants.

It is considered that the cylinder that hits the plate is flat-nosed and the velocity at the impact is under 1000 m/s. it is also considered that the angle between the plate and the cylinder at the moment of the impact is 90° and therefore the energy required for the rough cracking of the plate can be expressed with the relation [2]:

$$E_{plugging} = \tau \cdot \pi \cdot d^3 [\frac{h}{d}]^2 \quad (2)$$

With the mention that it starts from the assumption that $\tau \approx 0.6\pi$, τ - describing the shear resistance. Thus, replacing the shear resistance in relation (2), the energy required for plugging becomes [2]:

$$E_{plugging} = 0.6\pi^2 \cdot dh^2 \quad (3)$$

The transition from cracking to penetration starts the moment when the energy required for cracking equals that required for penetration, and once the diameter of the cylindrical body - the thickness of the plate ratio exceeds a value of 0.42, the penetration phenomenon becomes much more likely. Figure 2 illustrates the probability of occurrence of a response in the material according to the ratio h/d.

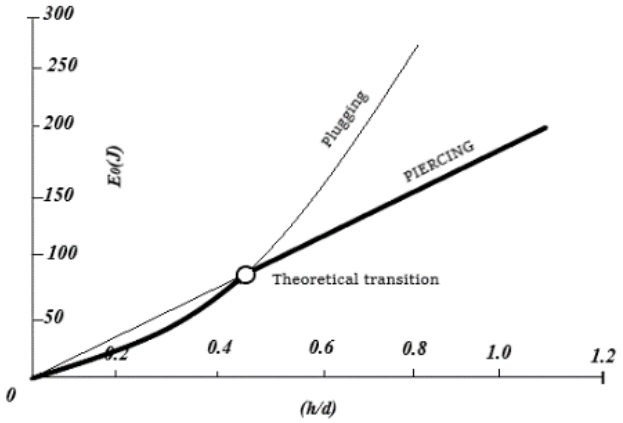


Figure 2. Transition from plugging to piercing for a plate with a diameter of 7.62 mm and σ=500MPa. E_0 represents energy required for perforation [2]

So based on the equation (2) we can confirm that the energy the material is able to absorb is proportional to its shear strength, which according to table 2 is greater for composite materials such as Kevlar and Dyneem compared to metals, therefore being able to absorb more energy, ensuring a better protection. For instance, the lateral interactions between molecular chains of Dyneema fibers, are formed by Van der Waals forces, hydrogen bonds forming one dimensional (aramid) and hydrogen bonds forming two dimensional (PIPD) networks making compressive strength increases from 0.02 to well above 1.0 GPa. [8] Although Dyneema fibers' axial compressive strength is almost negligible, their resin density is a bit lower than that of conventional epoxy resins it is quite suitable for personnel protection and other ballistic applications due to their high tensile strength and low density, but at the same time makes it unsuitable for structural aerospace composites if used by themselves [9]

The kinetic energy required for the projectile to perforate the plate can also be expressed by [2]:

$$E_0 = cd^{0.5}h^{1.4} \quad (4)$$

$$h^{0.7} = k\frac{m^{0.5}v_0}{d^{0.75}} \quad (5)$$

Where k is an empirically derived constant.

The aspect that equations (3) and (4) highlight is that the amount of energy the material absorbs is proportional to the thickness of the material, and due to their low-density composite materials can ensure more protection with less weigh than the materials typically used for personnel protection.

The second method of calculating the response mechanisms of a material, we will discuss, takes into account the properties of the material and uses the equation of penetration motion, expressing it using parameters such as the velocity the bullet has the moment it impacts the material [2]:

$$F = a_0 + a_1 \cdot v + a_3 \cdot v^2 \tag{6}$$

Where *v*-velocity of the projectile, a, a_1 and a_3 are constants.

The force with which the material has answer to the forces of the penetration of the projectile can be expressed by two equations, the first one proposed by Poncelet (8) and another one proposed by Recht (10), [2]:

$$F = m\frac{dv}{dt} = mv\frac{dv}{dx} \tag{7}$$

$$F_r = -\mu F = -A_x(P_d + C_\alpha \rho v^2) \tag{8}$$

Where: μ-strength coefficient of the material, A_x – the area of the projectile immersed in the target, P_d – the distortion pressure in the target, and the empirical C_α- dimensionless empirical constant. Poncelet based his equation on an equation (9) by Backman and Goldsmith, 1978 that describes the penetration *p*. [2]

$$p = c_1 \ln(1 + c_2 {v_0}^2) \tag{9}$$

In this equation c_1 and c_2 represent empirically derived constants.

The equation that Recht proposed (10) to express resistance force, uses parameters such as C_n- empirical dimensionless empirical constant dependent on the shape of the nose of the projectile, dimensionless constant C_V that takes into account the fact that the inertial pressure decreases over time, the α- the half-rod at the tip of the nose, *K*- the bulk modulus of the penetrated material, *f*- the coefficient of dynamic friction and τ_s- the static shear resistance [2]:

$$F_r = -A_x \; C_n \; C_v v \; \overline{K\rho} sin\alpha + 2\tau_s \ln \; 2Z_m \quad \cdot \; 1 + \frac{f}{\tan\alpha} \tag{10}$$

$$\text{Where } Z_m = \; \frac{E}{Y} \; \cdot \; 1 + 2\frac{E}{Y} \; ^{-0.5} \tag{11}$$

E being Young's modulus and *Y*- static shear resistance of the material.

So by incorporating the force definition into the equation of motion, it provides us an equation that describes the fully emersion of a projectile into a material/target. The equation describing the penetration can be written in the form of [2]:

$$x = \frac{2 \; \frac{m}{2A_p}}{C_n b} \quad v_{02} - v \; - \frac{a}{b} \ln \; \frac{a + bv_0}{a + bv} \tag{12}$$

$$A_p = \frac{\pi d^2}{4} \tag{13}$$

Where v_{02} is the speed at which the projectile enters entirely into the target material. And the constants a, b are calculated using the following equation [2]:

$$a = 2\tau_s \ln \; 2Z_m \quad 1 + \frac{f}{\tan\alpha}$$

$$b = C_v \; \overline{K\rho} \; a + \frac{f}{\tan\alpha} \; sin\alpha \tag{14}$$

To vaidate Recht's equation, a serie of experimental tests were compared to the results of the equation (12) for both the cases when a 7.62 mm bullet penetrates a plate and when only the core of the

bullet does the penetration. This results are depicted in *figure 3*, and it supports the corelation between the experimental data and the results of Recht equation. In the end the total depth of penetration is then given by equation (15), where *l* is the length of the ogive, with the assumption that *l<p. [2]*

$$p = l + x \tag{15}$$

The equation (12) also supports that the protection that the material provides is the depth of the penetration decreses with the increase in the values of certain prorieties such as the bulk modulus of the penetrated material and the static shear resistance. *Table 2* shows us that the values for these properties are slightly greater for the composite materials compared to the metals comonly used for balistic protection.

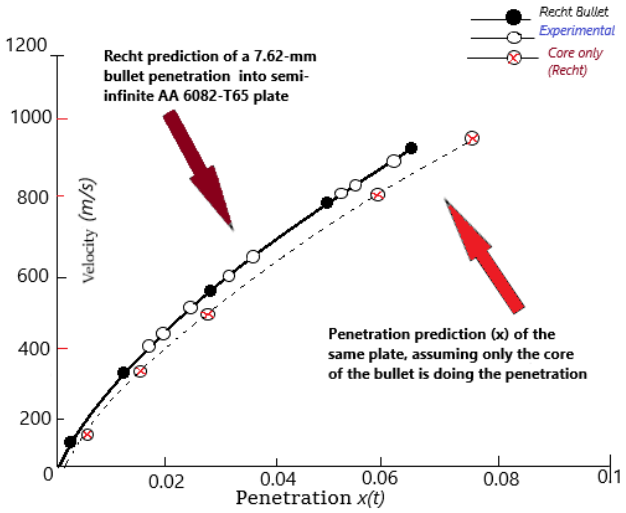


Figure 3 Penetration curves described by Recht's equations and experimental data of an FFC AP projectile, 7.62 mm in diameter (with or without collar) [2]

This chapter shows us the dependence between the strength and resistance characteristics of a material and the degree of protection they provide. Nowadays they are preferred for ballistic protection of the personnel, not only for their high degree of protection, but also because they give the fighters so much more mobility on the battlefield, compared to the protection means used in the past.

Conclusions

The modern design of means of personal protection has focused in recent years on two classes of materials: composite fibers and ceramic materials, with a special interest in the design of protective means made of materials that are part of the first class, being much lighter, but ensuring properties almost identical to those used traditionally, sometimes superior.

A disadvantage of these materials is the much higher price, compared to those traditionally used, which can pose a problem for the defense industry, but despite that these materials are gaining ground due to their strength properties and low mass.

Composite materials use the high tensile strength of their fibers to ensure adequate protection against threats (that occur in a fight), and their low densities ensure the mobility of fighters, having the advantage of a much-reduced mass, compared to the classical means of personal ballistic protection. Also, these fibers have excellent energy absorption abilities, and by stratifying them, the resistance to penetration is increased, implicitly increasing the degree of protection provided. [2]

Therefore, there are many factors to consider, when it comes to choosing materials to ensure the best protection of staff. It is important to be effective against threats, but also to ensure efficiency in the performance of missions by staff, these means having to be as little restrictive as possible, which is why composite materials are the perfect compromise between protection and mobility.

Acknowledgements

The author is truly grateful to their colleagues within Center for Navy Scientific Research and Innovation, Constanta, Romania, who have contributed to this paper and their valuable discussions and input and their colleagues within the Military Technical Academy "Ferdinand I" for their valuable input and providing the means for the author to be able to attend this prestigious event.

References

1. L Wang1, S Kanesalingam2, R Nayak and R Padhye, *"Recent Trends in Ballistic Protection"* ,School of Fashion and Textiles, RMIT, University, Australia
2. Paul J Hazell, *„Armour Materials, Theory, and Design"* , Paul J. Hazell, The University of New South Wales, Canberra, Australia
3. Ian G. Crouch, „The Science of Armour Materials", Woodhead Publishing in Materials
4. *„Ballistic Protective Textiles – An Overview"* , Birendra Acharya
5. Tomasz Garbowski, Tomasz Gajewski, Jakub Krzysztof Grabski *„Mechanics of Corrugated and Composite Materials"*
   STANAG 2920 „BALLISTIC TEST METHOD FOR PERSONAL ARMOUR MATERIALS AND COMBAT CLOTHING"
6. NATO - AEP-2920 „PROCEDURES FOR THE EVALUATION AND CLASSIFICATION OF PERSONAL ARMOUR BULLET AND FRAGMENTATION THREATS"
7. https://repository.tudelft.nl/islandora/object/uuid:f0228918-d5c2-46ed-adf0-976dd825050a/datastream/OBJ
8. http://www.icas.org/ICAS_ARCHIVE/ICAS2008/PAPERS/625.PDF

RESEARCH ON THE AIRCRAFTS AND DRONES WAKE VORTICES AND THEIR EFFECT ON THE FLIGHT SECURITY

Camille Yaker[1], Arthur Tijou[1], Laure Velasco[2], Thomas Flourou[2], Cristian-Emil Moldoveanu[3], Constantin Enache[3], Alin-Constantin Sava[3], Răzvan Mircioagă[3]

[1)]French Military Academy of Saint Cyr, FRANCE, camille.yaker@st-cyr.terre-net.defense.gouv.fr
[2)] "Paul Sabatier" University of Toulouse, FRANCE, laure.velasco@etu.iut-tlse3.fr
[3)] Military Technical Academy "Ferdinand I", Bucharest, ROMANIA, cristian.moldoveanu@mta.ro

Abstract: *The objective of this research is the wake turbulence generated by a flying aircraft, aiming to deepen and develop knowledge of highly complex phenomena closely related to the wake turbulence. The main purpose of the research is to determine the characteristics of the wake turbulence of the aircraft in order to find solutions to avoid aviation incidents that may occur when another aircraft falls within the range of turbulence generated by the first aircraft. The objectives pursued are: identifying risks that may affect the safety and security of airports due to the wake turbulence of aircrafts; mathematical modelling and simulation of the wake turbulence of aircrafts; study of the mechanisms of vortex instability that affect the wake of aircrafts; optimizing aircraft traffic in the airport area in safe conditions.*

Keywords*: Wake Vortices, Turbulence, Security.*

Introduction

The wake flow generated by a plane consists of vortices that can be a danger to another plane following it. These vortices are due, in a schematic manner, to the flow around the wings under the effect of the pressure difference between the lower side and the upper side. When the atmospheric conditions are favourable, one can notice the trace of these vortices in the sky behind the planes, by entraining the gases generated by the engine, as well as the condensation at the flight altitude during the vortices. The purpose of this research paper is to study the behaviour of longitudinal vortices under the influence of external turbulence. In this context, three important elements are dealt with: two physical phenomena (vortices generated by aircraft and external turbulence) and the numerical methods used to study these phenomena.

The main effect of wake turbulence on an aircraft is the induced rolling motion that can even lead to its overturning. This phenomenon can become extremely dangerous during take-off or landing phases when the aircraft is moving at a low altitude and can no longer recover.

Aircraft with small wings are the most affected. The effect of the wake depends on many factors, among which we mention the mass and the span of the aircraft that falls within the range of the wake, as well as the relative position between the aircraft and the wake. Due to the wake turbulence, countless air accidents have occurred over time.

1. Mathematical model of the wake vortices

To simulate the turbulent flow of the wake generated by an aircraft usually it is used the *Large Eddy Simulation* method, aiming to solve the complete Navier-Stokes equations but reducing the number of points needed to discretize the calculation range in case of turbulent flows. The main idea of LES is to

practice a "*cut*" at a wavelength $k = k_c$ and to directly simulate the corresponding large structures of $k < k_c$ and to model the small ones corresponding to $k > k_c$ [1].

Large-scale structures are less universal and depend very much on the geometry of the flows. If they are simulated directly, it is no longer necessary to find a model characteristic of these structures. *Small-scale structures* are less affected by the geometry of the flow, so it should be much easier to find a universal model with which to represent these turbulence structures. The velocity field is thus decomposed by the sum of a velocity field of the *large-scale structures* and a velocity field of the *small-scale structures*, represented by the wavelength that is not captured by the mesh size of the computational domain discretization grid.

Starting from the Navier-Stokes system of equations for the unfiltered field we will determine the filtered equations:

$$\begin{cases} \dfrac{\partial \bar{u}_j}{\partial x_j} = 0 \\ \dfrac{\partial \bar{u}_i}{\partial t} + \dfrac{\partial \overline{u_i u_j}}{\partial x_j} = -\dfrac{1}{\rho}\dfrac{\partial \bar{p}}{\partial x_i} + 2\nu \dfrac{\partial \bar{s}_{ij}}{\partial x_j} \\ \dfrac{\partial \bar{T}}{\partial t} + \dfrac{\partial \overline{T \cdot u_j}}{\partial x_j} = \dfrac{\partial}{\partial x_j}\left(D_\mu \dfrac{\partial \bar{T}}{\partial x_j} \right) \end{cases} \Rightarrow \begin{cases} \dfrac{\partial \bar{u}_j}{\partial x_j} = 0 \\ \dfrac{\partial \bar{u}_i}{\partial t} + \dfrac{\partial \bar{u}_i \bar{u}_j}{\partial x_j} = -\dfrac{1}{\rho}\dfrac{\partial \bar{p}}{\partial x_i} + \dfrac{\partial}{\partial x_j}\left(2\nu \cdot \bar{s}_{ij} - \tau_{ij}^{sm} \right), \\ \dfrac{\partial \bar{T}}{\partial t} + \dfrac{\partial \bar{T} \cdot \bar{u}_j}{\partial x_j} = \dfrac{\partial}{\partial x_j}\left(D_\mu \dfrac{\partial \bar{T}}{\partial x_j} - q_j^{sm} \right) \end{cases} \quad (1)$$

where $\tau_{ij}^{sm} = \overline{u_i u_j} - \bar{u}_i \bar{u}_j$ and $q_j^{sm} = \overline{T u_j} - \bar{T}\bar{u}_j$.

The tensor of the previously introduced stresses can be broken down as follows [4]:

$$\tau_{ij}^{sm} = \overline{u_i u_j} - \bar{u}_i \bar{u}_j = L_{ij} + C_{ij} + R_{ij}, \quad (2)$$

where

$$\begin{cases} L_{ij} = \overline{\bar{u}_i \bar{u}_j} - \bar{u}_i \bar{u}_j, \text{ tensiuni Leonard;} \\ C_{ij} = \overline{\bar{u}_i u'_j} - \overline{u'_i \bar{u}_j}, \text{ tensiuni combinate;} \\ R_{ij} = \overline{u'_i u'_j}, \text{ tensiuni Reynolds.} \end{cases} \quad (3)$$

Most models used in LES are based on the concept of turbulent viscosity ν_t the expression of which is obtained by assuming that small structures are in energetic equilibrium. Assuming that the dissipation is equal to the production of energy, we can determine the relation for the turbulent viscosity:

$$\nu_t = (C_s \Delta)^2 \left(2\bar{S}_{ij}\bar{S}_{ij} \right)^{1/2}, \quad (4)$$

where C_s is the Smagorinsky constant.

The filter band is of the order of the smallest solved structures:

$$\Delta = \sqrt[3]{\Delta_1 \Delta_2 \Delta_3}, \quad (5)$$

The strain tensor is given by:

$$\bar{S}_{ij} = \frac{1}{2}\left(\frac{\partial \bar{u}_i}{\partial x_j} + \frac{\partial \bar{u}_j}{\partial x_i} \right). \quad (6)$$

The Smagorinsky model uses the strain tensor to model the influence of small structures on the explicitly resolved flow. The problems raised by the Smagorinsky model result from the fact that this model is diffusive and does not allow the modelling of energy transfer from small structures to large

structures. This disadvantage is highlighted in the case of simulating inhomogeneous flows such as flow through a channel.

Another disadvantage of the method is that no unique value can be found for the Smagorinsky constant. The Smagorinsky model is therefore not universal. Constant C_s can also be determined theoretically:

$$C_s = \frac{1}{\pi}\left(\frac{3 \cdot C_k}{2}\right)^{-3/4} \approx 0.18, \qquad (7)$$

by $C_k = 1.4$, a Kolmogorov constant.

To initialize the calculations, a vortex dipole based on the Oseen model will be used as the base flow. An Oseen-type *solitary vortex* used in the calculations has as main parameters the circulation Γ_0 and radius r_0, which corresponds to a maximum rotational speed. The position of the vortex centre is given by the coordinates (y_0, z_0) in a transverse plane (Oyz). Using a cylindrical coordinate system (x, r, θ) the origin of which is the centre of the vortex, the rotational speed $u_\theta(r)$ and the vortex $\omega_x(r)$ of eddy are given by the ratio [9]:

$$u_\theta(r) = \frac{\Gamma_0}{2\pi r}\left(1 - e^{-r^2/r_0^2}\right); \omega_x(r) = \frac{\Gamma_0}{\pi r_0^2} e^{-r^2/r_0^2}. \qquad \mathbf{(8)}$$

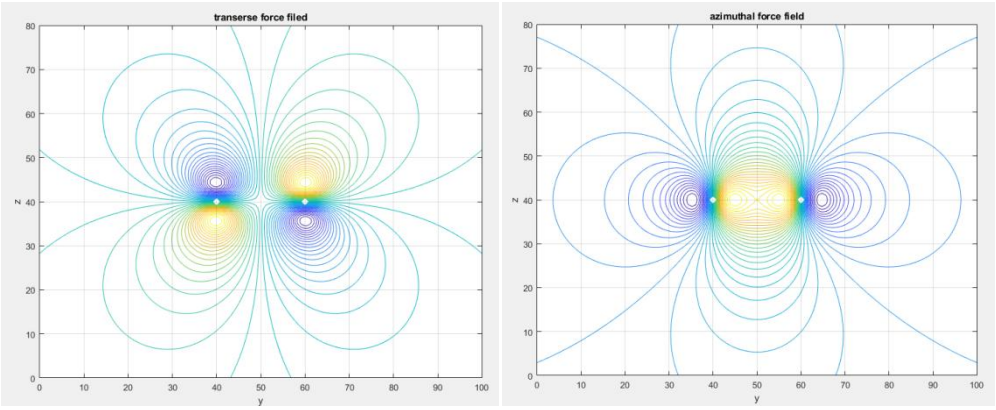


Figure 1: Distribution of the initial velocity field in a transverse plane for a pair of counter-rotating longitudinal vortices

To model a ***vortex dipole***, two counter-rotating longitudinal vortices such as those described above were used, having the circulation $\Gamma_{01} = -\Gamma_0$, $\Gamma_{02} = \Gamma_0$, located at the distance b_0 one from the other**.** Figure 1 shows the speed distribution in this situation . The reference parameters are [5]:

$$U_{ref} = w_d = \frac{\Gamma_0}{2\pi b_0}; L_{ref} = b_0; \mathrm{Re} = \frac{\Gamma_0}{2\pi\nu}. \qquad \mathbf{(9)}$$

The method of representing a pair of counter-rotating vortices adopted is the superposition of two isolated longitudinal vortices followed by an initial adaptation calculation:

$$\begin{cases} v(y,z) = -\dfrac{\Gamma_0}{2\pi}\dfrac{z-z_0}{r^2}\left(1-e^{-\frac{r^2}{r_0^2}}\right) \\ v(y,z) = \dfrac{\Gamma_0}{2\pi}\dfrac{y-y_0}{r^2}\left(1-e^{-\frac{r^2}{r_0^2}}\right) \end{cases}; \quad \textbf{(10)}$$

where $r = \sqrt{(y-y_0)^2 + (z-z_0)^2}$.

2. Numerical simulation of the wake vortices in ground effect

By numerically simulating in FLUENT/ANSYS the evolution of a pair of counter-rotating longitudinal vortices in the presence of the ground, a downward trajectory is obtained, similar to the theoretical behaviour represented in Figure 2.

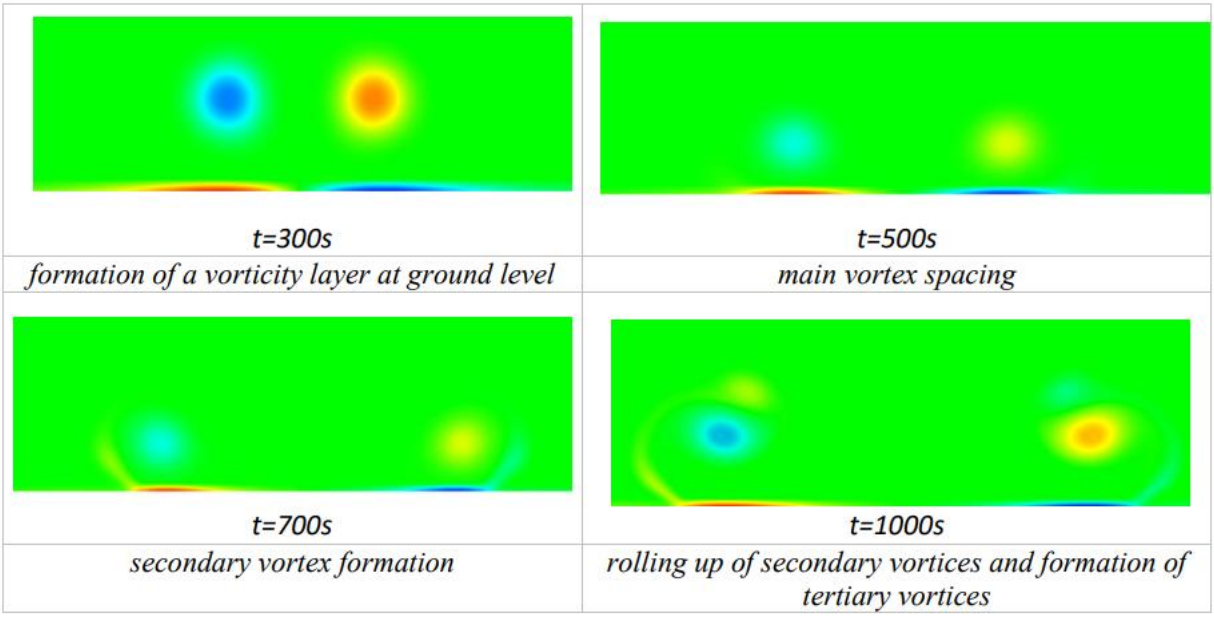


Figure 2: Simulation of the wake vortices in ground effect

It is seen the presence of a layer of vorticity formed above the ground. This vorticity is of the opposite sign of the vortex that generated it. At t = 600s, the layer starts to torn off and a secondary vortex (whose vorticity is of the same sign as the boundary layer) is generated. This one interacts with the main vortex. Although its intensity is lower it exerts a force on it which drives it in a rotational movement. This explains the upward movement of the main vortex. Moreover, main vortices also exert a force on the smaller one which has a rotational movement around the main vortices. After a whole, we can notice the formation of a tertiary vortex (t = 1000s). As long as the vorticity of the vortex is high enough, it can detach the boundary layer and create new vortices.

In order to simulate the effect of the supplementary boundary layer it was used an obstacle in order to generate a physical field of perturbation based on the boundary layer (Figure 3). After 1000 iterations of 10 s it was possible to observe the formed boundary layer (Figure 4).

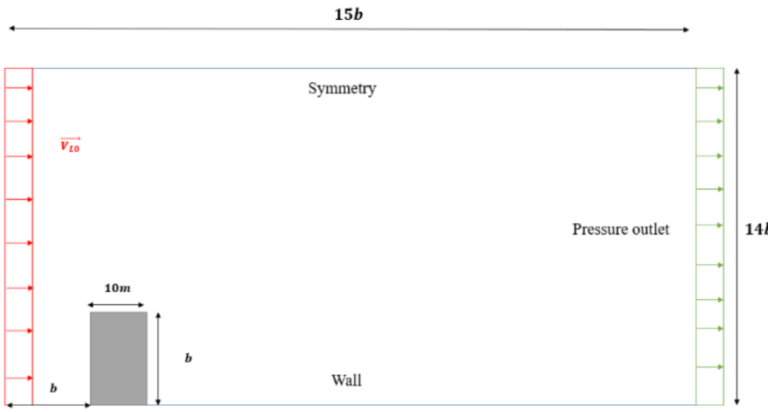


Figure 3: Geometry of the simulation for boundary layer generation

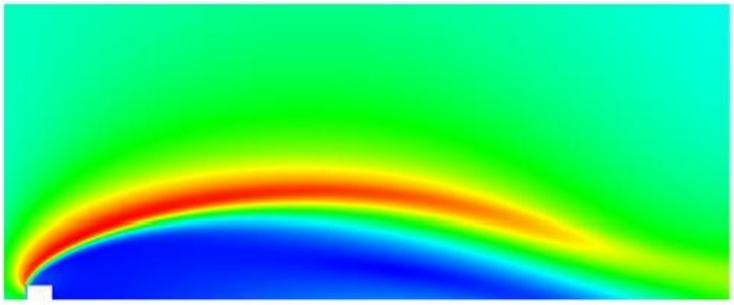


Figure 4: Laminar boundary layer

Then, it was will generated the dipole of vortices above the laminar boundary layer (Figure 5). This situation corresponds to the landing phase of an aircraft. To do so it was added the model of the dipole of vortices to the boundary layer simulation. The initial time of this simulation, $t = 0s$ corresponds to the moment when the boundary layer is fully formed, i.e. a calculation time of $t = 10\,000s$ of the previous calculation.

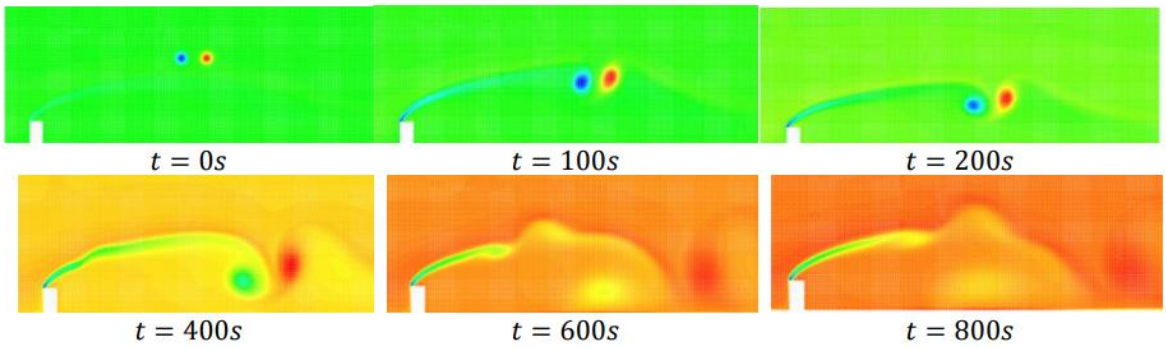


Figure 5: Vorticity field for wake vortices initially situated above the boundary layer

The second simulation (Figure 6) corresponds to a take-off phase, the wake vortices being initially situated in the boundary layer.

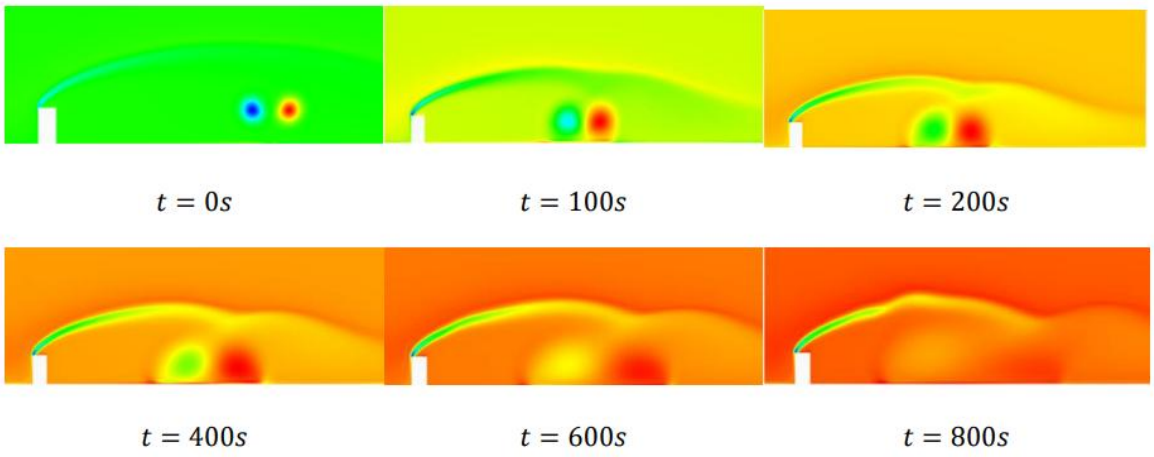


Figure 6: Vorticity field for wake vortices initially situated in the boundary layer

To conclude, even if the atmosphere generated by the perturbation stays almost a laminar flow, wake vortices are dissipated faster in take-off phase if we consider the speed of the aircraft and the atmosphere condition equivalent in the two situations. To observe a simulation in accordance with a real situation, we have to generate a turbulent boundary layer. To do so we will modify the source of the perturbation.

Conclusions

Using these simulations in laminar regime, it was possible to observe the characteristics of the ground effects on the vortex flows in a qualitative way. First, it was observed the descent of the vortex dipole at a constant speed up to an altitude equivalent to a wingspan. Then it was noticed that this speed decreases and that the vortices start to move apart. At a certain distance from the ground, the vortices are subject to the rebound effect due to the viscosity of the ground. These vortices rise and secondary vortices are created after the boundary layer is detached. These vortices rotate around the main vortices and although their vorticity is lower, they still influence the trajectory of the main vortices. Other vortices of low intensity are also created along the horizontal path of the main vortex until it dissipates.

The study based on the building perturbation permits to compare the behavior of vortices under a disturbed atmosphere and a dipole under a stable atmosphere. The first conclusion is that the disturbance improves the vortices dissipation. Without an atmosphere boundary layer, i.e. in a stable atmosphere, vortices dissipate slower for a landing whereas it is dissipated faster into a disturbed atmosphere, which represents an increase of 47%. This time saving is considerable in an operational context.

References

1. **Moldoveanu C.E.,** Moraru F., Şomoiag P., Boisson H.C., Giovannini A., *Turbulence Modelling Applied to Aircraft Wake Vortex Study*, MTA Review, Volum XXI, nr. 1/ **2011**, ISSN 1843-3391;
2. **Moldoveanu C.E.**, Giovannini A., Boisson H.C., Şomoiag P., *Simulation of Wake Vortex Aircraft in Ground Effect*, INCAS Buletin, Volum 3, nr. 1/**2011**, pp. 55-61, ISSN 2066-8201;
3. **Moldoveanu C.E.,** *Modelarea şi simularea numerică a siajului turbulent al aeronavelor*, Editura AGIR, Bucureş ti, **2017**, ISBN: 978-973-720-700-5;
4. **Moldoveanu C.E.**, *Modélisation et simulation des ecoulements turbulents – Simulation des grandes echelles des tourbillons de sillage*, Edition Universitaires Européennes, Saarbrucken, Germania, 222 pag., ISBN: 978-613-1-52198-0, **2010**;

5. **Moldoveanu C.E.**, Şomoiag P., Vedinaş I.,Ferrier P., *Researches Concerning Aircraft Wake Vortex*, 1st International Conference New Challenges in Aerospace Sciences "NCAS 2013", Bucharest, 7-8 November **2013**;

6. **Cocle, R., Dufresne, L., Winckelmans, G**., *LES of multiscale instabilities in wake vortex systems*, International Symposium on Complex Effects in Large Eddy Simulations, Limassol, Cyprus, 20-24 septembrie 2005;

7. **Eriksson, S., Svard, M., Nordstrom, J**., *Simulations of Ground Effects on Wake Vortices at Runways*, Technical report, UPPDALA UNIVERSITET, Sweden, 23 iunie 2007;

8. **Fabre, D., Sipp, D., Jacquin, L**., *Kelvin waves and the singular modes of the Lamb-Oseen vortex*, Journal of Fluid Mechanics Vol. 551, pag. 235-274, 2006;

9. **Holzapfel F.,Stephan A., Tchipev N., Heel T., Korner S., Misaka T**., *Impact of Wind and Obstacles on Wake Vortex Evolution in Ground Proximity*, 6th AIAA Atmospheric and Space Environments Conference, Atlanta, 16-20 iunie 2014;

10. **Leweke T.**,*Far-Wake. Fundamental Research on Aircraft Wake Phenomena.* Publishable Final Activity Report, Marseille, France, 2008;

11. **Misaka T.**, **Holzapfel F., Gerz. T. Manhart M., Schwertfirm F**., *Large-Eddy Simulation of Wake Vortex Evolution from Roll-Up to Vortex Decay*, The 49th AIAA Aerospace Sciences Meeting Including the New Horizons Forum and Aerospace Exposition, Orlando, Florida, 4-7 ianuarie 2011;

12. **Uchiyama T.**, **Shimada S**., *Numerical simulation of the interactions between a vortex pair and solid particles near a wall*, Powder Technology Journal, Vol.257, pag. 55-67, mai 2014;

13. **Wickramasinghe N.K., Harada A., Miyazawa Y**., *Flight Trajectory Optimization for an Efficient Air Transportation System*, The 28th International Congress of the Aeronautical Sciences, Brisbane, Australia, 23-28septembrie 2012.

PARTICULATIRIES REGARDING THE UPGRADING OF AVIATION BOMBS INTO LASER-GUIDED BOMBS

Alin-Constantin Sava, Vasile Nuțu, Cristian-Emil Moldoveanu, Constantin Enache, Pamfil Șomoiag

Military Technical Academy "Ferdinand I", Bucharest, ROMANIA, alin.sava@mta.ro

Abstract: *The objective of this research is it is the argumentation of the specific phenomena encountered during the process of transforming an aviation bomb into a laser-guided bomb. An important feature is the dynamic analysis of the trajectory bomb. The specific characteristics resulting from the specifications of the chosen guidance kit will be reflected in the general behaviour of the guided bomb as a whole. The influence of the guidance law in the design of guided bombs, on the evolution of the bomb on the guided part of the trajectory.*

Keywords*: precision guided munitions, laser guided bomb, guidance kit, guidance law.*

Introduction

Precision guided munitions (PGM), now a common equipment of any modern army, emerged as a technical solution to military operational requirements to destroy pinpoint targets with minimal collateral damage. PGMs have transformed air-to-ground attack operations; instead of using hundreds of classic bombs to attack a single target, a single air transport platform, using the guided munitions of the equipment can attack several targets while minimizing collateral damage.

Other advantages of guided munitions over unguided ones is the much longer range, the clearly superior accuracy that materializes in the reduction of the number of shots required to provide the desired effects on the battlefield. The main disadvantage of these weapons is the cost, especially when we talk about long-range missiles.

Precision guided munitions include the following types of munitions: missiles launched from aerial platforms, missiles launched from naval platforms, missiles launched from multiple launchers, guided bombs.

The influence of the guidance law on the behavior of guided bombs

The fins of the empennage in the unguided version have a non-zero mounting angle, this increases the stability of the bomb's trajectory. The empennage used for the guided version does not have such an angle, because a rotational movement, even if it is of low speed, can only negatively influence the evolution of the bomb on the guided trajectory.

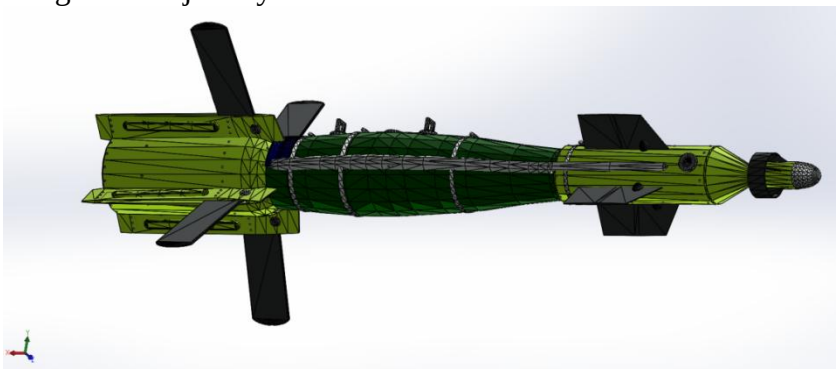


Figure 1: ***Missile – external mesh***

In order to direct the bomb on its trajectory, the control surfaces are located on the directing module. They are arranged in canard configuration. There are four control surfaces, two for each channel.

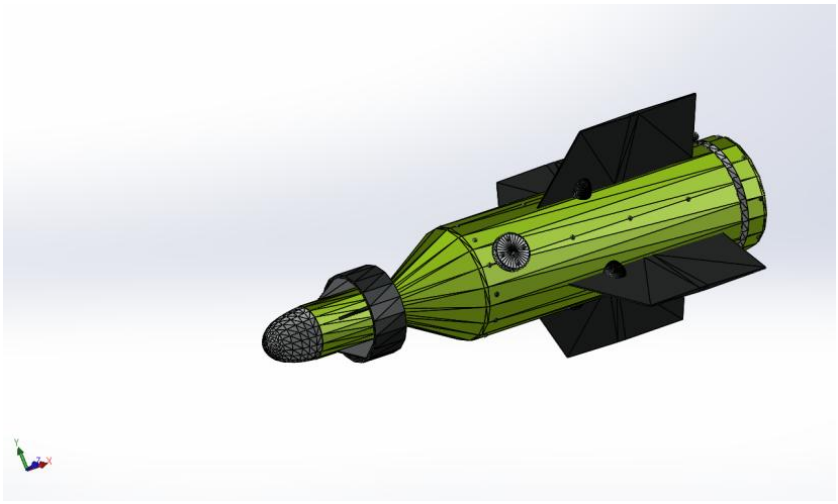


Figure 2: ***Guidance kit***

The choice of the guidance law is of particular importance in the design of guided bombs, since it depends to the greatest extent on the evolution of the bomb on the guided part of the trajectory. The guidance law is closely related to the type of action mechanism chosen. In this case, the mechanism chosen is one specific to guided bombs, with a simple construction, like a double action piston, the piston can only be located in one from the two extreme positions.

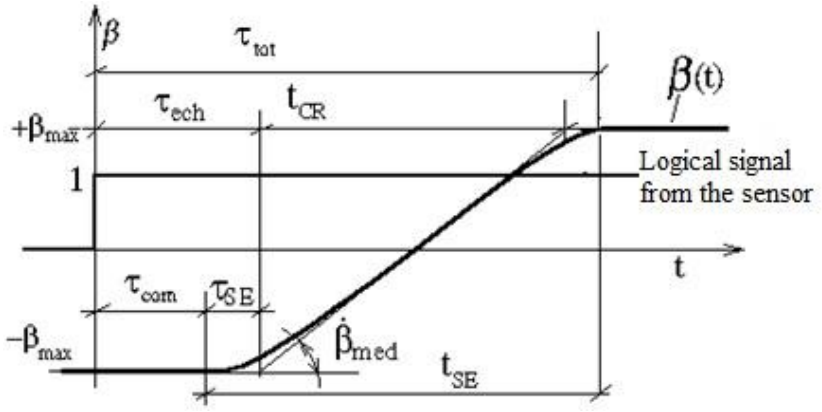


Figure 3: ***The typical response of the execution element***

The movement of the piston begins more slowly, then for a certain period it is done at an approximately constant speed, given by the constructive characteristics of the execution element. The approximately constant movement speed of the piston is justified by the integrative nature of the gas filling phenomenon of the available volumes. The total duration of the piston movement is tSE.

This model is characterized by a global delay, τech, which is the sum of the delay τcom and that corresponding to the execution subsystem, τSE, and by the rise time, tCR. The rise time is given by the ratio between the maximum stroke, 2βmax and the average speed of variation, $\dot{\beta}_{med}$. We will consider the rise time tCR as a constant of the system, and the global delay, τech, which will be further assigned by τ, as a parameter that can be controlled, through its component τcom. [1]

Taking into account the above, the related guidance law in the complex becomes:

$$\beta(s)=\beta_{\max}\cdot e^{-s\tau}\left(\frac{2}{t_{CR}}\frac{1}{s^2}-\frac{2}{t_{CR}}\frac{1}{s^2}e^{-st_{CR}}\right)\Rightarrow \quad (1)$$

$$\left.\begin{aligned}\beta(s)&=\beta_{\max}\cdot\frac{2}{t_{CR}s^2}\cdot e^{-s\tau}\left(1-e^{-st_{CR}}\right)\\ sign\varepsilon&=\frac{2}{s}\end{aligned}\right\}\Rightarrow \quad (2)$$

$$\beta(s)=\frac{\beta_{\max}}{st_{CR}}e^{-s\tau}\left(1-e^{-st_{CR}}\right)sign\varepsilon(s)$$

The actual form of the guidance law is as follows:

$$\beta=\beta_{\max}f\left[sign(\varepsilon(t-\tau)),t_{CR}\right] \quad (3)$$

The steering angles of the control surfaces can thus be expressed through the relations:

$$\begin{cases}\beta_v=\beta_{\max}f\left[sign(\varepsilon_v(t-\tau)),t_{CR}\right];\\ \beta_h=\beta_{\max}f\left[sign(\varepsilon_h(t-\tau)),t_{CR}\right].\end{cases} \quad (4)$$

An important role for the behavior of the bomb on the guided branch of the trajectory is the choice of the guided delay time τ, on which the number of switches and the accuracy of the bomb largely depend.

Numerical simulation, however, involves knowing the numerical values for the mass and aerodynamic characteristics of the guided bomb, among which we list its mass of 285 kg for the this model.

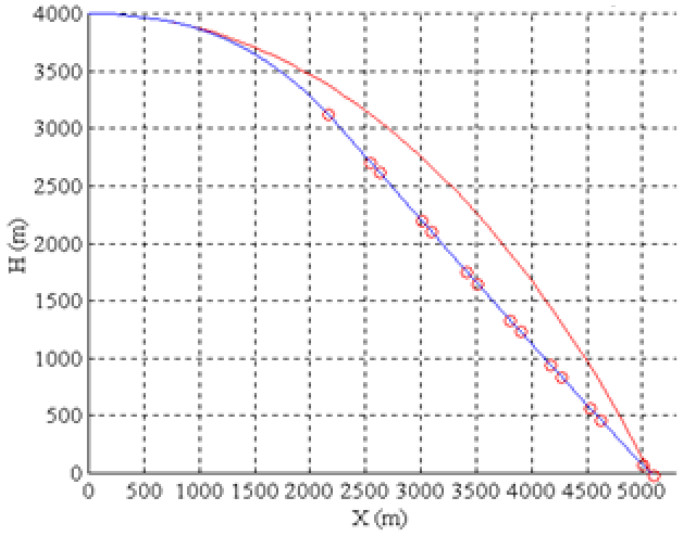


Figure 4: ***The evolution of the bomb on its trajectory. Guided bomb trajectory vs. unguided bomb ones***

The evolution of the bomb on the trajectory is the one represented in figure 4. The unguided trajectory of the bomb is the one drawn in red, and the guided one in blue. The points where the command is given to switch the control surfaces from one extreme position to the other are marked by red circles. The difference between the point of impact with the ground for the guided trajectory and the point of

ballistic impact is less than 1m, a value that confirms the accuracy of the calculus.

The number of switches is ncom=15 switches, the traced trajectory corresponding to a ordered delay time τ=0.2 seconds and a launch speed of 200 m/s (the launch was made from horizontal flight).

The number of switches and the accuracy of the bomb have an inverse influence on the ordered delay time. Decreasing the ordered delay time, until almost canceling it, leads to a considerable increase in the accuracy of the bomb.

As can be seen from the figure, after about three switches, the bomb enters a stable target tracking regime, the evolution on the trajectory being oscillatory, the time between the two switches tending to the ordered delay time.

A decrease in the commanded delay time would lead to a decrease in the time in which an oscillation takes place and implicitly lead to a considerable increase in the number of switchings. The increase in the number of switches leads to the increase in the volume of working agent consumed.

To obtain an acceptable compromise between the number of switches and the accuracy of the bomb, it is necessary to simulate the evolution of the bomb for several launching contexts, to determine the error for each context and the number of switches.

Conclusions

For a given structure of the guided bomb, the delay time in the guidance law is one of the main factors influencing the accuracy of the target tracking process. The connection between delay τ and steering precision can be highlighted through the periods of pseudo-oscillating evolutions when tracking the target on the two channels, which are directly dependent onτ.

The amplitude of the lateral oscillations of the trajectory relative to the line of sight is dependent on the oscillation periods, so τ conditions the scattering of the drop points. In order to obtain high precision, the τ value should be reduced to a minimum, the effect of "bang-bang" commands in this case approaching the effect of gradual "chopper" commands.

Reducing the value of the delay τ to the limit of the equivalent type of delay of the commands can have undesirable effects, at least from two points of view: reducing the possibilities of filtering the signal from the sensor, which can lead to the instability of the tracking regime (too high sensitivity of the guiding module); as well as the increase in the work agent consumption of the execution subsystem.

References

1. Nutu V., Răduţu L., *Missile control actuation systems,* MTA Publishing House, 2002, ISSN 9738290414 1843-3391;

2. Zvîncu N.D., Moldoveanu C.E., Şomoiag P., Sava A.C., Mandache-Dodoi A.D., Dîrloman F.M., Determining the Optimal Time Between Launchings when Firing Multiple Unguided Missiles from Larom Platforms, International Scientific Conference ―Defense Technologies, DefTech 2021, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, Bulgaria, 2021

3. Sava A.C., Birsan Gh., Vedinas I., Piticari I.L., The impact of kinetic projectiles of 76 mm cal. AHEAD type artillery ammunition on the lifting surface of *the aerospace vehicles,* LandForces Academy Revue, Sibiu, Romania, 2016

RESPONSE SURFACE OPTIMIZATION, BASED ON CONTACT STATIC STRUCTURAL ANALYSIS OF NON-PNEUMATIC WHEELS WITH FOUR TYPES OF SPOKES IN THE ENVIRONMENT OF ANSYS WORKBENCH

Genadiy Y. Hinkov

Department of Resources and Technologies Management, "Vasil Levski" National Military University, Veliko Turnovo, Bulgaria, diverser_186@abv.bg

***Abstract**: The text describes the results of Response surface optimization after conducting Static structural analysis of four structural types of non-pneumatic wheels in the environment of ANSYS Workbench. The main intention of the work is to compare the behavior of four most popular shapes of spokes for non-pneumatic wheels, subjected to similar loading and boundary conditions and to choose the most applicable among them.*

***Keywords**: Response Surface Optimization, Static Structural Analysis, Different patterns of non-pneumatic wheel spokes, Comparison.*

ОПТИМИЗАЦИЯ ПО РЕАКЦИОННА ПОВЪРХНИНА, ВЪЗ ОСНОВА НА КОНТАКТЕН СТАТИЧЕН ЯКОСТЕН АНАЛИЗ НА НЕПНЕВМАТИЧНИ КОЛЕЛА С ЧЕТИРИ ВИДА СПИЦИ В СРЕДАТА НА ANSYS WORKBENCH

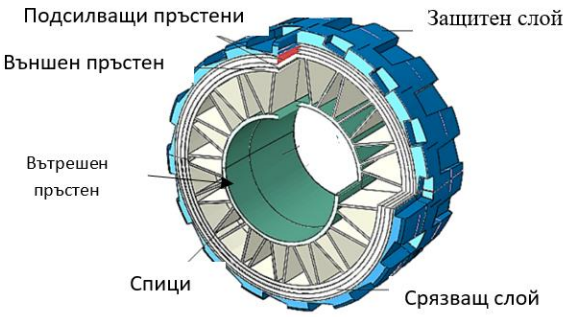
Генадий Й. Хинков

Увод

Непневматичните колела са идея, възникнала в средата на миналия век и възродена от световните автомобилни компании. Въпреки, че не разполагат с гасител на напрежения и трептения като въздух, затворен в камера, непневматичните колела следва да бъдат неуязвими от пробив, външни удари, взрив и нарушена цялост, което ги прави отличен заместител на пневматичните колела в бъдеще особено в условията на бойна среда. Компанията Michelin е предложила идея за непневматични колела, служещи за въздушни витла при полет на превозното средство, чрез хоризонтиране на равнината на въртене. В този текст са разгледани четири от най-утвърдените в световен мащаб форми на спици за непневматични колела. Моделите на колела са подложени на статичен якостен анализ с формулиран контакт с равна хоризонтална бетонна повърхност и последваща оптимизация по реакционна повърхнина. Ситуацията позволява едновременно изследване на софтуера, поведението на спиците и съвременната конструкция на непневматичното колело като механизъм.

1. Статичен якостен анализ на непневматични колела в контакт с хоризонтална бетонна повърхност

Разгледани са модели на непневматични колела с четири форми на спиците: двойки прави спици; големи шестоъгълни спици; малки шестоъгълни спици и дъгообразни спици. Непневматичните колела са изследвани от Senanayake C., Mohan A., Kongara M. и други. Непневматичното колело има срязващ слой и гъвкави спици, направени обикновено от полиуретан. То има защитен слой и два подсилващи пръстена[1]. Изображение на разрез на описания модел е представено на Фигура 4.



Фигура 4: Разрез на модел на непневматично колело.

Поради факта, че стоманените пръстени не позволяват силно нелинейно поведение на външния слой, при прилагане на сила на тежестта върху главината,, спиците над нея биват подложени на опън, а спиците под нея на натиск.

Моделите, създадени за настоящото изследване включват главина и пръстен от алуминиева сплав, спици от полиуретан, външен и вътрешен подсилващи пръстени от стомана, между които е разположен срязващият слой от полиуретан с дебелина 5 мм, гумен защитен слой и хоризонтална бетонна плоча. В средата на ANSYS Workbench за моделиране на частите на колелата са използвани следните материали:

За подсилващите пръстени е използвана конструктивна стомана (structural steel) с модул на еластичност: $E = 200\,000$ МПа; коефициент на Поасон $\mu = 0{,}3$ и плътност $\rho = 7850$ кг/м^3;

За бетонната плоча бетон (Concrete) с модул на еластичност:$E = 19360$ МПа; и коефициент на Поасон $\mu = 0{,}1414$ и плътност $\rho = 2392$ кг/м^3;

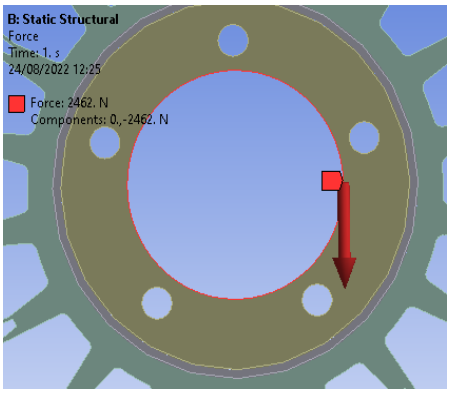
За главината и вътрешния пръстен е използвана алуминиева сплав с модул на ност: $E = 71\,000$ МПа; и коефициент на Поасон $\mu = 0{,}33$ и плътност $\rho = 2770$ кг/м^3

За спиците и срязващия слой полиуретанова гума (Rubber, polyurethane), моделиран с двуконстантен модел на Мууни-Ривлин, в който $C_{10} = 670000$ Па, $C_{01} = 168000$ Па,коефициент на несвиваемост $D = 1{,}2.10^{-9}$ Па$^{-1}$и плътност $\rho = 1200$ кг/м^3;

За защитния слой е използвана естествена гума (Rubber, natural) моделирана с двуконстантен модел на Мууни-Ривлин, в който $C10 = 160000$ Па, $C01 = 41000$ Па и коефициент на несвиваемост $D = 1{,}2.10^{-9}$ Па$^{-1}$ и плътност $\rho = 949{,}8$ кг/м^3.

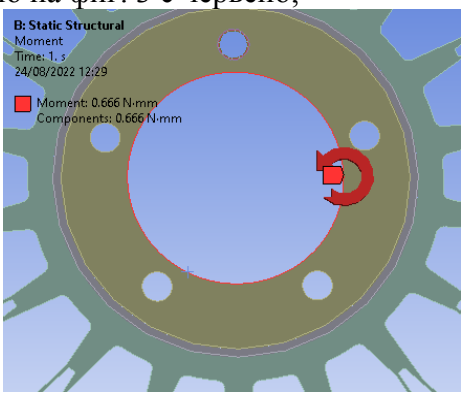
Статичният якостен анализ цели да докаже, че колелата ще устоят на предвидените натоварвания, при експлоатацията на наземно достанционно управляемо превозно средство. Приложените натоварвания и гранични условия са следните:

Сила във отрицателно вертикално направление, приложена върху отвора на главината, както е показано на Фигура 5 с червено с големина $F = 2462\ N$;



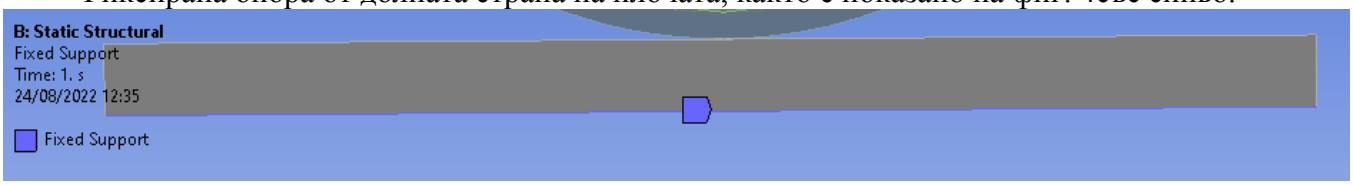
Фигура 5: Вектор на силата, приложена в отвора на главината.

Въртящ момент, породен от двигателя, приложен в отвора на главината с големина $M = 666\ N.mm$, както е показано на фиг. 3 с червено;



Фигура 6: Въртящ момент, приложен в отвора на главината.

Фиксирана опора от долната страна на плочата, както е показано на фиг. 4със синьо.



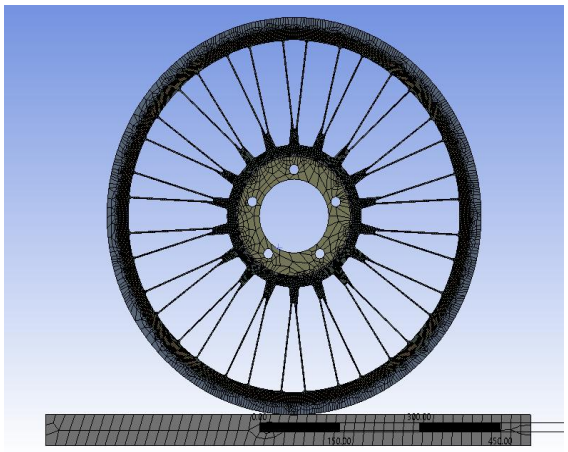
Фигура 7: Фиксирана опора, приложена в основата на бетонната плоча.

За целта на оптимизацията са използвани равнинни модели на колелата. Равнинните модели са получени чрез опцията Midsurface и силно съкращават времето за изчисление, но не отчитат взаимодействието между слоевете в равнината. Счита се, че всеки слой по ширина на колелото е еднакъв и е натоварен еднакво.

Дефиниран е триещ контакт по Усилен метод на Лагранж, който включва предимствата на глобяващия метод и нормалния метод на Лагранж. Зададен е коефициент на триене 0,8.

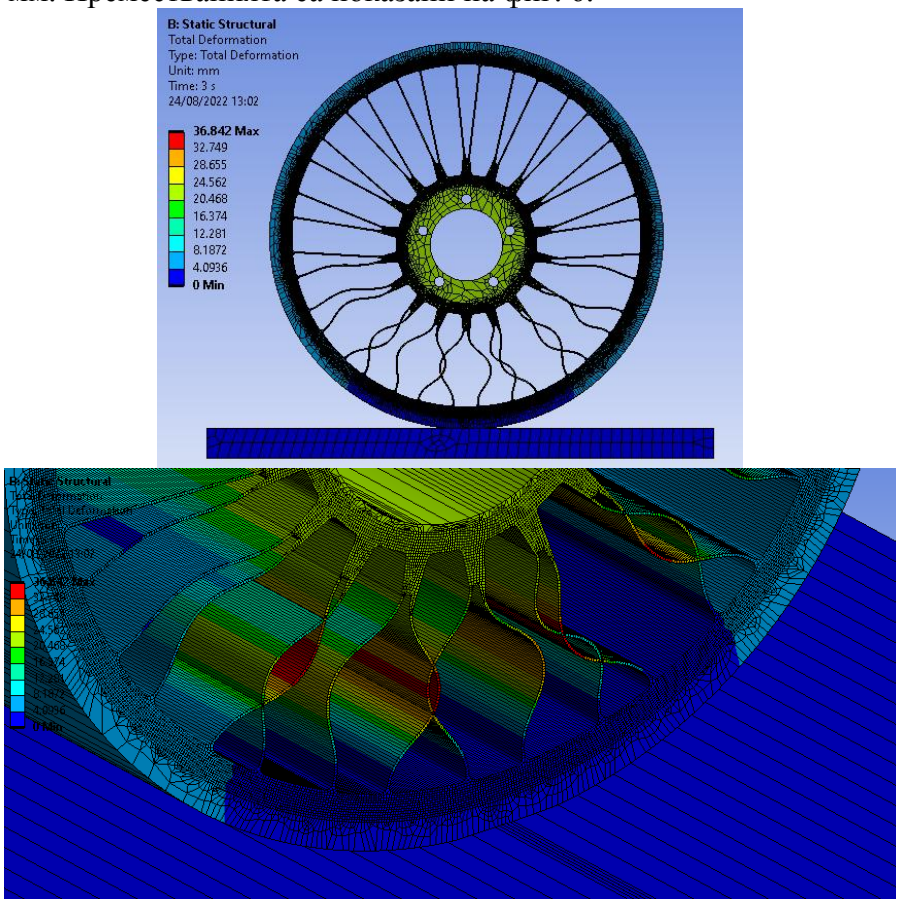
1.1.Контактен статичен якостен анализ на непневматично колело с двойки прави спици:

Крайно-елементният модел на колело с двойки прави спици е показан на фиг. 5.



Фигура 8: Равнинен крайно елементен модел на колело с двойки прави спици.

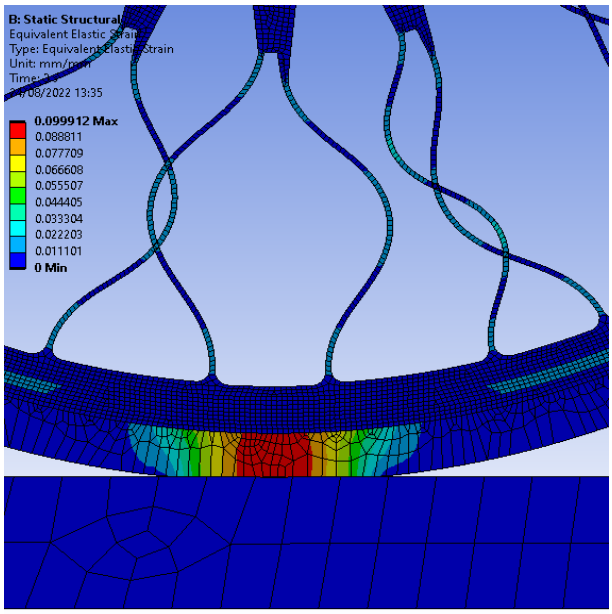
Използван е максимален размер на елементите в колелото 2 мм, за да се обхване взаимодействието между слоевете на съставните части на колелото. Дебелината на спиците на това изображение е 2 мм. Преместванията са показани на фиг. 6.



Фигура 9: Премествания в колело с двойки прави спици.

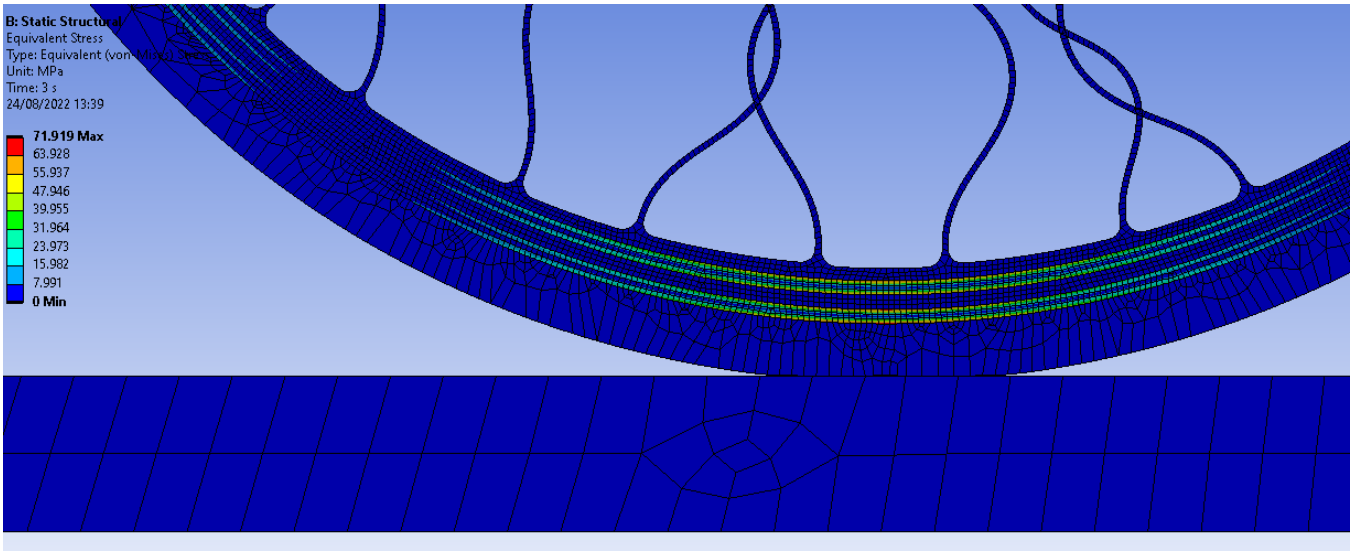
Максималните премествания достигат 36,842 мм и се наблюдават в спиците, които проявяват нелинейно поведение. Това поведение може да доведе до термичен ефект, износване на материала и да намали трайността на колелото. Преместването в главината е около 21 мм.

Максималните еквивалентни еластични обемни деформации настъпват в зоната на контакта на защитния слой с бетонната повърхност и достигат 0,999 мм/мм, както е показано на фиг. 7.



Фигура 10: Максимални еквивалентни обемни деформации.

Максималните еквивалентни напрежения се наблюдават в прекъснати области от контакта на подсилващите стоманени пръстени и съседните им слоеве. Те достигат 71,919 МПа и са показани на фиг. 8.



Фигура 11: Максимални еквивалентни напрежения.

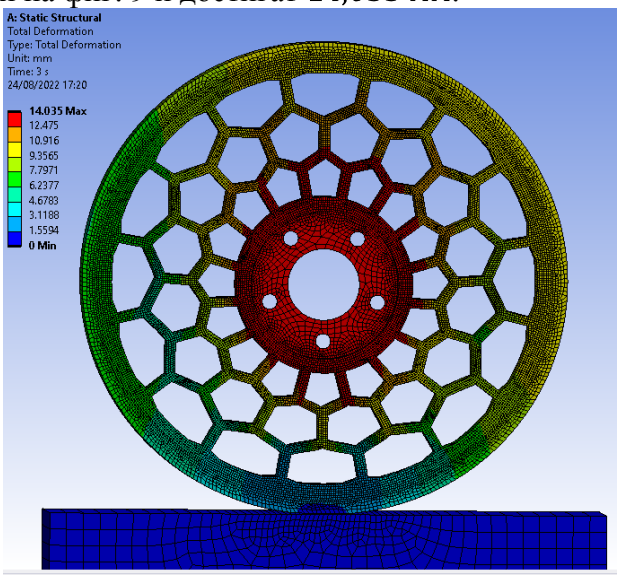
Полиуретанът и гумата са свръх еластични материали т. е. допускат до 800 % деформации при незначителни напрежения в материала.

Изводи от анализа: Тъй като усилващите пръстени не са обект на интерес, не следва да се отчитат максималните еквивалентни напрежения за останалите типове колела.

Коефициентът на Поасон за свръх еластичните материали е близък до 0,5, а коефициентът на несвиваемост близък до нула, поради което те претърпяват високи обемни деформации най-вече при натиск. Тъй като защитният слой не е обект на интерес, не следва да се отчитат максималните обемни деформации за останалите типове колела.

1.2. Контактен статичен якостен анализ на непневматично колело с големи шестоъгълни спици:

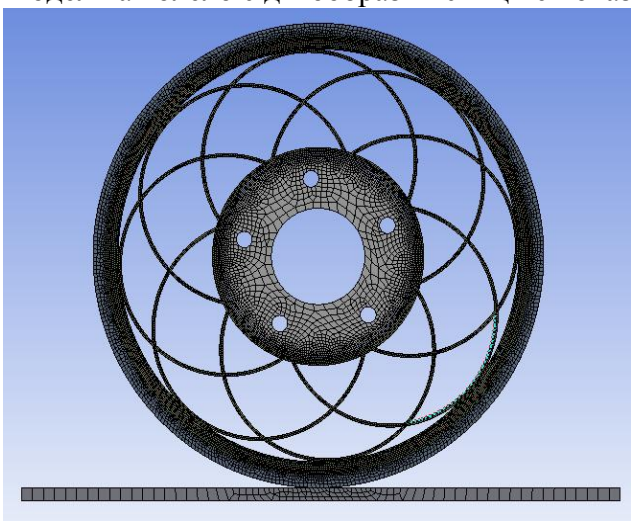
Дебелината на спиците на модела е 10 мм, а максималните премествания, които са в зоната на главината са показани на фиг. 9 и достигат 14,035 мм.



Фигура 12: Максимални премествания при колело с големи шестоъгълни спици.

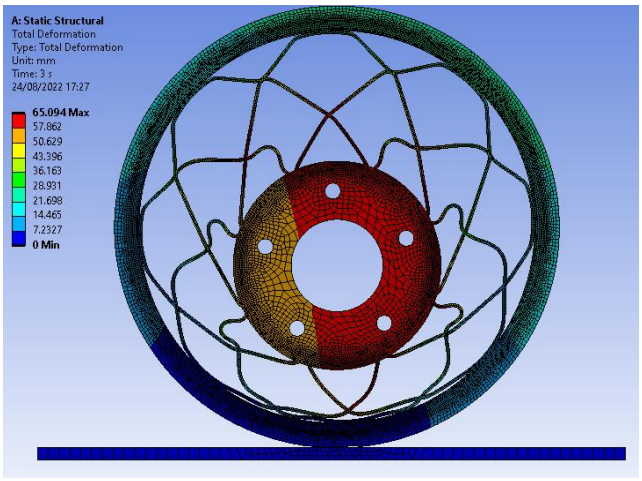
1.3. Контактен статичен якостен анализ на непневматично колело с дъгообразни спици:

Крайно-елементният модел на колело с дъгообразни спици е показан на фиг. 10.



Фигура 13: Равнинен крайно елементен модел на колело с дъгообразни спици.

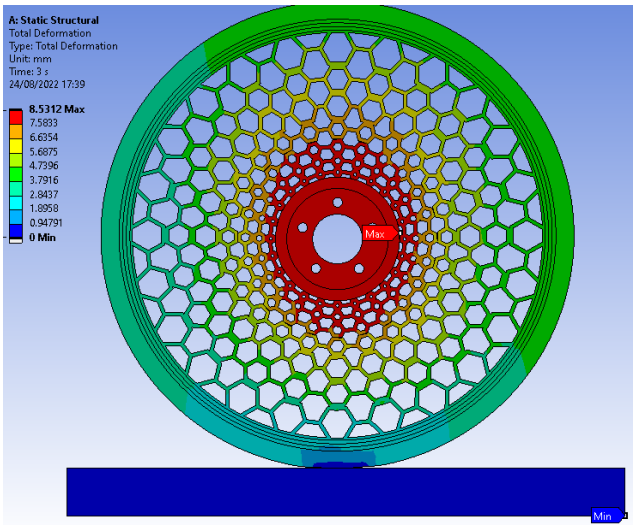
Дебелината на спиците на модела е 5 мм, а максималните премествания, които са в зоната на главината са показани на фиг. 11 и достигат 65,094 мм.



Фигура 14: Максимални премествания при колело с дъгообразни спици.

1.4. Контактен статичен якостен анализ на непневматично колело с малки шестоъгълни спици:

Дебелината на спиците на модела е 5 мм, а максималните премествания, които са в зоната на главината са показани на фиг. 12 и достигат 8,5312 мм.



Фигура 15: Максимални премествания при колело с малки шестоъгълни спици.

Изводи от статичните анализи: Колелото с дъгообразна форма допуска най-големи премествания, а колелото с малки шестоъгълни спици допуска най-малки премествания.

2. Конструктивна оптимизация на непневматични колела въз основа на проведения контактен статичен анализ.

ANSYS Workbench провежда оптимизация по метода МОГА- модифициран оптимизационен генетичен алгоритъм. Генетичните алгоритми работят на случаен принцип, поради което се справят с всякакъв вид нелинейности и прекъснатости на функциите в областта им.

2.1. Проект на експеримента:

Данните от проведените проекти на експеримента са дадени в табл. 1.

Таблица 1: Обхват на вариране на променливите.

Тип спици на колело	Входен променлив параметър 1	входен променлив параметър 2	Входен променлив параметър 3	Обхват на вариране на променлива 1	Обхват на вариранена променлива 2	Обхват на вариранена променлива 3
Двойки прави	Дебелина на спиците (мм)	ширина на спица (мм)	—----------	От 100 до 300	От 2 до 15	—-------
Големи шестоъгълни	Дебелина на спиците (мм)	ширина на радиалните спици (мм)	ширина на концентричните спици (мм)	От 100 до 300	От 5 до 15	От 5 до 15
Малки шестоъгълни	Дебелина на спиците (мм)	ширина на радиалните спици (мм)	ширина на концентричните спици (мм)	От 100 до 300	От 5 до 15	От 5 до 15
Дъгообразни	Дебелина на спиците (мм)	Вътрешен радиус на спица ($_0$)	—----------	От 100 до 300	От 140 до 155	—-------

2.2.Реакционна повърхнина:

Изследването на чувствителността показва, че масата и максималните премествания са имат сходна чувствителност към входните параметри, като при шестоъгълниците дебелината е решаваща, а при другите два типа ширината на спиците е решаваща.

От реакционните повърхнини се разчита ниско значение на концентричните спици за преместванията, при дъгообразните спици, решаващ е радиусът.

2.3.Процес на оптимизация:

Цел на оптимизацията е да се минимизира масата, ограничително условие е максималните премествания се запазят по-малки или равни на 40 мм.

Резултатите от оптимизацията са представени в табл. 2.

Таблица 2: Оптимални стойности, получени след решаване на оптимизационните задачи.

Вид спици	**Двойки прави**	**Големи шестоъгълни**	**Малки шестоъгълни**	**Дъгообразни**
Стойност на параметър 1	100,63	100,02	100,01	194,26
Стойност на параметър 2	6,807	9,833	4,001	147,05
Стойност на параметър 3	—----------	5,819	4	—----------
Стойност на маса на спиците	8,1592	6,432	5,930	12,068
Стойност на максимални премествания	39,986	39,976	17,411	39,973

Изводи от оптимизацията:

1. Малките шестоъгълни спици превъзхождат всички останали с най-малката си маса и преместване много по-ниско от ограничителното условие в оптимизационната задача.
2. Дъгообразните спици допускат най-големи премествания и същевременно масата им е най-голяма.

Заключение:

Проведен е статичен анализ на четири модела на напневматични колела с различни спици в средата на програмата ANSYS Worbench. Въз основа на статичния анализ е проведена оптимизация по реакционна повърхнина. При непневматичните колела най-големи еластични обемни деформации възникват в контактната зона на защитния слой със земната повърхност, най-големи напрежения в усилващите стоманени пръстени, а най-големи премествания в областта около главината или в области на нелинейно поведение на спиците. Графичният модул за създаване на модели Space Claim показва слабости при работа със заоблени ръбове и изтегляне на съседните им. След оптимизацията е установена непригодност на дъгообразните спици за конкретният сценарий на натоварване, докато малките шестоъгълни спици превъзхождат останалите. Предстои да се анализира преминаване на неравност с висока скорост в системата Explicit Dynamics на ANSYS Workbench.

Благодарности:

Анализите са проведени благодарение на безплатен лиценз, дарен от ANSYS на Националния Военен Университет „Васил Левски".

References

1. Mohan, Aravind & Johny, C & Tamilarasu, A & Bhasker, Pradeep & Krishnaiah, Ravi. (2017). Design and Analysis of Non-Pneumatic Tyre. IOP *Conference Series: Materials Science and Engineering.* 263. 062061. 10.1088/1757-899X/263/6/062061.
2. Senanayake, Chanaka & Premarathna, Aruna & Wijesundara, Kushan & Jayasinghe, J. A. S. C. & Ranathunga, R.. (2021). Performance Comparison of Solid Tires and Non-Pneumatic Tires Using Finite Element Method: Application to Military Vehicles. *13-th International Research Conference General Sir John Kotelawala Defence University*, Faculty of engineering, University of Peradeniya. Paper ID 146.
3. Kongara M. et al. (2018). Modeling And Analysis of Honeycumb Airless Tire. *Anantapur. IJSART Volume 4, issue12,*. ISSN (online): 2395-1052.

APPLYING OPTIMIZATION METHODS IN LOGISTICS

Andrey I. Bogdanov, Vanko V. Ganev

Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Shumen, Bulgaria, a.bogdanov@shu.bg; Artillery, AD and CIS faculty, National military inuversity "Vasil Levski", Shumen, Bulgaria, vvganev@nvu.bg

***Abstract**: The report deals with various models and methods for solving logistical optimization tasks in competition. It describes a particular method for assessing the customer logistics service.*

***Keywords**: logistics service; optimization tasks*

ПРИЛАГАНЕ НА ОПТИМИЗАЦИОННИ МЕТОДИ В ЛОГИСТИКАТА

Андрей И. Богданов; Ванко В. Ганев

Факултет по технически науки, Шуменски университет „Епископ Константин Преславски”, Шумен, България, a.bogdanov@shu.bg; Факултет „Артилерия, ПВО и КИС“, Национален военен университет "Васил Левски", Шумен, България, vvganev@nvu.bg

***Abstract**: Докладът разглежда различни модели и методи за решаване на задачи за логистична оптимизация в условията на конкуренция. Той описва конкретен метод за оценка на клиентската логистична услуга.*

***Keywords**: логистично обслужване; оптимизационни задачи*

Увод

Логистиката и логистичните системи съществуват и се развиват, за да обслужват потребителите, а логистичният цикъл се отъждествява с цикъла на изпълнение на поръчката на клиента. Логистичното обслужването на клиентите се явява крайна фаза на веригата от логистични дейности и резултат на тяхното успешно функциониране. То е важен елемент на маркетинг-микса на организацията, тъй като осигурява реалното достигане на продуктите до клиентите и по такъв начин пряко влияе на логистичните разходи, на печалбата и рентабилността.

Изложение

Изследванията на основните логистични дейности, включително поведението на логистичните системи и тяхното оптимизиране, се осъществява чрез разнообразни методи. Твърде често се използват и методите на математическото моделиране. Същността на тези методи се състои в това, че конкретна сложна логистична дейност, процес (логистична система или части от нея) се представя чрез друга такава, наречена модел, който в една или друга степен е адекватен на тази система. При построяване на подобни модели задължително се спазват следните изисквания:

- поведението, структурата и функцията на модела да бъдат адекватни на моделираните логистични дейности, процеси, системи.

- отклонението на параметрите на модела от съответните параметри на моделирания обект да не излизат извън рамките на допустимата точност на моделиране.

- резултатите от изследването на модела и неговото поведение трябва да извеждат нови свойства на моделираните логистични дейности (процеси, системи), не намерили отражение в изходната им формация, използвана за съставянето на дадения модел.

- моделът трябва да бъде значително по-удобен за изследване и изучаване, отколкото реалният аналог.

Съблюдаването на посочените изисквания създава и осигурява реализирането на качествено нови възможности, по-важни от които са [1, 5]:

- става възможно изследванията за установяване на целесъобразността от създаването и използване на конкретната логистична система и/или нейни звена да се провеждат още на етапа на проектирането на системата;

- изследванията се извършват без намеса във функционирането на логистичната система;

- пределно допустимите стойности на обемите на материалните потоци и другите параметри на логистичната система могат да бъдат определяни без риск от разрушаване на моделираната система.

Решаването на моделите се осъществява с помощта на съответни математически методи. В отделни случаи се налагат допълнителни преобразувания или опростявания на моделите, за да се приведат до такъв вид, за който съществуват рационални методи за решаване. Изборът на подходящ метод за намиране на решенията на моделите е съществен момент от моделирането на логистични дейности, процеси и системи.

Най-често срещаните в литературата модели, предназначени за изследване в логистиката, могат да бъдат разделени в три групи [1, 6, 8]:

Първо, модели и методи, предназначени за решаване на логистични задачи в условия на определеност, без ограничения от динамиката на външната среда.

Второ, модели и методи за решаване на логистични задачи в условия на риск и неопределеност, но не отчитащи конкуренцията.

Трето, моделите и методите, предназначени за решаване на логистични задачи в условия на конкуренция. (табл. 1)

Таблица 1

Модели в условията на определеност	**Модели в условията на риск и неопределеност**	**Модели в условията на конкуренция**
Подпрограми	**КЛАСОВЕ**	
	А	**В**
1. Модели формализиращи отделни логистични операции и/или функции	А. Без оптимизация	В. С използване на оптимизационни модели
2. Модели в които се изследват две или повече логистични операции и/или функции	А. Еднокритериални задачи	В. Многокритериални задачи
3. Модели, формализиращи цели логистични системи	А. Анализиране на системите , оценка на ефективността на системите	В. Проектиране на логистични системи

Всяка от групите от своя страна се подразделя на три подгрупи, в рамките на които се формират отделни класове модели и методи. Разграничаването на подгрупи се определя от степента на отчитане в конкретния модел на логистичните операции и функции, докато класовете се разгра-

ничават в зависимост от сложността на моделите, за разрешаването на които се изискват специални процедури, например оптимизация.

Първата група модели се считат за най-разпространени и използвани в стопанската практика. Към клас "А" на тази група следва да бъдат отнесени:

- модели за избор на доставчик, посредник, спедитор, вид на транспортно средство, начин на превози и т.н.;
- модели за прогнозиране на количеството необходими материални ресурси, обема произвеждана продукция, текущите запас в склада и т.н.;
- адитивни времеви модели („точно на време");
- модели за определяне на потребностите;
- модели за определяне на запасите и др.

Към клас "В" на същата група се отнасят моделите, при които се използват оптимизационни методи, в частност математическото оптимиране, например, транспортна задача на линейното оптимиране, задачата за търговския пътник, различни комбинаторни методи.

Към втората група се включват модели, при които се обхващат две или повече логистични операции или функции. В този смисъл моделите от тази група се формират на базата на получени резултати от моделите от първата група. Разделението на тази група на класове се осъществява на основата на броя на използваните критерии за оптимизация. Към първия клас се отнасят тези модели, при които отсъства оптимизационна процедура или се използва само един критерий за оптималност. Във втория клас модели се включват преди всичко многокритериалните оптимизационни модели, като например:

- определяне на оптималния размер на доставката;
- определяне на оптимални срокове за осъществяване на доставките;
- формиране на номенклатурата и асортимента на разпределителните и търговски центрове на различни равнища;
- избор на вида на транспорта и начините на превозите.

За моделите от третата група е характерно, че се включват всички звена и елементи на моделираната логистична система (мрежа, верига или канал). Към първия клас модели могат да бъдат отнесени тези, които са свързани с анализа на ефективността на дейностите в цялата логистична система. Към втория клас се отнасят моделите за проектиране на логистични системи с използване на принципите на „минимизиране на общите логистични разходи" или „икономически компромиси". По такъв начин те са ориентирани към решаването на един от главните проблеми на теорията и практиката на логистиката - проектирането на логистични системи.

Моделите и методите за оптимизиране на логистични системи имат основното предназначение да изключат интуитивния подход при вземането на управленски решения и да ги обективизират. На практика, в логистичната практика като цяло, както и при изграждането и експлоатирането на логистични системи, творческата интуитивна дейност на отделни специалисти и колективи в много случаи се оказва решаваща. В този смисъл широко приложение в логистиката намират редица методи, основани на използването на опита, квалификацията и творческия потенциал на специалисти по организацията и управлението на различни стопански и производствени процеси.

Като най-важни комплексни критерии за оценка на логистичното обслужване се очертават: достъпност, функционалност и надеждност.[4] Те се явяват основни измерители за качеството на обслужване и осигуряват контрола и оценката на неговата ефективност.

Критерий № 1. Достъпност. Тя се свързва с наличието на запаси за непрекъснато и своевременно задоволяване потребностите на клиентите. Достъпността на запасите отразява възможностите на предприятието да доставя продукта на клиента тогава, когато е необходимо.

Критерий № 2. Функционалност. Тя се определя с времето от момента на постъпване на поръчката до момента на нейното изпълнение, т.е. с цикъла на изпълнение на поръчката. Функционалността характеризира възможностите за поддръжка на очакваните срокове и гъвкавост на операциите при обслужването на клиентите.

Критерий № 3. Надеждност. Надеждността на обслужването е способността да се поддържа планираното равнище на достъпност на запасите и функционалността на операциите. Надеждността се изразява, чрез способността на обслужването да функционира без отказ. Тя може да се определи като вероятност за безотказна работа на дадена система в течение на определен период от време при определени условия.

При оценката на равнището на логистичното обслужване е целесъобразно да се изберат най-значимите услуги, както и тези, които оказват съществено влияние върху разходите.

С приложение са три основни подхода за анализ и оценка на логистичното обслужване - проучване на клиентите, моделиране и експерименти и симулации.[3]

Първи подход: Проучване на клиента. Той се явява традиционен метод за анализ и оценка на логистичното обслужване. Положителното е, че се осигурява информация за целите и намеренията на клиентите и очаквания модел на тяхното поведението. За целта се задават въпроси, като: колко и какви продукти допълнително биха закупили, ако обслужването е на по-високо равнище; какъв е минималният приемлив стандарт на обслужване; кои са решаващите елементи, които считат, че трябва да бъдат част от тяхното логистично обслужване и други. Едновременно с това добре проектираното проучване е отлично средство за събиране на информация и за конкурентите и техните потенциални възможности.

Втори подход: Моделиране. То се основава на анализа на връзката между продажбите и факторите, свързани с логистичното обслужване на клиентите. Целта е да се установят характеристиките на влиянието на обслужването на клиентите върху продажбите, като за повишаване на надеждността и достоверността на модела се извършва и емпирична проверка. Едновременно с това, за изолиране и измерване на ефектите от логистичното обслужване на клиентите се изисква всички останали пазарни и непазарни фактори да останат постоянни. Друго съществено изискване е да се обхванат всички фактори, осигуряващи желаното равнище на обслужване на клиентите, както и да се отчита времевата разлика между промените в равнището на обслужване и изменението на продажбите.

Трети подход: Провеждане на експерименти и симулации. Те се явяват "лабораторни" техники за установяване модела на вземане на решения от клиентите при различни равнища на логистично обслужване. Използват се и контролни проверки на пазарната среда за наблюдения на промените в поведението на клиентите при различни равнища на обслужване, наблюдава се и размера, до който продажбите се променят директно при алтернативни равнища на обслужване. Основно изискване е лабораторната среда точно да копира реалните условия. Целта на симулацията е да разкрие, какво може да се случи при действителни пазарни условия и да предложи възможност за наблюдение във виртуална "безрискова" обкръжаваща среда.

Анализът и оценката на логистичното обслужване е целесъобразно да се осъществи и чрез комплекс от следните показатели:[5] (таблица 2.)

Таблица 2. Показатели за оценка на логистичното обслужване

Вероятност за дефицит	
$P(Q) = \frac{1}{n}\sum \frac{Q_{ні}}{Q_{общі}}.100\%$	$Q_{ні}$ - количеството на поръчките на і-я клиент, неудовлетворени от наличните запаси за определен период от време $Q_{общі}$ - общо количество на поръчките на і-я клиент за този период *n*- общ брой клиенти
Норма на насищане със запитвания	
$N_З = \frac{1}{k}\sum_{i=1}^{k} \frac{З_{налі}}{З_{трі}}.100\%$	$З_{налі}$ - общо количество на наличните запаси от *і-я* вид продукция за определен период от време $З_{трі}$ - количество на запасите от *і-я* вид продукция, необходими за удовлетворяването на всички запитвания за поръчки на клиентите *k*- количество на продукцията

Пълнота на обхвата на поръчките	
$П_{охв} = \sum_{i=1}^{n} H_i$	H_i - случаите за определен период от време, когато всички запаси на предприятието от *i-я* вид продукция са поръчани от клиентите *k*- количеството на продукцията
Степен на удовлетворяване на очакванията на клиентите за изпълнение на поръчките навреме	
$T = \frac{1}{n}\sum_{i=1}^{n}\left(\frac{t_{ожi}}{t_{фi}}\right)$ $T \to 1$	$t_{ожi}$ -време за изпълнение на поръчките, очаквано от i-я клиент $t_{фi}$ - фактическо време за изпълнение на поръчките на i-я клиент *n*- общ брой клиенти
Непрекъснатост на изпълнението на логистичните операции	
$K = \frac{1}{n}\sum_{i=1}^{n}\frac{Q_{ci}}{Q_{Bi}}$	Q_{ci} - количеството на поръчките на i-я клиент, изпълнение в съответствие с изискваните срокове Q_{Bi} - общо количество на изпълнените поръчки на i-я клиент n- общ брой клиенти
Гъвкавост на логистичните операции	
$F = \frac{Q_{уд}}{Q_{тр}}$ $F \to 1$	$Q_{уд}$ - количество на удовлетворените изисквания $Q_{тр}$ - количество на допълнителни услуги, предоставени на клиентите
Равнище на недостъчно обслужване	
$Y = \frac{Q_{пр}}{Q_{общ}}$	$Q_{пр}$ - количество на поръчки, по отношение, на които са постъпили рекламации от страна на клиентите $Q_{общ}$ - общо количество на поръчките
Надеждност на обслужването	
$H = f(P(Q); N_З; П_{охв}; T; K; F; Y)$	$P(Q)$ - вероятност за дефицит $N_З$ - норма на насищане със запитвания $П_{охв}$ - пълнота на обхвата на поръчките T – степен на удовлетворяване на очакванията на клиентите за изпълнение на поръчките навреме K – непрекъснатост на изпълнението на логистичните операции F – гъвкавост на логистичните операции Y – равнище на недостатъчно обслужване

За оценка на равнището на логистично обслужване може да се използва и обобщаващ показател, изчисляван по формулата:

$$\eta = \frac{m}{M} x100 \qquad (1)$$

където:

η - равнище на логистичното обслужване;

m - количествена оценка на теоретично възможните обеми на оказаните логистични услуги;

M - количествена оценка на фактическите обеми на оказаните логистични услуги.

Следва да обобщим, че задълбочената оценка на логистичното обслужване изисква приложението на система от методи, а именно – проучване на клиентите, моделиране, провеждане на експерименти и симулации, както и комплекс от показатели, характеризиращи нивото на изпълнение на логистичното обслужване. Всеки един от тези методи съдейства за оценяване на логистичното обслужване в различни аспекти, които в своята съвкупност изцяло го характеризират.

Заключение

Протичащите в икономическия живот на страната сериозни промени, свързани основно с икономическата криза оказват голямо влияние върху организациите от всякакъв тип. С цел повишаване на своята конкурентоспособност, организациите насочват своите ежедневни усилия към намаляване на разходите и бързи и адекватни реакции, съобразени с изискванията на клиентите. Те търсят иновативни решения и технологии, целящи подобряване на нивото на обслужване на клиентите, задържане на старите и привличане на нови клиенти. Основната им задача е да се преборят с конкуренцията и да оцелеят при намаленото потребление.

Ето защо, е целесъобразно да се търсят начини за повишаване на качеството на предлаганото логистично обслужване, но с по-малко разходи. По наше мнение такива възможности предлагат оптимизационните и симулационни методи.

References

1. Благоев Б. и др. Стопанска логистика, Изд. „Наука и икономика" Икономически университет Варна, 2009.
2. Гаторна Дж. Основи на логистиката и дистрибуцията, Изд „Делфин прес" Бургас 1996.
3. Чейз Р. Производственный и операционный менесжмент, Москва 2007.
4. Coello C, An Empirical Study of Evolutionary Techniques for Multiobjective Optimization in Engineering Design, Department of Computer Science, Tulane University.
5. Andersson Johan, A survey of Multiobjective Optimization in Engineering Design - Department of Mechanical Engineering, Linköping University, Sweden.

ARTILLERY BLASTERS

Ivelina Angelska

** NITI SHC Kazanlak, Bulgaria, angelska.i@abv.bg*

***Abstract**: The document presents a brief description of artillery blasters and their purpose.*

***Keywords**: artillery blasters*

Въведение

Възникването и развитието на взривателите и взривателните устройства е свързано неразривно с общото развитие на артилерията, която е решавала задачи в различните исторически периоди в зависимост от нивото на техниката и степента на развитие на производството. Началото на развитие на взривателните устройства се характеризира с използването на прости запалки за задействане на снаряди със сферична форма, намерили широка употреба в артилерията от XVI до XIX век. С преминаването на нарезни артилерийски системи започва използването на взриватели с ударно действие, сработващи при среща на снаряда с преграда. Непосредствено след ударните, се появяват дистанционните взриватели и запалки, позволяващи преди стрелба да се включат една или друга дължина на дистанционния състав, осигуряващ разрив на желаното разстояние.

Взривателят е устройство, предназначено за взривяване на разривния заряд на боеприпас (артилерийски снаряд, мина, авиобомба, бойната част на ракета, торпедо). Според принципа на работа взривателите се делят на контактни, дистанционни, безконтактни, командни, а също и на такива с комбинирано действие. Първият най-обикновен взривател е разработен от Алфред Нобел за осигуряване на надежден взрив на изобретения от него динамит и се състои от капсул и детонатор. Инициращият импулс в него е огънят. Впоследствие в армиите на различните държави получават широко разпространение ударните взриватели, които доминират в продължение на последните 100 години.

1. Огнева верига

Огневата верига на взривателя представлява верига от последователно сработващи средства за иницииране и пиротехнически елементи, формираща детонационен или възпламенителен импулс. В най-общия случай може да бъде разгледана като състояща се от две части: възпламенителна и детонационна.

Пиротехническата представлява верига от последователно сработващи елементи като капсул-възпламенител и елетровъзпламенител.

За разлика от пиротехническата верига, която като правило изработва огневи импулс, детонационната част на огневата верига включва устройства, чиято крайна цел е изработването на детонационен импулс, необходим за предизвикването на разрив на боеприпаса.

Използваните в огневата верига на взривателите капсул-възпламенители и капсул-детонатори са чувствителни към резки външни въздействия. При разработването и производството на посочените елементи се вземат мерки за изключване на възможността за сработването им от силите на инерция, възникващи при изстрел. Поради това, във взривателите се използват устройстрва, изолиращи елементите на огневата верига един от друг.

В зависимост от това кой елемент е изолиран, взривателите се делят на три групи:

- взриватели предпазителен тип, в които капсул-детонаторът или електродетонаторът са изолирани от детонатора по такъв начин, че сработването им до момента на взвеждане не предизвиква инициирането на детонатора;
- взриватели полупредпазителен тип, в които капсул-възпламенителят или електровъзпламенителят са изолирани от капсул-детонатора или петардата така, че сработването им до момента на взвеждане не предизвиква инициране на капсул-детонатора или петардата;
- взриватели непредпазителен тип, в които капсул-възпламенителят или електровъзпламенителят не са изолирани от капсул-детонатора или петардата, а капсул-детонаторът и електродетонаторът не са изолирани от детонатора.

Повечето от съвременните артилерийски взриватели са предпазителен или полупредпазителен тип, тъй като осигуряват по-голяма безопасност на траекторията до момента на извършване на взвеждането.

В детонационната част на огневата верига се наблюдава процес на детонация на веществото, основните особености, на който се заключва в следното:

- енергията и последователното инициране на взривната реакция се осигурява благодарение на разпространението на ударната вълна по взривното вещество;
- скоростта на процеса на детонация винаги е много по-голяма от скоростта на звука в изходното взривно вещество;
- продуктите на детонация непосредствено зад фронта на ударната вълна в първия момент се движат в посока на разпространението на вълната, следствие на което налягането в зоната на реакция е много високо.

Детонационната част на огневата верига може да съдържа следните елементи: елетродетонатор или капсул-детонатор, предавателен заряд и детонатор.

Пиротехническите устройства се състоят от една или повече запресовки от пиротехнически състав, който гори на слоеве с определена скорост, устройство на възбуждане на горенето и изпълнително устройство.

Пиротехническата запресовка се състои от възпламенителна подпресовка, основна запресовка и усилител. Като средство за възпламеняване се използва елетровъзпламенител.

Скоростта на горене на пиротехническия състав се определя от технологични фактори, от процеса на производство на пиротехническия състав и процеса на производство на пиротехническото устройство. Скоростта на горене зависи и от вътрешни фактори – вътрешни свободни обеми, херметичност, изменение на налягането в процеса на горене, температурата.

1.2 Време на действие на пиротехническите устройства

Определянето на времето на действие на пиротехническите устройства се свежда до намирането на определящия размер h на пиротехническата запресовка в съответствие със зададените параметри – свободен обем, вид на състава, плътност на запресовка или до намиране на времето на действие на зададена конструкция на устройството. При получаване на разчетните зависимости за пиротехническо устройство с време на действие над 0,1 s могат да бъдат пренебрегнати отделните нестационарни процеси като този на възпламеняване на запресовката, изменението на температурата на газовете в затворения обем и др.

Основните фактори, определящи времето на действие на пиротехническото устройство на взривателя са скоростта на горене на пиротехническия състав (U) и геометричните размери на запресовката (h и S).

Скоростта на горене на пиротехническия състав се определя от технологични фактори, т.е. от процеса на производство на пиротехническия състав и процеса на производство на пиротехни-

ческото устройство. Такива фактори са качеството на суровините, дисперсността на компонентите, плътността на запресовката, точността на геометричните й размери. Скоростта на горене зависи и от вътрешни фактори, характеризиращи процеса на горене в конкретния взривател – вътрешни свободни обеми, херметичност, изменение на налягането в процеса на горене, тип на инициращия елемент (капсул-възпламенител или електровъзпламенител), температура и др.

Скоростта на горене зависи и от външни фактори – температура на околната среда, сили действащи на взривателя в процеса на експлоатация.

Най-голям интерес представлява анализът на влиянието на вътрешните фактори върху времето на действие на пиротехническото устройство.

Общият израз за определяне времето на горене на запресовка е

$$t = \int_0^H \frac{dh}{U} \qquad (1)$$

където: H - определящият размер на пиротехническата запресовка (височина в цилиндричния канал на втулката или дължината в пръстеновидния канал);

h – текущата координата на фронта на горене на запресовката;

U – геометрична скорост на горене на запресовката от пиротехническия състав.

В най-общия случай геометричната скорост на горене на запресовката U се определя от зависимостта

$$U = A + B\,.p^{\nu} \qquad (2)$$

Където A, B и ν са коефициентите, зависещи от свойствата на състава;

p – налягането в обема на взривателя.

За повечето малогазови състави използвани в съвременните взривители, коефициентът $\nu = 1$ и законът за горене имат вида:

$$U = A + B\,.p \qquad (3)$$

Значенията за коефициента на газообразуване и средните молекулярни маси са разчетени на базата на уравненията на екзотермичната реакция на разлагането на състава.

2. Сили действащи на взривателя

2.1. Сили, действащи върху детайлите на взривателя при изстрел

Основните сили действащи върху детайлите на взривателя при изстрел са следните:

А) Инерционни сили, възникващи при движение на артилерийски снаряд в канала на оръдието.

По време на движението на снаряда в канала на артилерийското оръдие върху детайлите на взривателя действат следните сили на инерция:

- осева сила – предизвикана от ускорението на постъпателното движение на снаряда;
- центробежна сила – предизвикана от въртенето на снаряда около ос;
- инерционна сила – възникваща от тангенционалното ускорение на снаряда поради нарастване на ъгловата му скорост;
- кориолисова сила на инерция.

Описаните по-горе сили на инерция действат върху детайлите на вривателя при движение на снаряда в канала на оръдието независимо от това, дали детайлът се движи или се намира в неподвижно състояние относно снаряда. При наличие на движение на детайл от взривателя спрямо

снаряда възниква още една сила – кориолисова сила на инерция. Тя се предизвиква от кориолисово ускорение на детайла.

2.2. Сили, действащи върху детайлите на взривателя по време на полет на снаряда

По време на полет на снаряда върху външните детайли на взривателя могат да действат две сили на реакция: сила, предизвикана от налягането на въздуха и сила на удара на тези детайли с дъждовни капки.

А) Сила на въздушния поток – при движение на снаряда във въздуха върху външните детайли на челния вривател освен атмосферното налягане действа и динамично. Това налягане се предизвиква при спирането на наблягащия въздушен поток от челната част на взривателя. Силата на реакция Q от действието на въздушния поток може да се използва за взвеждане на предпазителните механизми на различни по своето устройство челни взриватели – с турбинки, въздушни клапани, бутала и др. Тази сила може да оказва и временно въздействие, затруднявайки взвеждането на предпазителните механизми или да предизвиква преждевременно сработване на взведените ударни механизми. Силата Q е равна на:

$$Q = P\,д\,.\,F \tag{4}$$

където:

Рд - динамичното налягане на въздуха върху външната повърхност на детайла от взривателя;

F - проекцията на тази повърхност върху равнина, перпендикулярна на вектора на скоростта;

Налягането *Рд* се определеля като разлика между спиращото налягане *Pm* и статичното атмосферно налягане на въздуха *P0 :*

$$P\,д = Pm - P0 \tag{5}$$

Въздушният поток, обтичайки снаряда се разсича на множество струйки. Сред тези струйки има една среда, разграничителна струйка, приближаваща се към върха на снаряда по нормалата и при удар с него губи цялата си кинетична енергия.

Точката, в която скоростта на потока е равна на нула се нарича критична точка на нулевата скорост. Тя се намира на върха на челната част на снаряда или в ценъра на мембраната на взривателя. Налягането в тази точка се нарича спиращо налягане *Pm*.

При установен въздушеп поток зависимостта между *Pm* и скоростта на потока *V0* може да се намери чрез преобразуване на известното уравнение на Бернули:

$$Pm = P_0 \quad 1 + 0{,}2.\ \frac{V0}{a} \tag{6}$$

В случай, че потокът се движи със свръхзвукова скорост, формулата не може да се използва т.к. се нарушава непрекъснатостта на изменяне на налягането, плътността и температурата.

Б) Сили на реакция, действащи върху детайлите на челен взривател при среща с дъждовни капки – при движение на снаряд в зоната на валеж върху външните детайли на челния взривател действа сила на реакция, предизвикана от удара на дъждовните капки, снежинките или частици град. Това явление е прието да се разглежда като процес на мигновен удар в неподвижна мембрана на капка имаща скорост, която е равна на скоростта на движение на снаряда.

2.3. Сили, възникващи при движение на реактивен снаряд в активния участък от траекторията

При определяне на силите, действащи върху детайлите на взривателя при полет на реактивните снаряди, трябва да се имат предвид следните особености на тяхната вътрешна и външна балистика:

- при полет на реактивния снаряд се различават два основни участъка на траектория – активен и пасивен. В активния участък реактивният снаряд е подложен на въздействието на силата на тягата P, силата на съпротивление на въздуха *Rвъзд* и силата на земното притегляне *Mg*;
- в момента на пускане на направляващите реактивния снаряд има скорост на пускане равна на *Vg*. В края на активния участък от траекторията, снарядът придобива максимална скорост *Vmax*. Скоростта при пускане на направляващите е от порядъка на 10-150 m/s;
- при стрелба реактивните снаряди изпитват осеви ускорения, както на направляващите, така и в активния участък на траекторията. Тези осеви ускорения не са големи и това се обяснява от сравнително малките налягания в камерите на двигателя и относително голямото време на действие на двигателя в активния участък от траекторията. За противотанковите неуправляеми реактивни снаряди дължината на активния участък от траекторията е сравнително не голяма.

При движение на реактивния снаряд в активния участък от траекторията масата му M непрекъснато се изменя. Началната маса на реактивния снаряд се определя от зависимостта:

$$M0 = Mn + Mr \tag{7}$$

където:

M0 –начална маса на реактивния снаряд [kg];

M – променлива маса на реактивния снаряд [kg];

Mr – маса на горивото [kg];

Mn – пасивна маса на реактивния снаряд [kg].

Ако с *G* се означи масовия разход на гориво за 1 s то $\int_0^t Gdt$ представлява масата на горивото изгорено за време t. Тогава променливата маса на реактивния снаряд може да се определи от уравнението:

$$M = M0 - \int_0^t Gdt \tag{8}$$

Скоростта на горене и максималното налягане на газовете в камерата на двигателя на реактивния снаряд зависят от началната температура на заряда. Затова и силите, действащи върху детайлите на взривателя се изменят в зависимост от тази температура. Например в температурен диапазон от +50°C до -50°C тези сили се изменят два или повече пъти.

Приблизително може да се приеме средно, че при промяна на температурата на заряда с 1°C налягането в камерата на двигателя се променя с 1%.

Максималното налягане на барутните газове Pmt при определена температура t и при известно максимално налягане P m15 може да се изчисли по емпиричната формула:

$$Pmt = \frac{Pm15}{1-0.01\,(t-15)} \tag{9}$$

При движението на реактивен снаряд в активния участък от траекторията върху детайлите на взривателя действат следните сили:

За реактивни невъртящи се снаряди със стабилизатор:

- осева сила на инерция S предизвикана от линейното ускорение на снаряда.

За реактивни снаряди със стабилизатор и турбореактивни снаряди:

- осева сила на инерция S предизвикана от линейното ускорение на снаряда;

- центробежна сила на инерция С предизвикана от центростремителното ускорение на снаряда;
- инерционна сила Т възникваща от тангенционалното ускорение на снаряда;
- кориолисова сила на инерция К;
- сили на налягане върху външните детайли на взривателя;
- сили, възникващи в резултат на нутационно-прецесионното движение на снаряда.

2.4. Сили, действащи върху детайлите на взривателя при удар и проникване на снаряда в преграда

При удар на снаряда в преграда върху детайлите на взривателя действат сили на реакция и сили на инерция. Силата на инерция действаща върху детайл на взривателя, неподвижен относно снаряда в общ случай е равна на произведението на масата на детайла и абсолютното ускорение на тази точка от снаряда, в която се намира центърът на масата на детайла и е насочена в посока, обратна на посоката на ускорението. Специални изследвания за определяне силата на инерция S са извършени много малко. Съпротивлението на преградата обикновено е изучавано, за да се определи максималната дълбочина на проникване на снаряда или скоростта на удара, необходима за ефективното поразяване на целта. При праволинейно движение на недеформиращ се снаряд в преграда осевата инерционна сила може да се определи като произведение на осевото претоварване на снаряда и теглото на детайла от взривателя.

Ако силата R е известна, отрицателното ускорение J се определя като отношение между R и масата на снаряда M. Следователно силата на инерция S насочена по оста на снаряда се изразява с формулата:

$$R = m.\frac{R}{m} = \frac{R}{G}.P \qquad (10)$$

където:

P - теглото на детайла от взривателя;

G - теглото на снаряда;

При удар на снаряда във вода възникват сложни и малко изучени явления. Челната част на взривателя, потапяйки се във вода раздвижва водните слоеве с голяма скорост. За движение на водата се изразходва част от кинетичната енергия на снаряда, в следствие на което скоростта му на движение намалява. Намаляването на скоростта е незначително, но става за кратко и затова претоварването на снаряда може да е голямо.

В изложеното досега снарядът се разглеждаше като абсолютно твърдо тяло. В действителност всеки снаряд при среща с преграда изпитва едни или други деформации. Ако вътрешните напрежения в детайлите на снаряда не са големи, тези деформации са еластични.

Заключение

Появата на голямо разнообразие от боеприпаси довежда до разработването и производството на взривателите, които трябва да удовлетворят широк кръг тактико-технически изисквания. Наред с повишаване на изискванията към взривателите с ударно действие се появява необходимостта от висока точност и надеждност на действие на дистанционните взриватели, в резултат на което пиротехническите устройства в тях биват заменени с часовникови.

References

1. Петков Б**.,** *Артилерийски взиратели, теория и разчет.* София, 1994.
2. Прохоров, Б. А. *Артилерийски боеприпаси.* М., Машиностроене 1973.
3. Абрамович, Г.Н. *Приложна газодинамика.* С.,Техника, 1973.

POSSIBILITIES FOR REPLACEMENT OF THE THERMOSET PHENOLFORMALDEGYDE USED IN THE MANUFACTURE OF PRODUCTS FOR THE BULGARIAN ARMY WITH THERMOPLASTIC EQUIVALENTS

Blagovest I. Bankov

CIS faculty, National military inuversity "Vasil Levski", Shumen, Bulgaria,
blagovest.bankov@gmail.com

***Abstract**: The work presented a comparative analysis between thermoset PF and thermoplastic – PA, PC, PTTK, and PET polymers. The advantages in the characteristics of the polymers and methods of processing are laid out, focusing on the possibility to replace products made of thermoset with thermoplastic polymer, witch are entered in the Bulgaria army.*

***Keywords**: Thermoset (TS), Thermoplastic (TP), Phenolformaldegyde (PF), Polyamide (PA), Polycarbonate (PC), Polyetheretherketone (PEEK), Polyethyleneterephthalate (PET)*

ВЪЗМОЖНОСТИ ЗА ПОДМЯНА НА ТЕРМОРЕАКТИВНИЯ ФЕНОЛФОРМАЛДЕХИД, ИЗПОЛЗВАН В ИЗРАБОТВАНЕТО НА ИЗДЕЛИЯ ЗА БЪЛГАРСКАТА АРМИЯ, С ТЕРМОПЛАСТИЧНИ ЕКВИВАЛЕНТИ

Благовест И. Банков

Факултет „Артилерия, ПВО и КИС", Национален военен университет "Васил Левски",
Шумен, България, blagovest.bankov@gmail.com

***Резюме:** В настоящата работа е представен сравнителен анализ между термореактивния PF и термопластичните – PA, PC, PTTK и PET полимери. Изложени са предимствата в характеристиките на полимерите и методите за преработка, като се акцентира върху възможността да се заменят изделия изработени от термореактивен с термопластичен полимер, използвани в изделия за българската армия.*

***Ключови думи:** Термореактив (TS), Термопластик (TP), Фенолформалдехид (PF), Полиамид (PA), Поликарбонат (PC), Полиетеретеркетон (PEEK), Полиетилентерефталат (PET)*

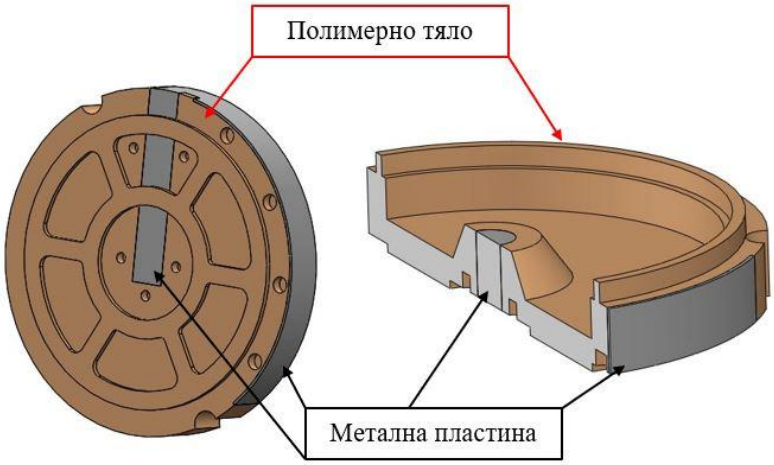
Увод

Използването на термореактивни полимери в оръжейните системи е често срещано поради техните свойства на топлоустойчивост и непреводимост на електричество. С изтичане позволения срок за съхранение и използване на боеприпаси, в които се срещат съставни детайли изработени от фенолформалдехидна смола (позната по-често под наименованието „бакелит"), е необходимо да се извърши тяхната утилизация. Поради самото естество на термореактивните смоли и тяхното омрежване при нагряване, значително се затруднява процеса по тяхната преработка и с

това се оскъпява цялостната процедура по управление на жизнения им цикъл. Тези затруднения от своя страна водят до изхвърлянето на тези изделия в депата за отпадъци или съхранението им в посочени от контролните органи места.

С напредването на полимерната индустрия се разкриват нови възможности за производство на тези компоненти от термопластични полимери, имащи сходни или превъзхождащи фенолформалдехидната смола качества, даващи шанс за значително по-лесна и евтина преработка. Част от термопластиците, които биха били използвани са –поликарбонат (PC), полиамид (PA) полиетеретеркетон (PEEK), полиетилентерефталат (PET) и др.

Едно често срещано изделие в българската армия, направено от фенолформалдехид и използвано в оръжейните боеприпаси е затварящата капачка в задната част на реактивния снаряд М-210Ф (122 mm снаряд за БМ21), която има контактен метален пръстен (фиг. 1).



Фигура 16: Затварящa капачка на реактивен снаряд М-210Ф.

Цел на разработката

Целта на настоящата работа е да бъдат разгледани част от възможните термопластични материали, които да заменят частта от термореактивния полимер на затварящa капачка за реактивен снаряд М-210Ф, като бъдат съпоставени механичните, термични и химички свойства на материалите, както и производствените технологии за изработка и преработка.

Изложение

1. Материални характеристики

В табл. 1 са представени различните свойства на материалите: фенолформалдехид (PF), поликарбонат (PC), полиетеретеркетон (PEEK), полиамид (PA) и полиетилентерефталат (PET).

Таблица 3: Свойства на разглежданите полимери.

Вид		Температурен диапазон на топене (°C)	UV Устойчивост	Якост на опън (MPa)	Свиване (%)	Удължение при скъсване (%)
Термопластик	PA	230-290	Добра	50-95	0,5 - 1,5	200 - 300
	PEEK	350-390	Отлична	90-120	1,2 - 1,5	30 - 150
	PC	280-320	Добра	55-77	0,7 - 1	50 - 120
	PET	260-280	Добра	45-70	0,2 - 3	30 - 70
Термореактив	PF	***	Отлична	22 - 48	0,3 - 0,45	0,2 - 0,6

От данните в табл. 1 се вижда, че съпоставените термопластици имат преимущества в якостта на опън и еластичността. Термопластичните полимери са с по-висок процент свиване,

който може да бъде избегнат с модифициране дизайна на изделието и проектиране на стени с максимално еднакви дебелини.

2. Технологии за изработка на изделия

2.1. Леене под налягане

Леенето под налягане е основен метод за производството на пластмасови изделия. Той е един от най-бързите процеси за масово производство на идентични елементи от високоточни инженерни компоненти до потребителски стоки за еднократна употреба. Той се характеризира с инжектиране под високо налягане на стопилка във формообразуващ инструмент и има няколко етапа, като най-времепоглъщащ е този на охлаждане [1] (Фигура 17).

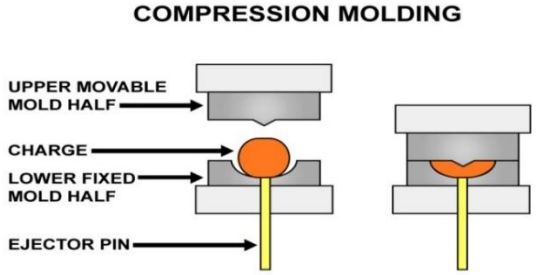
Фигура 17: Етапи на шприцването. [1]

И двата вида пластмаси се използват за леене под налягане. Основната разлика е в температурата на инструмента по време на процеса. За термопластичните стените на шприцформата са по-студени от самата стопилка, докато при термореактивните стените на инструмента са по-горещи от самия материал

Това от своя страна води до по-висок разход на енергия поради това, че металната форма има много по-ниска топлопроводимост от полимера. Въпреки това термореактивните полимери изискват по-ниско налягане на инжектиране спрямо термопластичните.

2.2. Компресионно формоване

Този метод се характеризира с това, че предварително се залага полимерен материал (термопластик или термореактив) във формообразуващия инструмент, който е предварително загрят и чрез прилагане на компресираща сила върху заготовката ѝ се предава формата на инструмента (Фигура 18).



Фигура 18: Компресионно формоване. [8]

При формоване с термореактивна смола е необходимо инструмента да е с по-високи градуси спрямо материала, поради необходимостта от втвърдяване на термореактива, което допринася за по-високите енергийни разходи при производство.

3. Методи за преработка на материалите

3.1. Методи за преработка на термореактиви

В днешно време се изследват възможностите да се преработват изделията с термореактивна структура поради рестрикции от различни правителства, и комисии. Една такава алтернатива за преработката им е изгарянето им под висока температура (450 – 500 °C), но и този подход генерира твърди остатъци, които биха могли да бъдат вложени в нови изделия с понижени качествени показатели. [5]

Друг способ е чрез термохимичния процес пиролиза, който представлява термично разлагане и изпаряване на молекули с по-ниско тегло в инертна атмосфера (наперим азот). В този процес термореактива се разлага на по-ниско молекулно ниво и в зависимост от температурата (най-често процеса варира от 550 до 700 °C от вида полимерната матрица) се превръщат във вид на газове като въглероден оксид и въглероден диоксид, водород и метан. Също така в процеса се получава и маслена фракция, която полепва по стените на съда за обработка.

Един от големите минуси на този метод е отделянето на въглеродния диоксид, който е основен причинител за климатичните промени. Поради тази причина има много регулатори за следене на тези и други парникови газове, както и редица споразумения между държавите, ограничаващи прекомерното отделяне на замърсяващи околната среда аерозоли.

Солволизата е трети способ за преработка. Тя се състои в химическо обработване на материала с различни разтворители. Основното предимство на солволизата в сравнение с пиролизата е по-ниската температура, необходима за разграждане на полимерната матрица.

Едни от разтворителите, които разграждат добре термореактивните полимери са пропанол или азотна киселина. [5]

При използването на концентрирана азотна киселина, фенолът се окислява интензивно, което води до дълбоко разрушаване на неговите молекули.

3.2. Методи за преработка на термопластици

Механично рециклиране, първоначално материала се натрошава чрез шредери на малки части, след което може повторно да се разтопи и вложи в нови продукти, но с по-ниско качество поради намалените свойства на преработения полимер.

Химична преработка, той включва разграждане на отпадъчни полимери до мономери или други продукти като мазут и газ. Някои от тези преработки включват процеси като – хидрогенериране, гликолиза, хидролиза, пиролиза, метанолиза, химическа деполимеризация, термичен крекинг, фоторазграждане и др.

Химическото рециклиране не е напълно развито и при термопластиците поради високите инвестиции и необходимостта от експертен персонал. [2]

Често използван способ е чрез изгаряне на отпадъчните полимери и производство на енергия, но не е екологично приемлив поради риска за здравето от токсични вещества във въздуха. [3]

Заключение

Термопластичните полимери могат да бъдат значително по-евтино преработени, чрез метода на механичното рециклиране, спрямо термореактивите.

Възможността от изгаряне и произвеждане на енергия дава широк потенциал за преработка на всички термопластици и благоприятства проучването на способи за ограничаване на вредните газове, произлизащи от горенето им.

Поради необходимостта на термореактивните полимери да се задържат във формообразуващи инструменти до втвърдяването им и последващо отнемане на температурата от инструмента за изваждане на изделието се увеличава времето на производство, и с това притежателната стойност на продукта, поради увеличените разходи за енергия и по-малко изработени бройки за 24 часа.

Друго предимство на термопластиците е възможността от изгарянето им при стартиране на реактивния двигател на боеприпаса (М-210Ф), което намаля възможността от нараняване от фрагменти при счупване на затварящата капачка.

Термопластиците позволяват да се изработят изделия с по-тънки стени без да се наруши функционалността им, което отново благоприятства за по-ниския разход на материал и енергия за изработа, и преработка.

Не на последно място, новите стратегии на правителства, комисии, неправителствени организации, учени и др., са насочени към замяната на термореактивните полимери с алтернативни термопластични поради по-благоприятната възможност за преработка.

References

1. Г. Тодоров, Ц. Караянчева, Т. Тодоров, Б. Романов. (2017). Възможности за моделиране на конформна охладителна система на шприцформи, изградени с адитивна технология. *Машиностроене и електротехника*, 10-11

2. M. Grigore. (2017). Methods of Recycling, Properties and Applications of Recycled Thermoplastic Polymers. *Journal Recycling*, 2(4), 24. https://www.mdpi.com/2313-4321/2/4/24

3. T. Azeez. (2020). Thermoplastic Recycling: Properties, Modifications, and Application. https://www.intechopen.com/chapters/68596

4. Y. Huang, B. Fei, R. Zhao. (2014). Ivnestigation of low-molecular phenol formaldehyde distribution in tracheid cell walls of Chinese fir wood. *BioRes*, 9(3), 4150-4158

5. Sh. Utekar, K. Suriya, N. More, A. Rao. (2021). Comprehensive study of recycling of thermosetting polymer composites – Driving force, challenges and methods. *Composite Part B*, 207(108596)

6. Zheng, R., Tanner, R., Fan, X. Injection Molding : Integration of Theory and Modeling Methods. Berlin: Springer-Verlag , 2011, с. 4. ISBN 978-3-642-21263-5

7. Elongation at Break. (2022). Omnexus. https://omnexus.specialchem.com/polymer-properties/properties/elongation-at-break

8. Moldex3D Help. (2021). *Compression Molding.* https://www.moldex3d.com/products/software/moldex3d/solution-add-on/compression-molding/

9. Plastic Melting Temperature Chart: what's the Melting Point of Different Plastic Materials. (2020). https://www.rydtooling.com/plastic-melting-temperature-chart/

10. Phenol formaldehyde. (2022). Designerdata. https://designerdata.nl/materials/plastics/thermosets/phenol-formaldehyde?cookie=YES

11. Phenilic – PF Phenol Formaldehyde Foam. (2021). Azo Materials. https://www.azom.com/article.aspx?ArticleID=728

12. UV Light Resistance. (2022). Omnexus. https://omnexus.specialchem.com/polymer-properties/properties/uv-light-resistance#PA-PC

13. Strength at Break. (2022). Omnexus. https://omnexus.specialchem.com/polymer-properties/properties/strength-at-break-tensile

14. Shrinkage. (2022). Omnexus. https://omnexus.specialchem.com/polymer-properties/properties/shrinkage

A STUDY OF THE VARIATION OF THE COORDINATES OF THE MIDPOINT OF HITS WHEN FIRING BULLETS WITH RADIAL GROOVES ON THE OGIVE

Krasimir G. Kalev, Rosen N. Lazarov, Miroslav St. Rashkov

Faculty of Artillery, AD and CIS, National military university Vasil Levski, Shumen, kraskalev@abv.bg; poceh_69@abv.bg

Abstract: *Reducing the ricochet effect of the bullet of an existing ammunition by changing the shape of its ogive, leads to changes in its external ballistic qualities (range and grouping of hits).*

Keywords: *ballistics, external ballistic, bullet shape*

ИЗСЛЕДВАНЕ НА ИЗМЕНЕНИЕТО НА КООРДИНАТИТЕ НА СРЕДНАТА ТОЧКА НА ПОПАДЕНИЯТА ПРИ СТРЕЛБА С КУРШУМИ С РАДИАЛНИ ИЗРЕЗИ ВЪРХУ ОЖИВАЛНАТА ЧАСТ

Красимир Г. Калев, Росен Н Лазаров, Мирослав Ст. Рашков

Факултет „Артилерия, ПВО и КИС" на Национален военен университет „Васил Левски", гр. Шумен, kraskalev@abv.bg; poceh_69@abv.bg

1. ВЪВЕДЕНИЕ

При изпълнение на бойни задачи в близост до водни обекти е възможно възникването на нежелани рикошети при среща на куршума с водната среда, които биха могли да доведат до наранявания на близко намиращи се хора (свои военнослужещи или цивилни лица).

Съществуват разработени двусрединни куршуми за стрелба от водна към въздушна среда и от въздушна към водна среда, които имат увеличена далекобойност във водна среда, но същите притежават занижени външнобалистични параметри (далекобойност и групираност на попаденията). При тях се наблюдава и намалено рикошетно действие на куршума от водната среда.

С цел ограничаване на рикошетите от водната среда един от подходите е да се преработи челната част на куршума на съществуващ боеприпас чрез изработване на радиални канали върху челната му част на определено отстояние от върха на куршума, като при това се запазят в максимална степен външнобалистичните параметри. [6]

Параметрите на куршума, които оказват влияние на полета му са:

- калибър (d) – оказва влияние върху челното съпротивление (c_x), коефициента на формата на куршума (i) и балистическия коефициент (BC_i);
- маса (m) – влияе върху инерцията на куршума, върху балистичния коефициент и върху действието на куршума в целта;
- начална скорост на куршума (v_0) – определя скоростта на куршума по време на полета по траекторията в зависимост от балистическия коефициент на модела;

- форма на куршума – определя коефициента на формата i. Оказва пряко влияние върху скоростта на движение на куршума чрез зависимостта си от въздушното съпротивление.

За определяне на групираността на стрелбата и оценка на изработените образци куршуми е приложена теорията на математическата статистика [5].

2. ИЗЧИСЛЯВАНЕ НА НЕОБХОДИМИЯ МИНИМАЛЕН БРОЙ НАБЛЮДЕНИЯ

Необходимият минимален брой опитни данни, който трябва да имат групите се определя, използвайки зависимостта [3], [4].

$$b = \frac{S^2 . U_{\frac{\alpha}{2}}^2}{\varepsilon^2}, \quad (1)$$

където:

b – брой на опитните данни;

S – средно квадратично отклонение на данните от извадката;

$U_{\frac{\alpha}{2}}$ = 3,0902 – квантил на нормалното разпределение при доверителен интервал 99,9%

ε – точност на оценката на математическото очакване.

Средноквадратичното отклонение на данните от извадката се изчислява посредством формулата [2], [3], [4]:

$$S = \sqrt{\frac{1}{b-1} \sum_{i=1}^{b} x_i - x^{\,2}} \quad (2)$$

където:

S – средно квадратично отклонение на данните от извадката;

b – брой на опитните данни;

x_i – стойност на данните от i-тите изчисления

x – средноаритметично на данните.

Точност на оценката се изчислява по формулата [3], [4]:

$$\varepsilon = t_{\frac{\alpha}{2}} \frac{S}{\sqrt{b}}, \quad (3)$$

където

ε – точност на оценката на математическото очакване;

$t_{\frac{\alpha}{2}}$ =3,8834 – квантил на нормалното разпределение на Стюдънт при доверителен интервал 99,9%;

S – средно квадратично отклонение на данните от извадката;

b – брой на опитните данни.

След извършване на изчисленията, за минимален брой опитни данни получихме b=12,665. Избраните брой изстрели в сериите е 20 патрона за модел за серия, което удовлетворява необходимия минимален брой опитни данни.

3. ОПИТНА ПОСТАНОВКА НА ПЛАНИРАНИЯ ЕКСПЕРИМЕНТ

Експериментът се провежда със стандартен куршум и с пет модела изработени от куршум на боеприпас с номенклатурен номер 7,62х54 мм, на който са изработени радиални канали по оживалната част, както следва:

- Модел 1: с един канал, разположен на 3 мм от върха на куршума;
- Модел 2: с два канала, разположени на 3 мм и на 6,4 мм от върха на куршума;
- Модел 3: с един канал, разположен на 6,4 мм от върха на куршума;
- Модел 4: с един канал, разположен на 12,7 мм от върха на куршума;
- Модел 5: с два канала, разположени на 3 мм и на 12,7 мм от върха на куршума.

При провеждане на експеримента групираността се определя на стандартно приетото от наставлението по стрелково дело за 7,62 мм ПК разстояние за проверка боя на стрелковото оръжие – 100 m. Стрелбата се провежда с балистична цев, монтирана неподвижно на станок „Баринов".

Съгласно Методика за полигонни изпитвания се определя групираността на 100 м от дулния срез за използваните боеприпаси и използваната балистична цев чрез произвеждането на 20 изстрела с всеки модел куршуми.

- произвеждат се по една серия от по 20 изстрела на единичен огън първо с фабрични боеприпаси, а после и за всяка подготвена група с различни куршуми;
- измерва се началната скорост на всеки един куршум;
- след изстрелване на всяка група патрони се измерват величините на отклонението на центровете на пробойните на всеки куршум в мишената от координатните оси, преминаващи през контролната точка. Измерването се извършва в милиметри. Стойностите на страничните отклонения вляво от точката се нанасят в бланката със знак минус, а вдясно – със знак плюс. Стойностите на вертикалните попадения под хоризонталната линия на точката се нанасят в бланката със знак минус, а над нея – със знак плюс;
- определя се групираността за всяка серия поотделно. Измерват се стойностите на разстоянията между центровете на пробойните в хоризонталната и вертикалната равнини на двете най-отдалечени попадения в милиметри посредством линия. За стойност на групирането се приема по-голямата стойност от измерванията.

За оценяване стойността на групираността на стрелковото оръжие е прието същата да се разглежда, като кръг с диаметър – D_{100}, в който попадат 100 % от попаденията. С цел по-прецизно изследване на изменението на групираността, тя се разглежда, не като кръг, а като елипса на разсейване, която се състои от голяма и малка ос (фигура 2.10). За стойности на диаметъра на кръга на групираността (D_{100}) се приема стойността на по-голямата от двете оси.

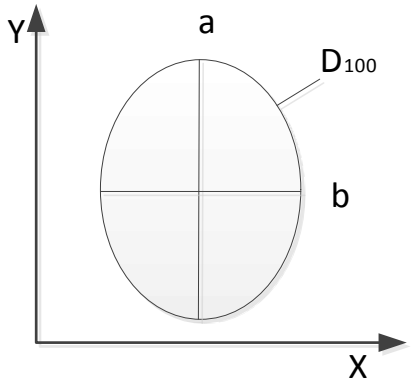
Необходимо е да се изчисли стойността на разстоянието между координатите на точките на попаденията. Това може да се постигне посредством формулите:

- за вертикалната равнина:

$$\Delta Y = Y_{max} - Y_{min} \quad mm \tag{4}$$

- за хоризонталната равнина:

$$\Delta X = X_{max} - X_{min} \quad mm \tag{5}$$



a – голяма ос на елипсата;

b – малка ос на елипсата.

D_{100} – диаметър на групираността.

Фиг. 1. Елипса на разсейване.

За определяне на стойностите на голямата и малката ос на елипсата на разсейването е необходимо да се проведат експериментални стрелби, при които ще се получат техните стойности за използвания модел куршуми. [7]

Таблица 1

№ по ред	Вид на куршумите в серията	ΔX	ΔY
1.	Модел 0	96	104
2.	Модел 1	93	196
3.	Модел 2	101	152
4.	Модел 3	124	145
5.	Модел 4	128	174
6.	Модел 5	105	130

След определяне на стойностите на голямата и малката ос на елипсата на разсейването, използвайки формули 4 и 5, се определя стойността на диаметъра на групираността (D_{100}). За стойности на диаметъра на групираността се приема стойността на по-голямата от двете оси.

Резултатите от извършените изчисления, съгласно формули (4 и 5) са представени в табл. 1.

4. РЕЗУЛТАТИ ОТ ПРОВЕДЕНИЯ ЕКСПЕРИМЕНТ

Произвеждат се двайсет изстрела за всеки модел куршуми. Пресмята се центърът на тежестта (средна точка на попаденията) по изразите:

(6) $$y_m = \sum_{i=1}^{n} \frac{y_i}{n}$$

(7) $$x_m = \sum_{i=1}^{n} \frac{x_i}{n}$$, [1]

където: y_i и x_i са хоризонталните и вертикални отклонения от средната точка на попаденията.

Измерените координати на попаденията на куршумите по мишенните листи след провеждане на изпитанието на групираност, максималното отклонение на координатите по X и Y за всяка една серия и средната стойност на отклонението са показани в табл. 2.

Таблица 2

№ по ред	**Щатни**		**Модел 1**		**Модел 2**		**Модел 3**		**Модел 4**		**Модел 5**	
	X	Y	X	Y	X	Y	X	Y	X	Y	X	Y
1	0	0	0	170	0	277	0	0	0	263	0	18
2	42	68	24	125	0	170	72	93	65	0	0	70
3	68	41	23	68	20	117	104	30	81	198	12	46
4	77	120	93	44	43	6	107	48	89	257	52	74
5	95	19	102	46	37	147	147	99	98	297	100	83
6	97	110	109	105	55	223	170	170	128	298	120	0
7	103	129	113	186	55	227	223	248	128	223	131	69
8	105	150	121	77	84	294	208	120	160	75	122	124
9	115	187	119	0	97	225	220	0	165	170	126	122
10	125	165	144	113	88	150	245	112	157	206	130	122
11	141	128	164	88	113	201	265	38	135	285	142	135
12	135	60	206	263	117	230	270	39	143	310	131	210
13	143	65	209	177	142	160	275	0	150	347	190	156
14	157	50	235	68	135	285	278	74	168	310	177	107
15	170	0	245	100	133	310	283	123	167	236	198	97

№ по ред	**Щатни**		**Модел 1**		**Модел 2**		**Модел 3**		**Модел 4**		**Модел 5**	
16	164	68	260	19	157	308	290	55	210	203	206	94
17	185	208	280	20	182	297			217	241	208	113
18	178	85	286	155	167	208			236	263	243	110
19	182	53	328	115	202	186			255	250	260	69
20	195	58	392	152	195	172					133	128
Максимално отклонение [mm]	195	208	392	186	202	310	290	248	255	347	260	210
Средна стойност на отклонението [mm]	123,8	88,2	172,6	104,5	101,1	209,6	197,3	78,1	144,8	233,3	134,1	97,4

5. ИЗВОДИ

Резултатите от проведените експериментални стрелби показват, че изработените радиални пръстени по оживалната част на куршума на боеприпас с номенклатурен индекс 7,62x54 мм оказват влияние върху групираността на попаденията при стрелба във въздушна среда. Групираността на стрелбата при куршум с изработен един пръстен на оживалната част е с по-големи отклонения в сравнение с куршум с изработени два канала по оживалната част. Куршумите с пръстени, разположени на по-голямо разстояние от върха осигуряват групираност с по-малки отклонения в сравнение с куршумите с радиален канал, изработен по-близо до върха на куршума.

Най-малко отклонение на групираността на попаденията по двете оси на елипсата на разсейването в сравнение с куршума на щатния боеприпас дава опитният образец, който е изработен с два канала по оживалната част, съответно на разстояние 3 мм и 12,7 мм от върха на куршума.

References

1. Давидов К. С., Цонев Ц. Г., Маринов М. Г., “Минимизиране на вероятността от появата на нежелан рикошет при стрелба към водна повърхност”., НВУ „В. Левски“ Факултет “Артилерия, ПВО и КИС Научна сесия 2012. Сборник научни трудове – част I., Ш., 2013 (110 – 117 стр.) ISSN 1313-7433.
2. Dimitrova Ya., Evaluation of hit’s grouping deviation due to tribological processes in bullet-rubber chopper wheel interaction, Сборник доклади от International scientific conference CONFSEC, Borovec 2018, year 2, issue 2(4), c. 217-220, ISSN (print) 2603-2945, ISSN (online) 2603-2953
3. Вълчев Хр., Йорданова П., Статистика, Шумен: Университетско издателство "Епископ Константин Преславски", 2004.
4. Дронов С. В., Многомерны статистический анализ. Учебное пособие. Барнаул, 2003.
5. Калев Кр., Топалов В. Статистически модел на износването в началната част на цевта на автоматична стрелкова система. VII Международна научна конф. „Научните изследвания-ключова роля в модернизацията на въоръжението, техниката и системите“ Хемус, Пловдив, 2014.
6. МО, Външна балистика, Държавно военно издателство, 1953 г.
7. Ванко Ганев, Росен Лазаров, Експериментално изследване на влиянието на формата на куршума върху рикошетното му действие при среща с водна повърхност, Сборник доклади от научна конференция „Логистиката и обществените системи“, Велико Търново 2021 г. Стр. 175-181, ISSN 2738-8042

URBANIZED ENVIRONMENT – DEFINITION AND TAXONOMY

Radoslav B. Ghalakov

Rakovski National Defence College", Faculty " Command-staben", Department "Land forces"
r.chalakov@rndc.bg,

Abstract: *Analyzing urban areas, it can be assumed that they are in "constant motion". The dynamic cycle in the urbanized environment varies with peak hours and the time of day where the planning of operations and the use of artillery fire in urban settings will need to be considered and impose constraints influenced by both the rhythm of the population and the movement of vehicles and people in the urban environment.*

УРБАНИЗИРАНА СРЕДА – ДЕФИНИЦИЯ И ТАКСОНОМИЯ

Радослав Б. Чалъков

Военна академия "Георги С. Раковски", факултет „Командно – щабен", Катедра "Сухопътни войски"
r.chalakov@rndc.bg

Чрез разбиране на ключови аспекти на оперативната среда от гледна точка на системата, командира и планиращият елемент могат след това да избират начини за постигане на оперативни цели.

Joint Publication 3-06

Урбанизацията е дългосрочен процес, който се характеризира както с увеличаване на населението, което живее в градовете, така и с разширяване на градските зони. В Европа процесът на урбанизация започва в началото на 18 век с началото на индустриалната еволюция и за два века се разширява хетерогенно върху целия континент.[1]

Урбанизираната среда (Градски район) представлява сложна среда за военните операции. Тази сложност произтича от много фактори като местоположение, история, икономическо развитие, климат, естествен терен, култура и други фактори.[2] Това разнообразие съществува не само сред градските райони, но и в рамките на всеки отделен квартал. В постоянно променящото се разнообразие от естествени и изкуствени характерни черти на градските райони, специфичната среда може да се приеме като - *Средата, която е съвкупността от фактори, определени от физикогеографските особености, инфраструктурата, психологическия климат и действията на*

[1] *Тълковен речник по териториално развитие (CEMAT)*
2 JP 3-06, Joint Urban Operations

противостоящите сили (ПС), които в обусловената си обвързаност налагат провеждане на допълнителни мероприятия при планирането, организирането и провеждането на тактическите действия.

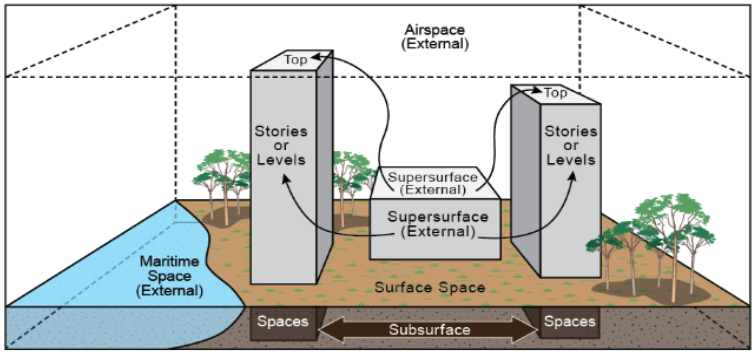
Според размера и плътността на урбанизираната среда се определя и броят на населението, с това и може да определят и видовете населените пунктове:

На национално нив о[i]	Документи на съюзнически армии.[ii]
много малки - до 5 000 жители	Село 3000 или по-малко.
малки - от 5 000 до 20 000 жители	Град (Town) над 3000 до 100000
средни - от 20 000 до 100 000 жители	Град (City) над 100000 до 1 000 000.
големи - от 100 000 до 500 000 жители	Метрополис над 1 000 000 до10 000 000.
много големи - с повече от 500 000 жители.	Мегаполис над1 000 000

Урбанизираната среда сблъсква командирите с комбинация от трудности, който рядко се срещат на друго място. Отличителните й характеристики са резултат от сложна топография и висока гъстота на населението. Сложността на топографията произтича от създадените от човека характеристики (конструкции, обекти, сгради и др) и прилежаща инфраструктура. Дали е голям град или малко село, всяка среда има разграничима система от компоненти, които постоянно се променят и си взаимодействат. Тази „система от системи" се състои от терен, общество и инфраструктура. Тези системи не са разделени в различни категории, а по-скоро са припокриващи се, взаимодопълващи, взаимосвързани и взаимозависими. Анализът на тези елементи, заедно с други фактори като мисия, ПС, метеорология, налични сили и средства, време, граждански съображения и др., допринася за по-пълно разбиране на обстановката от командирите и използването на артиелрийските формирования.

Урбанизиранят терен е най-разпознаваемият аспект на градската зона. Истинското му разбиране, изисква разбиране на многостранния характер на градския терен. Теренът се състои от естествени и изкуствени характеристики, сгради, улици подземни зони и други инфраструктурни обекти, който имат разнообразни модели, форми и размери. Безкрайни са начините, по които тези фактори могат да се преплитат и е трудно да се опише „*типичната"* градска зона. Въпреки това, тези елементи осигуряват рамка за разбирането на сложния релеф в градска зона. Освен това, изкуствените характерни черти на градските зони оказват съществено влияние върху тактиките и техниките използвани в операциите.

Урбанизираният терен обхваща морско пространство, въздушно пространство и повърхност, и то по отношение на тяхната дълбочина, ширина и височина. Това, което може да се отчете като особеност на урбанизираната среда, е че тя обхваща и подземните зони (вж. фиг. 1).



Фигура 1. Теренен анализ на градска среда (ATP 2-01-3)

Морското пространство – осигурява ключови пътища (приятелски и враждебни) за подход или основни комуникационни линии за градските зони, които граничат с този вид пространство.

Анализите показват, че през последното десетилетие повече от 80% от населението в световен мащаб живее в рамките на до 100 километра в близост до водни басейни, докато приблизително 75% от големите градове са до бреговата ивица. Възможността за предотвратяване на достъп и отказ до морското зона е фактор при планиране и провеждане на операции предприети в урбанизирана среда.

Въздушното пространство – използването на въздушното пространство е път за бързо приближаване към урбанизираната среда. Част от повърхностните препятствия в градски условия не влияят на полета на въздухоплавателните средства, но могат да попречат на излитането и кацането им. Различната височина на сградите и плътността им, както и други конструкции от градският терен влияят на полета и траекторията на боеприпасите, чрез ограничена видимост и физически ограничения на маневреността на малка височина в градското въздушно пространство.

Повърхностните площи – отнасят се за външни и надземни зони, осигуряващи основни пътища за подход и бързо предвижване. Липсата на открити пространства допълнително затруднява разполагането и използването на средствата за огнева поддръжка.

Подземните зони – включва вътрешно-повърхностни зони. Подземната зона може да се използва, като коридор за придвижване или линии на комуникация отсъстващи в други специфични среди. Подземните и вътрешни пространства в сградите са допълнителни предизвикателства на урбанизираният терен, което рефлектирайки върху дейността за събиране на разузнавателни данни.

Преди извършването на операции в урбанизирана среда е изключително важно да се разбере терена, където голяма част от трудностите и объркването с планирането и провеждането на операции в урбанизирана среда са резултат от основна липса на разбиране на общите характеристики на градския терен. Характеристиките в урбанизираната среда трябва да бъдат определени или поне достатъчно добре описани, за да се даде възможност за планиране. Плътността на строителството и населението, уличните модели, разделянето на секциите, богатите и бедните участъци, модернизацията и присъствието на полезните системи характеризират всички градове по света. Разликите в градските райони са по размер, ниво на развитие и стил.

Структурата на градската територия е в зависимост от характера на планировката и застрояването на участъците. По своята структура обикновено големите градове се делят на: административна (делова) част, намираща се обикновено в центъра на града;жилищни райони; индустриална зона; територия, заета от транспортни обекти (железопътни, морски, речни гари и летища); складови територии; незастроени територии; зони от трайни насаждения (паркове, защитни пояси), санитарно защитени зони (вододайни зони) и прилежащите предградия.[iii]

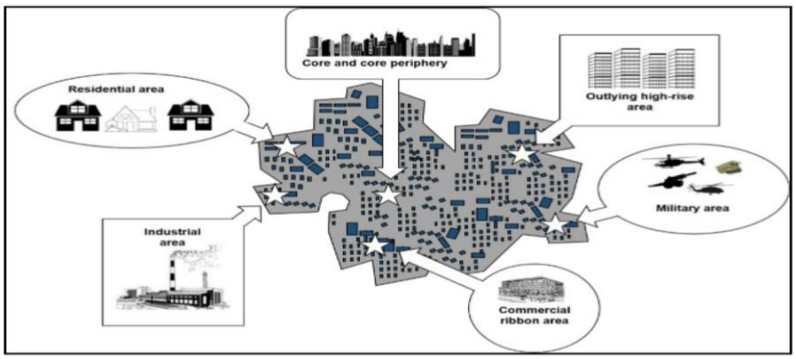
Планировката на населения пункт зависи главно от разположението на улиците и кварталите в него. Те могат да бъдат регулярни, нерегулярни и смесени. Регулярните планировки биват правоъгълна, радиално-кръгова и комбинирана.[iv]

Урбанизирано общество. Въпреки сложния за разбиране градски терен, той е сравнително ясен, в сравнение с разбирането на многостранния характер на градското общество. Операциите в градска среда, често изискват да се работи в непосредствена близост до местното население. Дори в евакуирани райони може да има население до десетки хиляди. Потребностите на цивилното население, неговите нагласи и действия могат да повлияят в различна степен на операциите провеждани в урбанизирана среда.

Урбанизирана инфраструктура. Инфраструктурата е тази система, която поддържа жителите на населените райони и тяхната икономика. Тя свързва физическия терен и градското общество.

Контролирането, унищожаването или защитата на жизненоважни части от инфраструктурата могат да изолират потенциални източници на заплаха, но и на подкрепа. Това важи особено, когато основните съоръжения от инфраструктурата са физически разположени в близост до района на зоната на операцията. Градската инфраструктура включва сгради, мостове, пътища, ле-

тища, пристанища, подлези, канализации, електроцентрали, индустриални сектори и др. подобни физически структури. В развитите страни, секторите на инфраструктурата и услугите са много сложни и добре интегрирани. В част от градове може да липсва дори основна инфраструктура. За да бъде по-добре обяснено как инфраструктурата на един град подкрепя населението, трябва тя да се разглежда като система от системи. Всеки компонент засяга населението, нормалната експлоатация на града и потенциалния дългосрочен успех на военните операции, провеждани там.



Фигура 2 Визуализация на градската инфраструктура (ATP 3-06 Urban Operations.)[v]

Исторически термин *„инфраструктура"* се появява във военната наука, като с него се обозначава териториалната организация на системата за поддържане и действие на въоръжените сили. През 40 – те години на XX-ти век, терминът е заимстван от икономистите и започва да се употребява широко и в най–разнообразен смисъл. НАТО разглежда инфраструктурата като *„система от стационарни обекти и отделни съоръжения на територията на една или няколко страни или района на операцията, които се явяват основа за развръщане на ВС и воденето на военни действия".*

По този начин инфраструктурата следва да се разглежда в три множества: функционално, структурно и съдържателно и се определя като: *„Съвкупност, система от отрасли и материални средства, които обслужват производството и осигуряват условия за функциониране на обществото – като пътища, съобщения, наука, образование, защитата и др"*[vi]

Важността на различните видове инфраструктурни обекти не се поражда само от факта, че тези елементи могат да се определят като ограничение, препятствие или да бъдат полезни за целите на операцията, при въздействие върху тях те могат да се превърнат от елементи създадени за подобряване на условията за живот в елементи за заплаха за него. Именно това ги превръща и в цел на атаки в повечето случаи, поради голямото им социално и икономическо или екологично значение. Евентуален пробив в тяхната сигурност и защита могат сериозно да застрашат здравето на личния състав и населението, околната среда, икономиката, дори и глобалната сигурност. Възможно е при пробив на инфраструктурни обекти на тактическо ниво, ефекта да се превърне в стратегически, да промени обществените нагласи, хода на операцията и т.н.

За обекти в цивилните и военните среди е възприето още едно понятие свързано с инфраструктурата – *критична инфраструктура*. Юридическият термин „*критична инфраструктура*" е приет в българското законодателство през 2005 г. с приемане на Закона за управление при кризи. Терминът е дефиниран като система от съоръжения, услуги и информационни системи, чието спиране, неизправно функциониране или разрушаване би имало негативно въздействие върху здравето и безопасността на населението, околната среда, националното стопанство или върху ефективното функциониране на държавното управление.

Таблица 1

ПАРАМЕТРИ НА ПОСТРОЙКИТЕ В РАЗЛИЧНИ ТОЧКИ В СВЕТА

СРЕДНА ДЕБЕЛИНА НА СТЕНИТЕ, (mm)

№	Територия за провеждане на операции	Материал за изра-ботване на стените	Части от града			
			Стар град централна част	Нов град квартали	Предградия в градовете	Пром. зони
малки градове по-малки от 50 000- жители и площ 15 км^2						
1	Близкият изток	тухлени	300 - 350	400 - 500	400 - 500	400 - 800
		каменни	500 - 600	500 - 600	500 - 600	600
		железобетонни	400 - 600	400 - 500	400 - 500	400 - 800
		смесени	400 - 600	500 - 600	500 - 600	600
2	Азия	тухлени	300 - 350	500 - 600	400 - 500	400 - 800
		каменни	600 - 800	500 - 600	500 - 600	800
		железобетонни;	400 - 600	400 - 500	400 - 500	400 - 800
		смесени	400 - 600	500 - 600	500 - 600	800
3	Европа	тухлени	400 - 550	400 - 500	500 - 800	600- 800
		каменни	600 - 800	500 - 700	600 - 800	800
		железобетонни;	400 - 600	400 - 600	600 - 800	600 - 800
		смесени	400 - 600	500 - 600	500 - 600	800
средни градове до 100 000 жители и площ 15 - 25 км^2						
1	Близкият изток	тухлени	300 - 350	400 - 500	400 - 500	400 - 800
		каменни	500 - 600	500 - 600	500 - 600	600
		железобетонни;	400 - 600	400 - 500	400 - 500	400 - 800
		смесени	400 - 600	500 - 600	500 - 600	600
2	Азия	тухлени	300 - 350	500 - 600	400 - 500	400 - 800
		каменни	600 - 800	500 - 600	500 - 600	800
		железобетонни;	400 - 600	400 - 500	400 - 500	400 - 800
		смесени	400 - 600	500 - 600	500 - 600	800
3	Европа	тухлени	400 - 550	400 - 500	500 - 800	600 - 800
		каменни	600 - 800	500 - 700	600 - 800	800
		железобетонни;	400 - 600	400 - 600	600 - 800	600 - 800
		смесени	400 - 600	500 - 600	500 - 600	800
големи градове до 500 000 жители и площ 35- 80 км^2						
1	Близкият изток	тухлени	300 - 350	400 - 500	400 - 500	400 - 800
		каменни	500 - 600	500 - 600	500 - 600	600
		железобетонни;	400 - 600	400 - 500	400 - 500	400 - 800
		смесени	400 - 600	500 - 600	500 - 600	600
2	Азия	тухлени	300 - 350	500 - 600	400 - 500	400 - 800
		каменни	600 - 800	500 - 600	500 - 600	800
		железобетонни;	400 - 600	400 - 500	400 - 500	400 - 800
		смесени	400 - 600	500 - 600	500 - 600	800
3	Европа	тухлени	400 - 550	400 - 500	500 - 800	600 - 800
		каменни	600 - 800	500 - 700	600 - 800	800
		железобетонни;	400 - 600	400 - 600	600 - 800	600 - 800
		смесени	400 - 600	500 - 600	500 - 600	800

Анализът на особеностите на урбанизираната среда, е неразделна част свързана с РОБП за зоната на операцията/кампанията, което ще оказва съществено въздействие, както върху боеспособността и способите за действие на собствените формирования, така и на враждебно настроените военизирани групировки и местно население. Налагащата оценка на основните особености на урбанизираната среда, имащи пряко влияние върху воденето на бойните действия са характеристики на средата, посредством които се определя влиянието и върху бойните действия, това са

параметрите на постройките разположението им, планировката, структурата, площи, конфигурацията, характера на постройките, плътност на застрояване, населението и инфраструктурата.

Структурата на урбанизираната среда (терен, общество, инфраструктура и др) е в пряка зависимост от планировката и застрояването на участъците:

- административна част, намираща се обикновено в центъра на населения пункт; жилищни райони;
- индустриална зона;
- територия заета от транспортни обекти (железопътни, морски, речни и летища);
- складови територии;
- незастроени територии;
- зони от трайни насаждения (паркове, защитни пояси)
- санитарно защитени зони (вододеини зони);
- прилежащи предградия.

Характерът на постройките и съоръженията оказват влияние най-вече със здравината, качеството и вида на материала (железобетон, камък, тухла, кирпич, дърво), от които са направени сградите, а така също и от дебелината на стените и височината на сградите. Там където преобладават дървени, кирпичени и тухлени постройки е възможно бързото им разрушаване, което затруднява изграждането на устойчива отбрана. Железобетонните сгради, съоръжения, гари, летища и комуникации са благоприятни за организиране на устойчиви опорни пунктове, затрудняващи бойните действия и налагащи допълнително огнево поразяване и създаване на щурмови групи и отряди за овладяването им. Трябва да се отбележи, че повечето жилищни и административни сгради имат сравнително тънки стени (30 – 40 см), които лесно се разрушават от оръдия с малък и среден калибър.

References

1. Закон за административно-териториалното устройство, изм. ДВ. бр.36 от 1 май 2021г.
2. Army_Field_Manual__AFM__A5_Master_ADP_Interactive_Gov_Web
3. Енев Е, Когнитивни процеси при управление на информацията в операции за урбанизирани територии, Монография, 2021г, ISBN 978-619-239-533-9
4. FM 3-06.Urban operations, Washington, D.C.: Headquarters, Department of theArmy.
5. ATP 3-06 Urban operations Headquarters, Department of the Army - december 2017
6. Хинов И., Влияние на боеспособността на тактическите формирования върху вземането на решение, дисертация; Рег. №RB 217308-083-06/СИ-29-51/24.02.2022 г.

EFFECTS OF AMMUNITION IN AN URBAN ENVIRONMENT

Radoslav B. Ghalakov

G. S. Rakovski National Defense College, „Command and Staff" Faculty,
Department „Land forces" r.chalakov@rndc.bg

Abstract: *Determining the effectiveness of the use of fire support means, as well as how to determine and report this effectiveness, will depend on the determination of the effectiveness of the munitions in order to determine the Collateral Damage Assessment (CDA) and the* Battle Damage Assessment *(BDA).*

Keywords: *Effects, Ammunition, Damage, Urban environment*

ЕФЕКТИ НА БОЕПРИПАСИТЕ В УРБАНИЗИРАНА СРЕДА

Радослав Б. Чалъков

Военна академия "Г. С. Раковски", факултет „Командно – щабен",
Катедра "Сухопътни войски", r.chalakov@rndc.bg

В днешните въоръжени конфликти се причиняват повече наранявани с експлозивни оръжия, отколкото с куршуми и противопехотни мини.
Д-р Марко Балдан, старши хирург, МКЧК, октомври 2019 г

Боеприпасите са предназначени за поразяване на жива сила и военна техника, разрушаване на съоръжения и укрепления, а също така за изпълнение на специални задачи (осветяване, задимяване, радиозаглушаване и др.). Към боеприпасите се отнасят авиационните и дълбочинни бомби, артилерийските изстрели и снаряди, бойните части на ракети и торпеда, гранатите, инженерните и морски мини, патроните за стрелково оръжие, подривните заряди, реактивните снаряди и др. Когато те изпълняват подобни функции, когато се използват в урбанизирана среда, както и когато те се използват другаде, въздействието от тяхното използване може да е различно.

Използването им в урбанизирана среда е довело до значителни наранявания и смъртни случаи на цивилни граждани и нанасяне на значителни щети на основната инфраструктура, домове и предприятия. Анализирането на техническите характеристики на боеприпасите и тяхното използване в урбанизирана среда, ще доведе до намаляване на загубите. Основните системи използвани в бойните действия в урбанизирана среда са 122 мм ракетни установки, 81-120 мм минохвъргачки, 122-155 мм артилерийски системи, 115-125 мм танкови оръдия и ракетни бомби. На база на тези системи фокусът ще бъде върху ефектите на боеприпасите им, присъща точност и прецизност на използваните оръжейни системи и характера на използването им.

Въздействие на боеприпаси в урбанизирана среда. Установено е, че ракетните боеприпаси и 122 mm реактивен снаряд М21ОФ-М имат най-широка площ на поразяване, въпреки че минохвъргачките и артилерийските снаряди са водещи по двуцифрени жертви. Танковите боеприпаси имат по-ограничена смъртоносна зона, отколкото други.

Въпреки че има мерки, които могат да бъдат предприети, за да се коригират ефектите на боеприпаса по отношение на начина, по който функционира, много системи като реактивната система за залпов огън (РСЗО), постигат определен ефект и възможност за изстрелване на единични снаряди по голяма площ (обикновено места на съсредоточаване на вражески части) и от голямо разстояние.

Въздействието на боеприпасите в урбанизиран терен е повлияно съществено от наличието на изградени инфраструктури и географски характеристики. Превозни средства, жилища, търговски имоти, фабрики, училища, болници и др осигуряват известна защита от боеприпасите, но също така ги усилват, поради канализирането и отразяването на взривните вълни.

Сградите и превозните средства допринасят за други осколки – тухли, бетон, стъкло и др, произлизащи от взривната вълна. Всички източници на гориво или токсични химикали в зоната на въздействие на боеприпаса могат да представляват допълнителна смъртоносна опасност за хората, както и нарушена структурна стабилност на сградите, които могат да бъдат сринати.

Интуитивният рефлекс сред хората да търсят убежище от боеприпасите при попадането им в сгради, превозни средства, тесни улици, тунели и подобни затворени или полузатворените пространства представляват смъртоносен риск. Освен отразяващите взривни вълни в такива пространства, засилването на ефекта на боеприпаса се получава поради наличието на голям брой хора и структури в рамките на ефективния обсег на боеприпаса, както и източници на вторични осколки. Това води до по-висок дял смъртни случаи, отколкото би било вероятно в открити пространства.

Хората са особено уязвими към свръхналягане и отразена взривна вълна. При преживяване на атака с боеприпас са видими само повърхностни синини, но не се изключват спукани тъпанчета, увредени бели дробове, вътрешно кървене, мозъчни увреждания, инфекции и отравяния и фрактури на костите.

Получените поражения зависят от ефектите, произтичащи от детонацията на боеприпаса, т.е. свръхналягане на взрива, осколки, топлинни и светлини въздействия и ефекти, произтичащи от обектите, засегнати от детонацията: отломки (т.е. парчета зидария, водопровод, стъкло, дърво, метал, костни фрагменти и т.н.) и образуване на кратери.

Влиянието на различни фактори, които е трудно да се отчетат точно върху големината на действие затруднява изключително много избора на вида боеприпас. За изчисляване на увреждащия ефект на боеприпаса се използват различни изчисления, като зоната на разрушения може да се определи както следва:

При използване на фугасни боеприпаси

Фугасните боеприпаси са обвързани с експлозивния ефект на боеприпаса произтичащ с контактно действие (в пряк контакт с обект), и върху ефекта на ударната вълна, с което фугасните боеприпаси са обвързани с калибъра, количеството взривни вещества и характеристиката на боеприпаса. Ефекта на боеприпаса се определя по формулите:

$$R_p = K_p \sqrt[3]{m_з} - b_з = K_p \left(\sqrt[3]{m_з} - \frac{b}{K_{p1}} \right). \quad (1.1.)$$

където:

K_P , K_{P1}- коефициенти, които определят размера на зоните на деструкция[3] в обекта

m - Масата на заряд, необходим за унищожаване на обект на разстояние R_p, се изчислява, както следва:

$$m_з = \left(\frac{R_p}{K_p} + \frac{b}{K_{p1}} \right)^3. \quad (1.2.)$$

където:

$R_{p\,-}$ радиуса на зоната, а разрушение на боеприпаса

[3] *Нарушаване или разрушаване на нормалната структура, нормалния строеж на нещо*

При използване на осколочни боеприпаси

Бойната ефективност на осколочните боеприпаси зависи от естеството на срещане на боеприпаса с повърхността, което се определя от редица различни фактори: физични и механични свойства на материала на тялото, детонация специфични характеристики на боеприпаса, характеристиката на боеприпаса, условия и др. В зависимост от естеството на среща с целта се определя и общият броят на осколките и тяхната маса. Формулата на Юстров определя общия брой на осколките.

$$N = \beta_0 \frac{m_{ВВ}}{d} \frac{\sigma_у}{\sigma_в \delta} \frac{\chi^2 + 0,5}{\chi^2 - 1}, \quad (1.3.)$$

където:

β_0 - е коефициент в зависимост от свойствата на взривното вещество (за тротилов еквивалент е = 46)

$m_{ВВ}$ – е масата на боеприпаса

d – калибър на боеприпаса

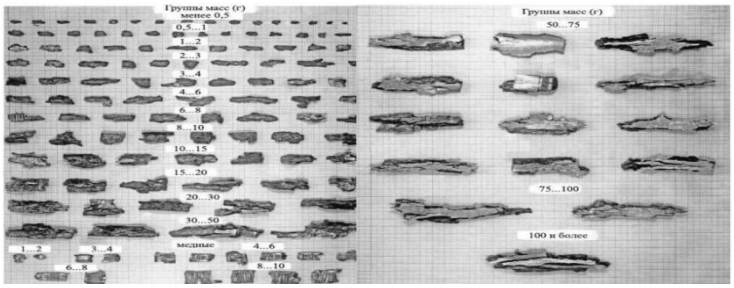
σ – характеристиката на материала на копуса на боеприпаса (еластичност, якост)

χ – плътност на материала на копуса на боеприпаса

Таблица 1

Разпределение на осколките по тегло

снаряд	Брой на осколките по тегло						
	0,5-1,0	1-2	2-3	3-4	4-6	6-8	8-10
53-ОФ-540	704	632	314	216	28	196	152
3-ОФ-25	115	1045	560	371	491	329	235
	10-15	15-20	20-30	30-50	50-75	75-100	Над 100
53-ОФ-540	268	176	199	192	87	32	21
3-ОФ-25	401	221	224	149	40	9	1



Фигура 1. Видове осколки по тегло

Точност и прецизност на системите

Точността и прецизността на взривното вещество на анализираните системи се различават значително. Танкови оръдия и управлявани самолети бомби могат да се използват в точна и прецизна функция за директен огън, когато са изпълнени определени условия, а системите за артилерийски огън и минохвъргачки са способни на относително високо ниво на точност при функция за индиректен огън. Въпреки това, поради по-ниска прецизност, присъща на техния дизайн, снарядите обикновено са разпръснати по широка площ, която се увеличава с разстоянието до целта. Неуправляемите артилерийски ракети като цяло не са точни, при тях нивото на точност и прецизност може да бъде непредсказуемо и несъвместимо с която и да е от системите, поради фактори като качество на боеприпасите, поддръжка на системата и практическия опит на стрелящия в използването на техниката при различни терени и метеорологични условия. Повечето системи за индиректен огън, използвани в днешните конфликти не са в състояние да постигнат необходимата висока степен на точност да попадение в малка точкова цел още с първия снаряд.

Анализът и процедурата за положително идентифициране на целта, оценка на непосредствената физическа среда и подбор на най-точното и прецизно въоръжение и боеприпас са ключови

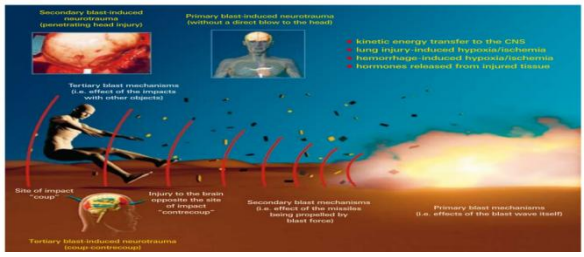
фактори за намаляване на съпътстващата щети (загуби). Въздействието върху цивилните граждани и инфраструктурата зависи от избора на оптимален тип боеприпас.

Като общо правило въоръжените сили трябва да имат задълбочени познания за ефектите на боеприпасите и трябва да могат да предвидят действието им от директен, индиректен или въздушен огън; избрани въз основа на редица променливи включително достъп и физическа близост до целта, география, време, налични оръжейни системи и съображения за ОСЗ.

Ефектите от използването на боеприпасите в застроени райони е особено важно по отношение на въздействието на осколките и отломките. Такъв пример е разработването на нови, по-малки бомби, оборудвани със системи за прецизно насочване като и бомби с малък диаметър до 110 кг.

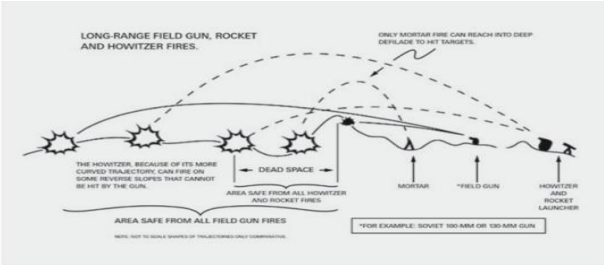
Фигура 2. Ефект от боеприпас с прецизно управление с малък диаметър.

Традиционно е използването на боеприпаси с значителни малки количества високо експлозивни съставки, обикновено допълнени от осколките, за да се постигне ефект на широка площ. Тези боеприпаси причиняват щети главно чрез взрив, осколки и термични ефекти.



Фигура 3. Ефекти на боеприпасите

Повечето боеприпаси са проектирани, разработени и използвани като оръжия с ефект на зона, често използвани от разстояние, за да се постигне максимален ефект срещу множество цели. Те могат да използват принципи на директен огън или индиректен огън (фигура 4), в зависимост от системата.



Фигура. 4 Сравнителен анализ на артилерийските системи

Важно съображение при използването на системи е необходимостта от осигуряване на точност и прецизност, подходящи за предвидените ефекти, за да се увеличи максимално ефективността на боеприпаса и все повече да сведе до минимум съпътващите загуби. Няколко усложняващи фактора трябва да бъдат напълно взети предвид, преди да може да се оцени реалистично бойната ефективност на боеприпасите, за да не се предоставят прекалено оптимистични прогнози за бойната ефективност:

- Действия на ПС – ефектите от действията и противодействието на ПС;

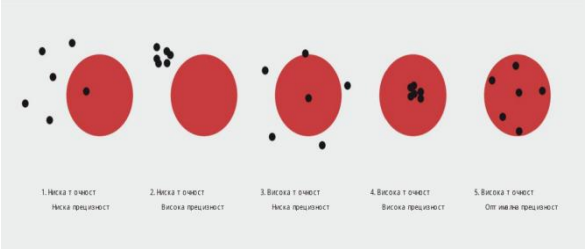
- Точност на попадение – измерване на това колко близо една система може да достави своите боеприпаси до целта;
- Въздействие на боеприпасите – характеристики на боеприпаса включващи взрив, осколки, налягане и др;
- Уязвимост на целта – чувствителността на целта към крайния ефекти или специфични механизми за поражение;
- Надеждност на боеприпаса – надеждност на функционирането му;
- Траектория – балистични характеристики на системите или боеприпаса.

Точност на попадение на боеприпасите

Сложният и предизвикателен характер на военните операции в застроена градска среда и рискът от нежелани ефекти, дължащи се на концентрацията на цивилни граждани и обекти от инфраструктурата на населения район (пункт). Постигането на висока степен на точност и прецизност при стрелба е от изключителна важност, ако целта е да се постигне въздействие върху конкретна цел и да не се удари нищо друго освен целта.

Като има предвид, че има особени разлики между използване на системите в зависимост от видът огън във всички ситуации, за попадение трябва да се знае точното местоположение (x, y). Термините *„точност“* и *„прецизност“* имат две различни значения, които често се разбират съответно като способност за поразяване на желана цел и способност за поразяване на тази цел последователно. Разликата между точност и прецизност може да бъде полезна във връзка със стрелбата. Ако стрелбата е точна, се получава *„групираност“* на ударите и попадение върху целта.

Ако стрелбата е прецизна, попаденията ще са по-близо заедно, в тясна група. Това обаче може да не е непременно близо до центъра на целта (фиг. 5).



Фигура 5 Точност и прецизност, засегнати от систематични и случайни грешки (червеният кръг представлява желаната област на въздействие). [4]

При системите за индиректен огън не всички боеприпаси удрят центъра на желаната цел. Една често срещана мярка за прецизност на оръжейната система е известна като *„вероятна кръгова грешка“ (CEP)* (фигура 6).

$$P_{kill} = \iint_A P_{impact}(x,y) \cdot P_{kill|impact}(x,y)\, dxdy, \qquad (1.4.)$$

, където:

$P_{impact}(x, y)$ - вероетността на боеприпаса да попадне в центъра на целта.

$P_{kill|impact}(x, y)$ - вероятността да се унищожи целта от осколките.

[4] *Източник: ARES Indirect-Fire Report,*

Въздействие на боеприпаси

Въздействието на боеприпасите може да бъде разделено на основните щети и техните ефекти, на вторичните и/или други ефекти предизвикани от взрива. Първичните ефекти на взривните оръжия се определят като тези причинени пряко от разрушителните ефекти, които се излъчват от точката на съприкосновение и включват взрив, свръхналягане, осколки, топлини и светлини ефекти.

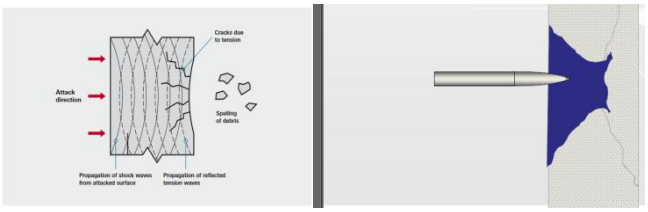
Вторичните ефекти на боеприпасите произтичат от средата, в която боеприпасът детонира. Най-значимите вторични ефекти включват вторични осколки и образуване на кратери. Вторичните ефекти произлизат от обекти, които са били засегнати от детонацията, и може да включват такива предмети като парчета зидария, стъкло и др. Вторичните ефекти обикновено са по-големи от първичните и радиусът им не е толкова голям колкото скоростта на движение.

Образуването на кратери може да причини значителни щети на подземната критична инфраструктура, включително на електроцентрали, комуникации и водоразпределителни съоръжения. Това може да е умишлено постигнат ефект получен от боеприпасите, както и създаване на препятствия по пътищата за подход или за нарушаване на инфраструктурата. Такива ефекти могат да имат допълнително хуманитарно въздействие. Кратерът може да предотврати използването на писта или летище от ПС, например, може също да попречи на доставката на хуманитарна помощ със самолети на по-късна дата.

Уязвимост на целта

Снарядът или осколките не е необходимо да проникнат в твърдото тяло, те просто удрят външната повърхност с достатъчно енергия, което на свой ред води до раздробяване. Възможен сценарий, е раздробяване на тухлена стена, ударена от взривна вълна, или в някои случаи снаряд или достатъчно енергични осколки, причиняващи вторично раздробяване във вътрешността на сградите.

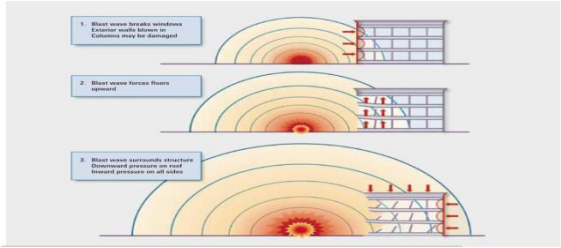
Значителна опасност за хората, които се намират в или около сгради и конструкции представлява вероятността те да бъдат смачкани от частичното или пълното унищожение на поразената инфраструктура.



Фигура 6. Разпространение на ударни вълни през средата на бетонна стена и тяхното отражение обратно като вълни на напрежение, които напукват средата и причиняват разцепване на отломки [5]

Ефектът на вълната върху структурата зависи от това каква е структурата и как е изградена. Когато се срещнат свръхзвуковият ударен фронт от детонация с твърда структура, една част от енергията се отразява, а друга част от нея се предава в структурата, а относителните количества зависят от свойствата на структурата.

[5] *(източник: Dynasystems Ltd. UK & GICHD). (05.05.22г)*



Фигура 7. Ефектът на взривна вълна върху сгради и конструкции.

В градските райони конструкциите отразяват ударната вълна в различни посоки. Поради плътно опакованите структури, типични за такива райони, взривната вълна не може свободно да се движи извън точката на детонация. Това води до възникване на взривна вълна частично абсорбирана, отразена и канализирана в и около заобикалящата я инфраструктура.

Нивото на точност и прецизност на системите се различават значително, въпреки това, техните потенциални ефекти ще бъдат повлияни от боеприпаса. Поради зависимата от дизайна, ниска прецизност на артилерийските системи, снарядите обикновено се разпространяват върху значителна площ, която се увеличава с увеличаване на разстоянието до целта. Това ограничава техническата им пригодност за използване срещу по-малки или движещи се цели, особено в урбанизирана среда.

Повечето артилерийски системи, използвани в днешните конфликти, не са в състояние да постигнат високата степен на точност, необходима за поразяване на малка точкова цел с първи изстрел. Неуправляемите артилерийски ракети не са нито точни, нито прецизни. Благодарение на дизайна си като система, при максимален обсег 122-мм система БМ-21 не би могла надеждно да въздейства върху площ, по-малка от 600 х 320 м, в която ще бъдат засегнати хора и структури. Прецизно насочвана още може да запази ефекта на широка площ поради огромната си мощност с използването на системи с калибър 122-155 мм.

References

1. Атанасов А, Влияние на огневите удари върху ефективността на огневата поддръжка в операциите на многонационални съвместни оперативни сили, Дисертация, С 2010г.

2. Асенов, В. „ Ефективност на стрелбата и управлението на огъня на артилерията”, Учебно пособие, С, ВА, 2004.

3. FM 2-91.4 intelligence support to operations in the urban environment headquarters, department of thearmy - june 2005

4. FM 3-09 field artillery operations and fire support - april 2014 headquarters, department of thearmy.

WEAPONEERING IN AN URBAN ENVIRONMENT

Radoslav B. Ghalakov, Andon P. Andonov

Rakovski National Defence College, Faculty " Command-staben",
Department "Land forces", Department "Air Force and Air Defence"
r.chalakov@rndc.bg, a.andonov@rndc.bg

Abstract: *Weaponeering is the process of estimating the quantity of a specific type weapon required to achieve a specific level of damage to a given target, considering target vulnerability, weapon effects, munition delivery errors, damage criteria, probability of kill, weapon reliability. Weaponeering is a core competency of targeting, although many confuse all targeting with weaponeering.*

РАЗЧЕТ НА СРЕДСТВАТА ЗА ВЪЗДЕЙСТИЕ В УРБАНИЗИРАНА СРЕДА

Радослав Б. Чалъков, Андон П. Андонов

Военна академия "Георги С. Раковски", Факултет „Командно–щабен",
Катедра "Сухопътни войски", Катедра "ВВС и ПВО"
r.chalakov@rndc.bg, a.andonov@rndc.bg

По време на война няма невредими войници.

Хосе Нароски

Конфликтите в урбанизираната среда се усложняват от факта, че някои от воюващите страни ще избягват да се изправят пред ПС на открито, като вместо това се смесват с цивилното население и дори започват атаки по населени места. Дали умишлено или неумишлено, или налагано от ПС, близост излагаща цивилните граждани в опасност, като привлича военните действия да се провеждат в урбанизирана среда. Изправени пред такъв ситуация и по примера на последните конфликти, ПС често избират средства или методи за борба, които не изискват от него да излага силите си на рискове и заплахи.

Въпреки че голяма част от съвременните конфликти през последните десетилетия се провеждат в урбанизирани райони, средствата и методите, бойните възможности, използвани от страните, досега не са претърпели еволюция в използването на средствата. Днес, бойните действия в градските райони често се водят с оръжия и тактики, които не са били първоначално проектирани или не са били адаптирани по друг начин за използване в такива зони. Средства за индиректна огнева поддръжка се използват в открити бойни полета и като цяло не са причина за безпокойство, когато се използват срещу военни цели в такива среди. Когато бъдат използвани срещу военни цели разположени в урбанизирана среда, те обикновено постигат резултати, които често надхвърлят желания ефект с опустошителни последици за цивилните граждани.

Ден 14 от събитията в Украйна (09.03.2022):
Руската артилерия обстрелва Украйна с часове.

Няма лесен избор за командира, когато се стигне до операции в урбанизирана среда. Защитата на цивилни граждани и цивилни обекти срещу опасностите от военни операции обикновено е много по-сложна в такива среди, а предизвикателствата само нарастват с гъстотата на населението, степента на интеграция на инфраструктура и взаимозависимост на основните градски услуги и непосредствена близост на цивилни и обекти от инфраструктурата до военни цели. Все по-често се правят изводи, свързани с оценка съпътстващите загуби и с вида въоръжение, което се използва и урбанизирана среда в които се използва.[vii]

От 2011 г., въз основа на наблюдението съпътстващите щети върху цивилните граждани, причинени от използването на средства за индиректна огнева поддръжка в урбанизирана среда, се призовава държавите и страни участващи във въоръжени конфликти, да разглеждат участието си от перспективата на функции Weaponeering[1], за да избягват използването на средства с възможности за широка зона на въздействие на боеприпасите в гъсто урбанизиран терен.

Разчет на средствата за въздействие (Weaponeering) е процес на оценка на количеството оръжие от специфичен тип, необходимо за постигане на конкретно ниво на въздействие върху дадена цел, като се вземе предвид уязвимостта на целта, ефектите на оръжието, грешките при попадение на боеприпаса, степента за боеспособност на целта, вероятността за унищожаване, надеждността на оръжието и т.н. Специалистите определят количествено очакваните резултати от използване на смъртоносни и несмъртоносни средства срещу цели. Списъците с цели осигуряват основата за дейностите по оценка на въоръжението. Тъй като ограниченията във времето могат да попречат на изчисленията на потенциалните ефекти срещу всички цели, изчисленията трябва да продължат по приоритетен начин, който отразява списъка с цели.

- Разпределение на средствата за въздействие. Разпределението на средствата е определяне на специфичен брой и видове въоръжение за използването му през определен период от време или за изпълнение на определена задача.
- Ефективност на средствата за въздействие. Тя е статистическа оценка на очакваните резултати от специфични ефекти на боеприпасите, среда, в което ще се използва, степента на боеспособност на целта, точност, надеждност на боеприпасите и балистика. Това трябва да бъде тясно свързано с оценката на ефективността на боеприпасите при оценката на бойните действия.

[1] *Weaponeering - дефинира термина като процес на определяне на количеството на конкретен вид смъртоностни и несмартоностни средства, необходимо за постигане на конкретно ниво на щети на дадена цел, като се има предвид уязвимостта на целта, ефектът от оръжието, точността на попадениена боеприпаси, критериите за повреда, вероятността за намаляване на боеспособноста..[8]*

- Данни за ефективността на средствата за въздействие. Трудно е да се съберат данни за бойната ефективност на средствата за въздействие. Оръжията не се управляват от лабораторни експерти, които методично следват плановете за изпитване, а от реалното им използване. Данните, използвани за прогнозиране на ефективността на оръжието, трябва да бъдат валидно представяне на това как хората и машините се представят в реални бойни действия. Много малко от този тип информация може да бъде възстановена от боен опит. Някои данни могат да бъдат получени от тестови стрелби, ако тестовете се контролират внимателно, за да се отчитат реалностите на използването им, но други данни просто не са налични и трябва да бъдат екстраполирани.

Основните стъпки при извършване на разчет на въоръжението са:

- Получената разузнавателната информация;
- Информация за наличните системи (наши и на ПС);
- Определяне на обектите, които да бъдат анализирани;
- Определяне на степента на въздействие, ако трябва да се извърши анализ на отделните цели;
- Определяне на ефективността на системите;
- Определяне на целите и желаните точки за въздействие;
- Извършване на оценка на ефективността на системите.

Получената разузнавателна информация. Изисквания за получаване на необходимите данни и има ли необходима специална информация за изпълнение на задача за определяне на избора на средства за въздействие. Изискванията ще послужат за разработване на целта, така и за избора на въоръжението.

Информация за наличните системи (собствените и на ПС). Познаване на огневите системите, които са на разположение за използване, както и вероятните тактики за използването им. Освен това резултатите от въоръжението ще дадат и допълнителна информация, полезна при изготвянето на препоръки за използването на въоръжението, включват: време за готовност и използване на въоръжението, степента на въздействие, бойният потенциала на системата, с което да се определят страничните щети и ROE.

Определяне на обектите, които да бъдат анализирани. Третата стъпка е да се проучат данните, предоставени за целите и да се реши кои елементи да се анализират за уязвимост т.е. къде целта е най-уязвима и за какво оръжие.

Някои цели издържат на определено въоръжение, така че може да е трудно да бъдат повредени или унищожени. Анализът на скорошните конфликти ще подпомогне извършването на оценка на ефективността на боеприпасите и ще спомогне при избор на средства за въздействие. При необходимост и в зависимост от вида и структурата на целта може да бъде проникнато и съдържанието вътре в нея да се унищожи с малко или никакво увреждане на самата структура на обекта. Следователно основният въпрос, на който трябва да се отговори е „Какъв вид щети трябва да бъдат нанесени на целта, за да се постигне поставената оперативна цел"?

Определяне на обектите, които да бъдат анализирани може да бъде разделено на две дейности: първо, извършване на функционален анализ и второ, извършване на структурен анализ. При изготвянето на функционален анализ се идентифицира функциите на всички части на обекта, определя относителната важност на всяка част и определя онези части, които са жизненоважни за работата на обекта. Структурният анализ предоставя голяма част от информацията, необходима за определяне на общата уязвимост на обекта. Той включва видове конструкции, размери на конструкции, оборудване и т.н. Резултатите от този анализ обикновено определят компонентите, по които ще се въздейства.[viii]

Определяне на степента на въздействие, ако трябва да се извърши анализ на отделните цели. Данните за уязвимостта на целта трябва да бъдат изразени по отношение на желаните резултати, когато по целта се въздейства. По-конкретно, желаното ниво на унищожаване,

подавяне или неутрализиране, с което се търси създаване на значително предимство за собствените сили.

Измерването на степента варира значително в зависимост от типа на целта, основните входни данни и формата на желаните резултати. Като цяло форматът на изходните данни включва: уязвими зони за снаряди; тежести на заряда и разстояния на разсейване на осколките; и смъртоносни поразяващи действия на снаряда. Критериите за въздействие трябва да включва времеви параметри. Искането въздействие може да включва, например, превозно средство неспособно да се движи в рамките на пет минути след удара или изискване да се въздейства върху системата за командване и управление „*да спре 20 минути след удара*". Тъй като някои оръжия могат да бъдат ефективни при постигане на първия тип въздействие, а други могат по-лесно да постигнат втория тип, е необходимо да се вземат предвид разликите в системите, необходими за въздействие. Определяне на степента на въздействие ще се извърши от формулата:

$$g = qvm^{\frac{1}{3}} \tag{2.1.}$$

Където:

q – коефицента определен от видът на целта и от видът на броепипаса,

v - скоростта на осколките

m - масата на боеприпаса

Скороста на осколите ще се определи по формулата:

$$v(s) = (v_0 + v_2)e^{\frac{-1}{c_1}(\frac{m_{ref}}{m})^{1/3}s} - v_2, \tag{2.2.}$$

Където:

v_0 – началната скорост,

v_2 и c_1 - константа описваща забавянето (c_1 = 17, 51m, v_2 = 17m/c

m_{ref} - масата на референта на осколката (m_{ref} = 0.5g).[2]

Определяне на ефективността на системите. Ефективността на използването на средствата за въздействие варират в зависимост от вида система, целта, степента на въздействие, среда. Има различни начини за определяне на ефективността на системите в зависимост от комбинацията цел/въоръжението. Средата се състои от множество единични цели. Сградите се третират като цели за площ, освен, ако една сграда не се счита за основна цел.

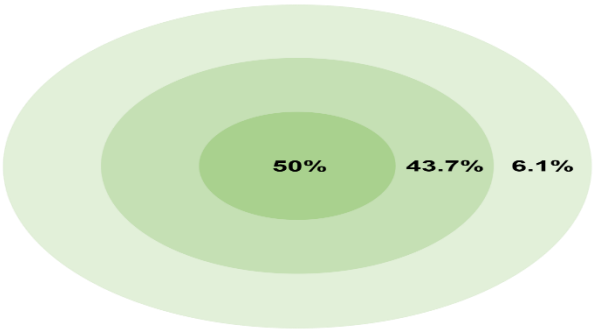
Определяне на целите и желаните точки за въздействие. Определя се желаната точка на въздействие (DPI)[3] или желаната средна точка на въздействие (DMPI)[4] , като при избора на точка за атака обикновено е най-добре, ако времето позволява, да се избере повече от една желана точка за въздействие и комбинация от средства за въздействие. Това позволява при ограничение в ресурсите или времето, да имат по-голяма гъвкавост при планирането. Целите в зоната за поразяване могат да се третират като единни цели, ако ефектите от степента на въздействие е по-голяма от вероятната кръгова грешка (CEP) *(Фигура 6)* е близка до размера на целта или комбинация от двете. [ix]

Вероятна кръгова грешка (CEP) се дефинира като *„радиус на окръжност, центриран в целта или средната точка на удар, в рамките на който вероятността от удар е 0,5"*.

[2] *В **пета глава** се описва подробно ефекта на боеприпасите.*

[3] *DPI - виж: JP 3-60 Joint Targeting 31 January 2013*

[4] *DMPI - виж: JP 3-60 Joint Targeting 31 January 2013*



x

Фигура. 6 Вероятна кръгова грешка (CEP)

Чрез комбинация на формулите (2.1 и 2.2) се определя ефективността на въздействие на боеприпаса и се определя точката на въздействие

$$s = c\left(\frac{m_{ref}}{m_{max}}\right)^{\frac{1}{3}} ln\left(\frac{v_0 + v_2}{\frac{g}{qm_{max}^{\frac{1}{3}}} + v_2}\right) \quad (2.3.)$$

Където:
s – точката на въздействие,

Множество DPI или DMPI трябва да се използват винаги, когато ефективната зона на поражение (в резултат на комбинацията от ефективното въздействие и CEP) е значително по-малка от площта на целта. Във всички останали случаи е достатъчна една точка на удар.

Извършване на оценка на ефективността на системите. По време на тази стъпка се оценяват различни системи и характеристики на боеприпасите, за да се определи най-добрата комбинация, която да се използва срещу всяка отделна цел. В тази стъпка се определя вероятността на резултата от попадението.

$$P_t = 1 - e^{\frac{-(A_E ntp)}{A_T}}, \quad (2.4.)$$

Където:

- Pt - процент на загуба за определено време
- AE - площа на действие на боеприпаса
- AT - площа/местото на целта
- n - броят на изстрелите за определено време
- t - времето прекарано *радиус на окръжност*
- p - вероятността на поражение от един изстрел
- $1\text{-}e^n$ – експоненциално разпределение на случайниа непрекъсната величина

Въз основа на тези стъпки се определят препоръчаните системи и боеприпаси, както и изчисленото ОСЗ. Извършването на оценка на ефективността на системите зависи и от поразяващото действие на боеприпасите. Трябва също да бъдат определени и видовете боеприпаси, които имат ще определени специфични ефекти.

Повечето системи за индиректен огън, използвани в днешните конфликти, не са в състояние да постигнат високата степен на точност, необходима за поразяване на малка точкова цел с първи изстрел. Неуправляемите артилерийски ракети не са нито точни, нито прецизни. Благодарение на дизайна си като система, при максимален обсег изследваната 122 мм система БМ-21 не би могла надеждно да въздейства върху площ, по-малка от 600 х 320 м, в която ще бъдат засегнати хора и

структури. Прецизно насочвана още може да запази ефекта на широка площ поради огромната си мощност с използването на системи с калибър 122-155 мм.

Планирането, организирането и провеждането на бойни действия в урбанизирана среда е процес, изискващ постоянно усъвършенстване на методите за работа на всички командири и техните щабове, умения за извършване на определени дейности в кратки срокове, със или без въздействие от ПС.

References

1. ATP_2-01.3_Intelligence_Preparation_of_the_Battlefield
2. Army_Field_Manual__AFM__A5_Master_ADP_Interactive_Gov_Web(1)
3. World Urbanization Prospects The 2018 Revision - Methodology
4. FM 3-06.Urban operations, Washington, D.C.: Headquarters, Department of theArmy.

COMMUNICATION AND COMPUTER TECHNOLOGIES AND CYBERSECURITY

NEW TECHNOLOGICAL TRENDS AND IMPACT FOR FUTURE OF CYBERSECURITY

Mihailescu Marius Iulian, Dumitru Dan

Faculty of Engineering and Computer Science, SPIRU HARET University, Bucharest, Romania,
m.mihailescu.mi@spiruharet.ro, d.dumitru.mi@spiruharet.ro

***Abstract**: Due to the latest events (pandemic situation and military tensions) that marked postively and negatively our existence, private and professionaly, the attacks on institutions and organizations increased significantly everyday, and new experiences were faced and they caught many professionals with the guard down. Many lessons were taught but not all of them were applied accordingly everyday in their activity. The current work objective is to bring into discussion a set of aspects that are well-known by professionals in field of cybersecurity but they are not used properly due to a variety of reasons. Based on a wide analysis of the most important concepts, technologies and frameworks on which cybersecurity risk management is based, we will need in the future to treat with a maximum responsability the way that we are applying and integrating cybersecurity within organizations. Re-designing the way that we are treating cybersecurity, how it twill fit within the CSIRTs teams, will represent the way if the battle against attacks will be won or not.*

***Keywords**: automotive hacking, mobile hacking, cloud computing, maritime cybersecurity, aviation cybersecurity, user behaviour*

Introduction

Cyber-enabled ships are among the most important infrastructures that already largely rely on digital services, according to the European Directive "EU 2016-679," and a deliberate disruption of their operations might cause financial loss, environmental harm, or even put human safety at risk. Maritime cybersecurity has not been thoroughly studied, despite some research being done in this area.In this essay, we first describe the security concerns and dangers that the contemporary maritime sector faces, particularly those that target the onboard systems. Finally, we explore a number of difficulties and unresolved issues that need to be addressed in further research. We start by describing potential mitigation activities that may be used in advance to prevent such assaults.

Today's vehicles are loaded with automated software that enables smooth connectivity for drivers in areas like airbags, cruise control, door locks, and advanced driver aid systems.

These vehicles use Bluetooth and WiFi to connect, which exposes them to a number of security flaws or hacker threats. In 2022, as automated vehicles become more prevalent, there may be an increase in attempts to take control of them or listen in on conversations using microphones. Autonomous or self-driving vehicles use an even more complicated process that demands stringent cybersecurity precautions.

With the introduction of AI into all commercial sectors, this technology combined with machine learning has significantly altered cybersecurity. The development of automated security systems, natural language processing, facial detection, and autonomous threat detection has all benefited greatly from AI. However, it is also used to create clever malware and attacks that get through the most recent data security mechanisms. Threat detection systems with AI capabilities can anticipate new attacks and immediately alert administrators to any data breach.

The goal of the current work is to analyze the latest technological trends and to identify the most dangerous vulnerabilities by analyzing the recent reports from ENISA within the current attacks, and

which were impacting the institutions and organization in a very sensitive context, such as COVID-19 pandemic situation and military tensions between Ukraine and Russia.

The structure of the paper is described as follows:

- *Section 1. Introduction.* The section presents the current context in which the research has been done. It is mentioned which are the sources used during the elaboration process of the current research.
- *Section 2. Automotive Hacking.* In this section we are discussing which are the trends and how an car can be hacked, which are the trends and general aspects related to the latest incidents related to the infrastructures (e.g., servers) and cloud-based solutions.
- *Section 3. Mobile Represents the New target.* The section discuss how a mobile device can impact organization/institutions and a wide variety of services, from automative hacking, to aviation and maritime services, taking into consideration the user behaviour as a prime factor in determining the nature of attack.
- *Section 4. Cloud and Its Vulnerabilities.* The section bring into discussion the latest vulnerabilities discovered in 2022 and trigger an alarm signal for the businesses environments.
- *Section 5. Case Study: Maritime Security and Its Application Vulnerabilities.* The section discuss about the main threats and how the attacks are impacting a variety of process from shore to sea side.
- *Section 6. Case Study: Cybersecurity based on User Behaviour.* In this section we are covering some important aspects regarding the user behaviour and the role that is playing within cybersecurity. Based on a proper analysis of the behaviour we can anticipate what the user is doing within the system.

Automotive Hacking

Automotive Hacking represents the process through which we are able to exploit vulnerabilities within the software applications, hardware components and communication systems that are installed on a automobile.

According to Auh0[1], Automotive-related cyber incidents increased by 605% from 2016 to 2019 alone, doubling from the previous year. These comprise data breaches, carjackings, and even taking over moving automobiles. But according to Justin Cappos, a researcher in computer science at New York University, the potential hazards are worse than anything we have yet seen.

Electronic control units (ECU), controller area networks (CAN), Bluetooth connectivity, key fob entry, and other computerized components are common in modern automobiles. Many people use the internet to access centralized servers as well. And there are numerous ways to attack each of these various electronic technologies [1], [2].

Server intrusions may be disastrous in a number of ways since they offer hackers access to all kinds of information, including sales data, mobile apps, and even the controls of every linked vehicle. There are numerous ways that data breaches might occur. It's possible that someone in your company downloaded malware, or an attacker may remotely access your network security using cloud security weaknesses.

Cloud-based installations are available from the general Internet and outside the network perimeter, in contrast to an organization's on-premises infrastructure. Although this infrastructure improves accessibility for customers and employees, it also makes it easier for attackers to access a company's cloud-based services without authorization. An attacker may gain direct access using compromised credentials or improper security settings, going unnoticed by the business [4].

Through the use of APIs, unconnected software products can interact and communicate without being aware of one another's internal workings. APIs are typically necessary and frequently provide ac-

[1] See https://auth0.com/blog/car-hacking-and-cybersecurity-in-automotive-industry/

cess to crucial corporate data. Businesses release a lot of public APIs to speed up the adoption of new technologies by enabling third-party developers and business partners to access their products and data.

Sometimes inadequate authentication and permission are used while implementing APIs. Anyone with an internet connection can view and potentially misuse data because they are entirely insecure. As a result, hackers and other bad actors are increasingly targeting unprotected APIs.

Mobile represents the new target

Between 2021 and 2022, a set of six threats were experienced within mobile devices, such as smartphones and tablets. The threats on mobile devices are increasing everyday due to the large of tasks that are performed by their users, the attacks happening on different level, such as malicious apps, network-level and exploitation of different vulnerabilities within the devices and mobile OS. The most dangerous threats experienced between 2021 and 2022 can be summarized as follows:

- Apps with malicious code and website with dangerous scripts
- Ransomware
- Phishing
- Man-in-the-Middle Attacks
- Root methods and jailbreaking
- Exploits related to the device itself and operating systems

Mobile devices are the target of the majority of phishing attacks since they are constantly on. Mobile users are particularly exposed, according to CSO, because they frequently monitor their email in real-time, opening and reading emails as soon as they arrive. Due to the lower screen sizes, email programs on mobile devices display less information, making consumers more vulnerable. For instance, unless you extend the header information bar, an email may just show the sender's name even after it has been opened. Never click on links in emails you don't recognize that can include images with hidden messages [12], [13]. Let the response or action items wait till you are at your computer if the problem is not urgent.

Training resources from the Infosec Institute state that improperly implementing strong encryption or using weak encryption algorithms can result in failed cryptography. To hasten the app development process in the first scenario, developers may choose to employ well-known encryption techniques in spite of their acknowledged security flaws. Because of this, any determined attacker can take advantage of the flaws to break passwords and get access. In the second illustration, programmers employ extremely safe algorithms but leave additional "back doors" accessible that reduce their efficacy. For instance, hackers might not be able to guess the passwords, but if developers introduce bugs in the code that let attackers change high-level app features—like sending or receiving text messages—they might not even require passwords to cause issues.

When wireless hotspots are accessible, nobody wants to use up their cellular data, yet free Wi-Fi networks are frequently insecure. In reality, three British lawmakers who consented to participate in a free wifi security experiment, according to V3, were readily compromised by tech specialists. Their VoIP chats, PayPal transactions, and social media accounts were all infiltrated. Use free Wi-Fi on your mobile device carefully for safety. Additionally, never use it to access private or confidential services, such as banking or credit card details.

Cloud and Its Vulnerabilities

Cloud storage is used by cybercriminals for a variety of things, including making false money. Businesses still misconfigure cloud storage, which has cost several companies millions of dollars, despite the potentially grave repercussions. One of the most prevalent vulnerabilities in cloud computing is this one.

Organizations run the danger of having their data exposed to the public when they improperly configure cloud storage. For a company and its clients, cloud misconfigurations can quickly turn into a serious cloud security breach. Businesses can encounter a variety of cloud misconfigurations. Here are a few instances of misconfiguration:

- **Misconfigured AWS security groups**: Access is controlled at the source, destination, port, and protocol levels by AWS security groups. They may be connected to EC2 server instances and other resources. To gain access to your cloud-based servers and steal your data, an attacker can take advantage of a weakness in the configuration of the AWS security group.
- **Missing restrictions for access:** If your cloud infrastructure is not adequately secured or protected against unauthorized access, your company may be at danger. Attackers may access cloud data and download sensitive information through unprotected cloud storage buckets, which could have major consequences for your company. When S3 buckets were first turned on by default on AWS, numerous data breaches occurred.

Each time a data breach occurs, millions of dollars can be lost. In accordance with Verizon's 2019 Data Breach Investigations Report, small businesses made up 43% of the victims. Small businesses are disproportionately affected by data breaches for a number of reasons, including the fact that they lack the same level of security as larger enterprises. They make attractive targets and typically sustain the most harm when their data is stolen within a big data context [3]. It is among the most hazardous flaws in cloud computing.

Case Study: Maritime Security and Its Application Vulnerabilities

Due to the rapid digital revolution that has brought new risks and regulatory obligations, cyber security is a subject that is becoming more and more relevant for the marine and offshore industries. Operational optimization is still a top priority, and those who can take advantage of emerging technologies and digital solutions will prevail. Because software-based operational systems are so crucial to ship operation, cyber security is a significant area of risk.

One of two categories—IT (standard information systems) or OT—is used to categorize cyber systems for ships and mobile units (operation and control systems).

When it comes to cyber security, IT is often more advanced, employing established practices, technology, and training that are deployed via an information security management system (ISMS) - at least onshore. IT system hacks can have a big financial and reputational impact. It normally has no effect on the secure operation of your ships and units, though.

In contrast, OT is less developed in terms of cyber security, and an attack on on-board OT systems could endanger the safety of the ship and its crew. As a class society, we collaborate with the sector to make sure that owners, yards, and suppliers are equipped to construct and manage offshore units and ships that are cyber-secure.

The aspects that makes cyber security extremely important for maritime, are related to:

- Commercial cyber hazards and requirements, such as TMSA 3 and a lack of insurance coverage, might affect the likelihood of receiving a charter and increase financial risk.
- Shipping and offshore are being impacted by an increase in cyber events. The increase of integrated boats also brings new risks that could remotely attack your ships and perhaps access or modify their control systems.
- Our sector is becoming more efficient because to new technologies, increased automation, and digitalization. Cybersecurity must also be in place in order to manage the risks and safety issues that this new technology presents, as well as to guarantee that vessel operations and crew and passengers safety.

- Owners, operators, and managers are being required by regulations and laws to take cyber risks into account. Examples include the IMO Guidelines on Maritime Cyber Risk Management and the IACS Unified requirements that are related to Cyber safety, E26 and E27.

Case Study: Aviation Security

Airports are subject to a number of cybersecurity dangers, some of which are occasionally avoidable. A distributed denial-of-service (DDOS) attack on the website of Bradley International Airport in Connecticut, US, is a recent illustration of this.

Through the use of botnets, or online networks of connected devices, several machines work together to overload a single website in an effort to crash it. In this instance, the threat was dealt with without much harm and business as usual was maintained.

In 2018, 380,000–500,000 customers of British Airways, the nation's flag carrier, were affected by a data breach. Login information, payment card information, and vacation reservation information were all compromised in the data breach. For more than two months, this data breach was not discovered.

This information was being stolen when credit card information was being input. It is obvious that the system had a problem because it was failing to check a certain section of the network.

People are more inclined to use the same password they use for other accounts than to create a new one while using airlines because, on average, they only use it twice a year. This raises the possibility of a successful data breach.

In the end, cybersecurity dangers do exist, and even while some are easier to avoid than others, there are staff people who try to ensure that these problems are not overlooked. Airports and airlines must invest time and money on training, but once it is finished, it must be repeated, and they are becoming more conscious of the importance of these procedures.

Case Study: Cybersecurity based on User Behaviour

In terms of adhering to security behaviors, it is crucial to highlight that computer users vary widely on an individual basis. According to a number of studies, individual variances in risk-taking, procrastination, and impulsivity can account for variations in adherence to security rules. We will also talk about the use of psychological techniques to increase compliance with security policies, which is crucial given the current human errors that might affect network security. These psychological techniques include the use of innovative polymorphic security warnings, rewarding and punishing good and bad cyber behavior, and encouraging increased consideration of the effects of one's activities in the future.

Sharing passwords, sharing information excessively on social media, accessing dubious websites, using unapproved external media, clicking links randomly, using the same passwords multiple times, opening attachments from suspicious sources, sending sensitive information via mobile networks, not physically securing personal electronic devices, and failing to update software are just a few examples of human errors related to cyber and network security [10].

Cyber security behaviors are influenced by individual variances in personality, cognitive, and behavioral features. The success of efforts to secure computer and information systems can be significantly influenced by individual variances in cognitive capabilities and personality factors. We go over a few of these psychological characteristics below.

As was previously mentioned, there are numerous human errors that can compromise computer and security systems. These errors include sharing passwords, oversharing information on social media, accessing dubious websites, using unapproved external media, clicking links randomly, using weak passwords, opening attachments from dubious sources, sending sensitive information via mobile networks, and not physically secured. However, phishing emails and password sharing have been the focus of the majority of studies on human errors.

Future studies should look into the individual differences and contextual factors (such as mood status, urgency at work, or multitasking) that underlie various other cyber security mistakes, including the use of the same or weak passwords across numerous websites, the failure to connect to virtual private networks, and the failure to encrypt data.

Conclusion

The current paper discussed those topics that are offering the most important battles in terms of securing infrastructure and computer applications and components due to the large amount of attacks that were occurring.

Starting from the last case study related to the user behaviour and its role that is played in computer security, to further understand the connection between cognitive processes and cybersecurity behaviors, however, future research should make use of computational models.

In terms of aviation cyber security, the airplanes represents the perfect target for a terrorist strike. Air terrorism also encompasses hazards to general aviation on the ground, such as airports and related infrastructure, in addition to the dangers posed by potential terrorist attacks on airborne aircraft. All kinds of air-related terrorism have the potential to erode public trust in the security of air travel, which might have a detrimental impact on particular airlines and other businesses in the aviation sector due to a reduction in passenger and cargo traffic. This article provides a general summary of the unquestionable current and prospective future dangers to in-flight security, as well as options and strategies for reducing the risks to a manageable level.

Despite sharing many of the same cybersecurity issues as other industries, it is increasingly clear that the marine sector matches the description of a critical infrastructure target for cybercriminals and is subject to hazards that might be seen as particular to this sector. For example, a successful hack may bring down a ship, leak sensitive data, take down the AIS of the ship, and/or generate fake or misleading AIS reports that would aid cyberpiracy and criminal, terrorist, or even state actors. This report examined the existing security risks and weaknesses facing the maritime sector today.

In aviation cyber security, maritime cyber security, and cyber security based on user behaviour we are dealing with mobile devices (smartphones, tablets, smartwatches) and which represent one of the important problem when it comes to certain attacks. Once these security breaches are resolved and fixed, then we are able to isolate and address any security issue with success using other tools based on artificial intelligence and machine learning [5-9], [11].

References

1. Thing, Vrizlynn L. L. and Jiaxi Wu. "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences." 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (2016): 164-170..
2. Meryem, Sghiri and Tomader Mazri. "Security study and challenges of connected autonomous vehicles." Proceedings of the 4th International Conference on Smart City Applications (2019): n. pag.
3. N. S. Loredana, "On recommendation systems applied in big data," *2016 8th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2016, pp. 1-6, doi: 10.1109/ECAI.2016.7861068.
4. Pham, Minh Thuy Truc and Kaiqi Xiong. "A Survey on Security Attacks and Defense Techniques for Connected and Autonomous Vehicles." Comput. Secur. 109 (2021): 102269..
5. A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi and R. Ahmad, "Machine Learning and Deep Learning Approaches for CyberSecurity: A Review," in IEEE Access, vol. 10, pp. 19572-19585, 2022, doi: 10.1109/ACCESS.2022.3151248.

6. Tarek Berghout, Mohamed Benbouzid, S.M. Muyeen, Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects, International Journal of Critical Infrastructure Protection, Volume 38, 2022, 100547, ISSN 1874-5482, https://doi.org/10.1016/j.ijcip.2022.100547.
7. Hanan Bahassi, Nahid Edddermoug, Abdeljebar Mansour, Azmi Mohamed, Toward an exhaustive review on Machine Learning for Cybersecurity, Procedia Computer Science, Volume 203, 2022, Pages 583-587, ISSN 1877-0509,https://doi.org/10.1016/j.procs.2022.07.083.
8. K. Y. Nikolskaia and V. B. Naumov, "The Relationship between Cybersecurity and Artificial Intelligence," *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 2021, pp. 94-97, doi: 10.1109/ITQMIS53292.2021.9642782.
9. Daniel Ventre, "Artificial Intelligence and Defense Issues," in *Artificial Intelligence, Cybersecurity and Cyber Defence* , Wiley, 2020, pp.105-186, doi: 10.1002/9781119788195.ch3.
10. F. Postolache and C. Ş. Dumitriu, "Reshaping the LMS IT Architecture and Educators Methodology through Blended Learning Approach," 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2021, pp. 1-6, doi: 10.1109/ECAI52376.2021.9515134.
11. Daniel Ventre, "On the Origins of Artificial Intelligence," in *Artificial Intelligence, Cybersecurity and Cyber Defence* , Wiley, 2020, pp.1-43, doi: 10.1002/9781119788195.ch1.
12. R. Vasil, F. M. Frigura-Iliasa, M. Iorga, H. Filipescu, M. Rogobete and M. Nen, "Digital Image Processing and Recognition in Industrial and Public Environments," 2019 2nd International Conference of Intelligent Robotic and Control Engineering (IRCE), 2019, pp. 37-41, doi: 10.1109/IRCE.2019.00015.
13. M. G. Rogobete, "An improvement of the time method for signal approximation. Electrocardiogram case study," *2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2022, pp. 1-7, doi: 10.1109/ECAI54874.2022.9847427.
14. V. Marascu, C. Stancu, V. Satulu, A. Bonciu, C. Grisolia, G. Dinescu, Material erosion and dust formation during tungsten exposure to Hollow-Cathode and Microjet Discharges, APPLIED SCIENCES-BASEL, Volume: 10, Issue: 19, Article Number: 6870, Published: OCT 2020. DOI: https://doi.org/10.3390/app10196870.

ARTIFICIAL INTELLIGENCE. SAME RULES, DIFFERENT PLAYGROUND

Elena Răducan

Automation and Electrical engineering, Faculty of Automation, computer science, electronics and electrical engineering/University "Dunarea de Jos", Galați, Romania, elena.raducan@ugal.ro

***Abstract**: The paper present an overview of Artificial Intelligence (AI) techniques succesful applied in heavy industry sector. Attention was paid mainly to underline the parallel between military appplications and industry applications where mathematical alghoritms are used to solve and/or identify a problem and in optimizing and controll an entire process. As result, can be state that the most important actor in this kind of analysis are the data collected from the field. Correct data with hygh level of accuracy give us the oportunity to obtain a good result.*

***Keywords**: Artificial intelligence, Big Data, mathematical modells , industry, military application*

Introduction

As everyone can see, in the past 10 years the AI subject "explodes" in all domains. Even if we talk about marketing, economies, social science, industry application, civilian and military application,…so on, AI is everyware, but it is not so new as we think. The figure below (Fig.1) was published by Harvard University in a special edition and we remark that in 1950 Alain Turing was the first researcher who put a machine to do something smart. At that time, with the existing technologies, the machine was able to execute simple command but not to register a sequence of several commands. Simply as that, on the first beginning the AI was not so intelligent but for that time the idea of Turing was brilliant. Back there, Alain Turing publisched a study where the main question was: "Can machine think?"[2]. He was not succed, at that moment, to make a machine to execute intelligent actions, because of the computer technologies limitation by '50es, but we can do this today! Even if, another question deserves to be asked today: why the humanity needs the implementation of AI in so many domains?

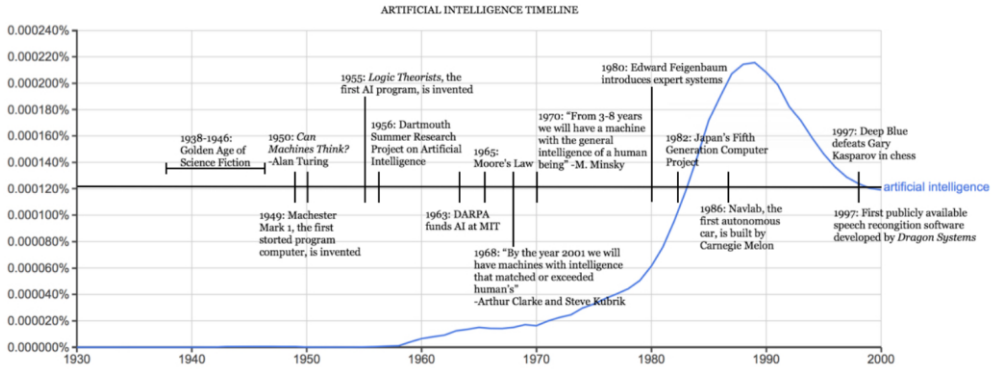


Figure 1: AI's technologie timeline. [1]

Earlier this year (January 2022) at World Economic Forum, another timline of AI was release, and it can easily see that AI is already everyware.

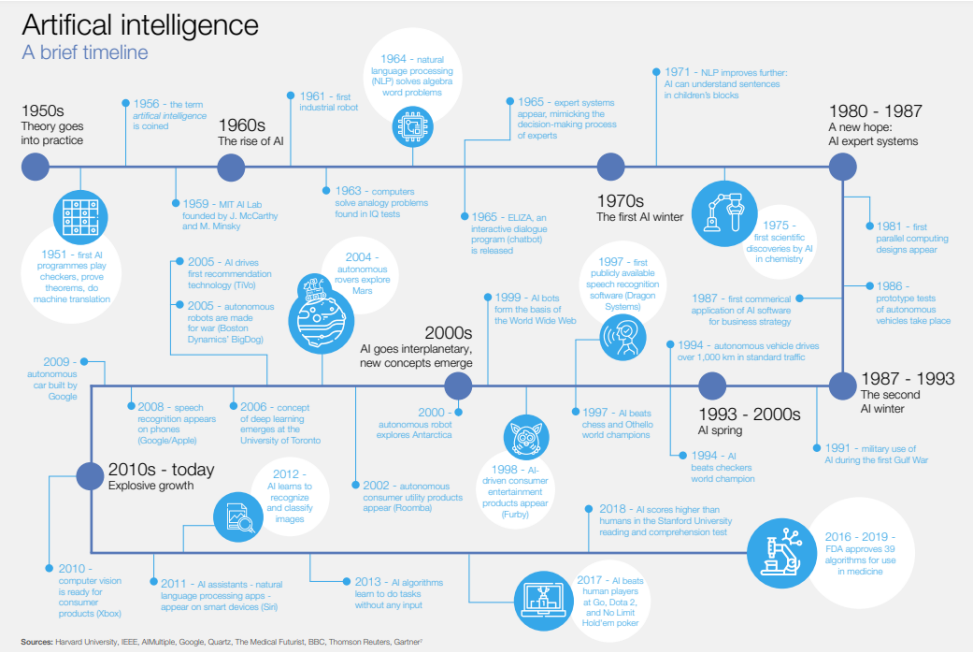


Figure 2: AI's timeline presented at Word Economic Forum [3]

In recent years, few scientifics paper have been accessible online, that claim that AI is increasingly entering in the military domain as well. However, many of them, do not describe real AI applications with real data due to the confidential nature of military research domain, real technologies used today being accessible to a small number of readers. The communication are formal one with the scope to understand the important of this technologies in military operation. Nowadays, the AI becoming a key tool in intelligence and analysis of the enemy's intelligence, and by helping to develops applications of autonomous weapon systems and vehicles. [4]

The AI have a huge potential in all area of life but even the expert do not have a clear opinion on the futures developments in this direction, and just the time will answer us to one of the concern, as Prof. Stephen Hawking said: " The rise of powerful AI will be either the best, or the worst thing ever to happen to humanity".[5]

Level of automation and AI's technique. The alpha and betta of the future.

According to Jorgen Frohm et al. in "Levels of automation in manufacturing", Oxford English Dictionary define automation as [6] :

"Automatic control of the manufacture of a product through a number of successive stage; the application of automatic control to any branch of industry or science; by extension, the use of electronic or mechanical devices to replace human labor"

Artificial Intelligence has also a definition, and according to Oxford English Dictionary, AI is: [7]

"The capacity of computers or other machines to exhibit or simulate intelligent behaviour", but many others definition are correlated the AI with Human Intelligence (HI).

At the beggining was still no major conflict between HI and AI, but nowadays this situation become unconfortable and has ethical implication because of the greater impact has the replacement of people already trained with the computers.[8]

Because of this half-half situation and because the AI already proved his power in almoste all the domains, the promotors of AI are trying to help people to be empowered and not threatened by AI. As example, in 2018 MinnaLearn and the University of Helsinky created a free online course with the goal to "demystify AI", with two section : Elements of AI and Building AI. This free online course is addressed to people from wide range of backgrounds, currently graduated by 850,000 people from 170 diffrents country.[9]

In industry, if we try to drawn the level of automation on a time-scale reactions of the systems, we observe that the existing 5 tipe of automation systems, from Level 0 to Level 4, are distributed as per Figure 3.

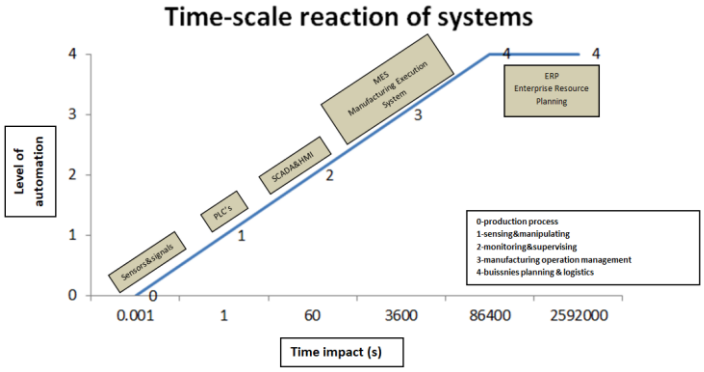


Figure 3: Time-scale reaction of the systems by level of automation.

Depending on the level of automation, the decisions are split between machines, sytem with software components and people, and the time reaction varies from micro-seconds to days and even months.

At the same World Economic Forum (WEF) mentioned above [3] the concept of AI present in industry by fusion with Industry 4.0 concept, appears as a new level of automation, Level 5, where "people do not need to be present" [3].

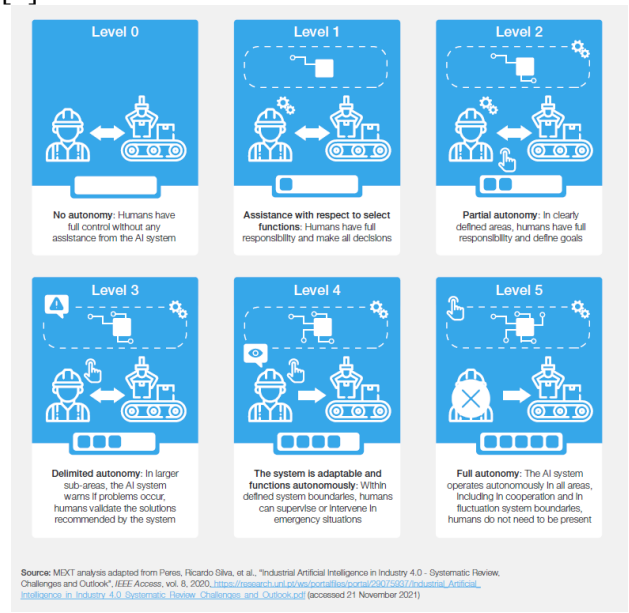


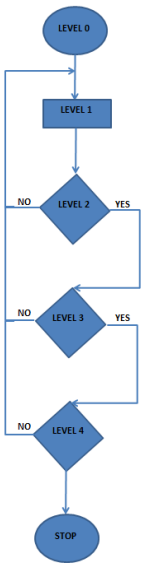
Figure 4: Levels of automation presented earlier this year at WEF [3]

More and more companies implemented already industry 4.0 concept by developing inside the companies and/or in cloud solution the Data Warehouse necessary to achieved the 4th levels of automation. Once you have this level of automation is easy to implement less or more intelligent alghoritms to do some data analysys. This kind of problem-solving techniques that involve the implementation of statistics, neural network, classifications alghoritms, so on, on large data Base (DB) are component of AI's technique. Because of that approach in the past decade, nowadays we reached a level of speed and complexity in about all the sectors, including the military sector. According to Natalie M. Scala et. Al. the Department of Defence (DoD) has been using analytics as long has been human conflicts [10]. Anyhow, if in industry we are talking about applying Machine Learning (ML) technique to identify, for example,

a disfunctionality of an equipment, or to investigate concept as predictive maintenance, in military sector the computer – integrated solution are includes in area such as: [10]

- Autonomous operations;
- Image processing;
- Target detection;
- Real-time system health monitoring.

If we are looking again at Figure 3, we can obviously see that we can not reach Level 4 of automation, the ERP-system, without the implementation of the lower levels of automation and without the necessary verification and validation from decisional levels of automation. The decisional level of automation can means for example a mathematical model implemented in Level 2, or the PLC's program to respect the rules, the manager, operator of machine, process engineers, and so on. To cut short, means people and computers need to validate differents steps from the entire automation system. If we do the logical diagram of that logical assumption, the result will be as per Figure 5 a. Now if we are looking to the Level 5 definition according to WEF, how the logic diagram will be?. For that we take the official definition of "autonomy" meaning. According to Cambridge dictionary [11], autonomy is : "the right of an organization, country, or region to be independent and govern itself ", and "the ability to make your own decisions without being controlled by anyone else", and the 3rd definition according to American Dictionary [11] is "the right of a group of people to govern itself or to organize its own activities". By extrapolating these deffinitions to Level 5 in industry, or civilian application, or economics, or, why not military organisations, the logical diagram will be as per Figure 5 b.



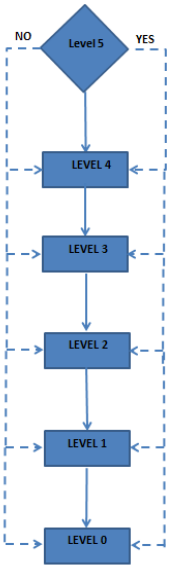


Figure 5:
a) Logical diagram of the operational decision in automation systems implemented today; b) Logical diagram that also include Level 5 of automations.

The particularity and the big difference between automation systems in industry and AI's systems in industry is that the final decision are taken by people based on reports generated by level 2, 3 and 4th of automation systems.

What needs to be emphasized is that the choexistency of all levels of automations, process operations, decision making processes and so on, can be, in the future, dictaded by autonomous systems which includes very complex AI alghoritms that play the "alpha" role and the others components havind the "betta" play-role.

The applyed techniques of AI's in different sectors. Military domain vs. industry sector

Depends on the goal, different techniques and mathematical algoritms can be applied. According to Lawrence Lewis on "AI and Autonomy in War: Understanding and mitigating the risks" [12][13], the AI techniques have the task to recognize statistical relationship inside the Data Sets, and are commonly employed to do: [12][13]

- Processing large and complex data set (Big Data approach);
- Predicting behaviour;
- Flagging anomalies or event of interest;
- Automating tasks;
- Identify important data and error correction.

The main functions that encurrage the use of AI's to support military sector are overviwed herebelow [13], and the existing taxonomy by application of military application are listet in Figure 6.

- Fast analysis and action;
- Performing autonoumus task;
- Controlling robotic and autonomous systems;
- Pattern recognition to predict future trends and detect anomalies;
- The recognition and classifications of objects and/or signals;
- Optimization to achieving the goal;
- Improving the quality of decision-making.

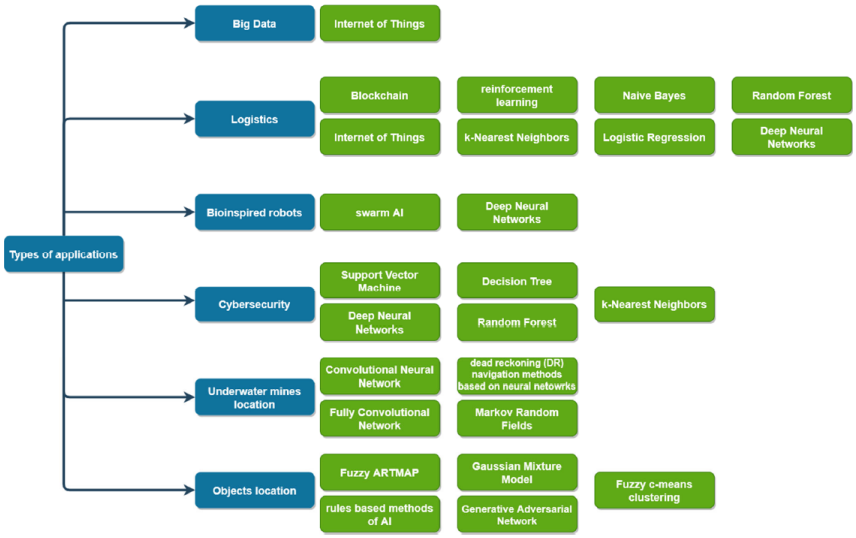


Figure 6: The classification of AI techniques in military applications. [5]

The classification by steps of implementation in industry and military domain examples, can be found in the table below:

Table 1: Industry vs. military application example.

Steps	Methodology	Industry example	Military example
Logical Analysis	Description of the logical relationship between the PREDICTORS and the TARGET.	PREDICTORS: Level of Production, Process parameters, Laboratory analyses + raw materials, energy costs etc. TARGET: Quantities, Qualities, Cost, etc.	PREDICTORS (for both defender and agressor): Manpower, Airpower, Land Forces, Naval Forces, Natural Resources, Logistics, Financials, Geography, etc. TARGET: Sovereignity defence (related to defensive military losses)
Data acquisition	SMALL DATA - accessible, synchronised, concise, precise and workable.	Supervisory control and data acquisition (SCADA)	"Historical + live data"
Statistical processing and interpretation of data	Correlation coefficients (direct/inverse proportional mathematical relationship) + minimum and maximum limits, average, median, etc.	Order of magnitude for correlations between Level of production and the Raw materials + energy costs according Business Plan.	Classification level of correlation between causal military resources and sovereignity defence.
Mathematical modeling in accordance with the Logical Analysis	Regression algorithms (best fit line - most precise numerical value) Classification algorithms (decision boundary forecast YES/NO, Good/Bad, etc.)	Applying Liniar Regression, Polynomial Regression, Neural Network, Random Forest, AdaBoost, etc., in order to obtain the most accurate model of the variability of the raw materials and energetical consumptions and costs.	Applying Liniar Regression, Polynomial Regression, Neural Network, Random Forest, AdaBoost, etc in order to obtain precise modelling between military defender losses and milittary agressor losses.
Descriptive / Predictive Analytics	Monitoring by correcting the deviations / Forecasting by planned PREDICTORS	Monitorization / Prediction of quantities, energies, costs.	Monitorization of different available military resources. Prediction of the defender and agressor military resources.
Prescriptive Analytics	Simulating conditions to minimize/maximize target objectives	Minimising production costs by imposing optimum process parameters according to the physico-chemical proprieties variability of the raw materials available on the market.	Simulating different scenarios of using the avalable military resources in order to discourage the agressor.
Action plan DOE - design of experiment DOR - defense operations research	Implementation of human / autonomous decision making rules	Optimising business decisions and process rules according production cost vs product selling cost (business plan / profit by data driven).	Optimising defensive military resources by maximizing the losses of the agressor.

Mathematical alghoritms applied for decisional management of one equipment. Study case example from industry.

The heavy industry may have secondary by-products components resulted from factory processes, as steam. To not be wasted the extra quantity of steam can be used to produce electrical energy. The data are generated for 6 months and the simulation was done in an open-source software, Orange Data Mining. Orange is an powerful platform that perfrom data analysis in all domain where Machine Learning techniques are suitable.[14]

Probabilistic theories are included in the process of ML and a machine can use such models to make predictions about future data and rational decision given by these predictions.[15]

The scope of the study was to apply two differents methods to identify the optimal production targeted (7MW) for a Turbogenerator (TG) that produce electricity from steam resulted from other processes on the productions lines.

In Figure 7 it is detailed the workflow created for this study in Orange data Mining platform from Data Source to final results.

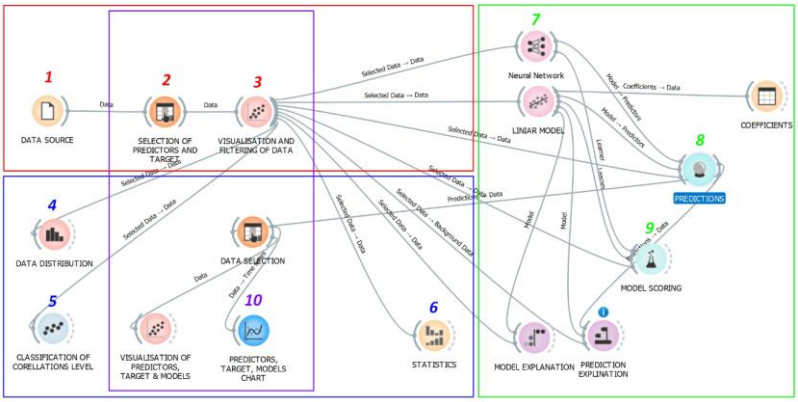


Figure 7: Workflow for TG case study

The inferential statistics is used because it uses less data than descriptive statistics, and it is used for estimation and underline conslusions on the Data Sets we own based on hypothesis testing methods.

In the next figure, the simulation resuts are presented, by using two different methods: multiple linear regression and neural network.

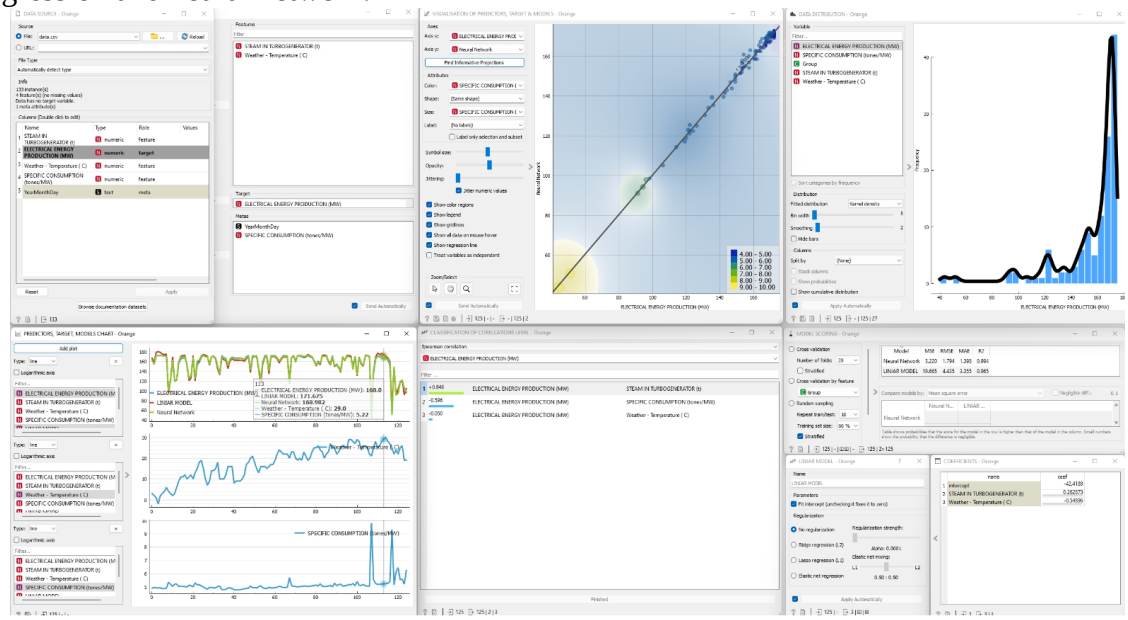


Figure 8: Simulation results

The simulation returned the following indicators from inferential statistics:

1. Multiple linear regression
- MSE (Mean Square Error) = 19.665
- RMSE (Root Mean Square Error) = 4.435
- MAE (Mean Absolut Error) = 3.355
- R2 (R-Squared – Coefficient of determination) = 0.965

2. Neural network
- MSE (Mean Square Error) = 3.220
- RMSE (Root Mean Square Error) = 1.794
- MAE (Mean Absolut Error) = 1.398
- R2 (R-Squared – Coefficient of determination) = 0.994

Given these results, we can already tell that neural network method is more precise regarding the deviations and the proposed target from the biggining (7MW production of electricity) can be achieved by applying the optimal control to steam flow in correlation with external temperature. More than this, for process engineers the temperature can also be called a "global causal predictor" due to the implication it has on all the industrial equipment functionalities and physico-chemical processes.

Conclusions

According to the simulations of 6 months data set, the TG can produce 7 MW by controlling the steam quantity depending on external temperature. In the models was used two predictors: external temperature and steam consumption, and one target: quantity of electricity produced. This study is a basic example of data analysis in industry sector by using multiple linear regression and neural network. Many other and more complex analysys are possible to implement if data are available.

This kind of analysis can be done in any domain if the target is to optimize a process by optimize the resources.

Today, with these advanced mathematics techniques, more than ever, the available data and the available mathematical solutions proves their power to meet the goals, and the future will show us in what level of decision we will be in the future.

References

1. Rockwell Anyoha,(2017). *The history of Artificial Intelligence,* Harvard University, Special edition on Artificial Intelligence, https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/
2. A. M. Turing (1950). *Computing machinery* and intelligence Mind 49, 433-460
3. Empowering AI leadership: AI C-Suite Toolkit, (2022), World Economic Forum, Geneva, Switzerland
4. Istvan Szabadfoldi, (2021), *Artificial intelligence in military application – opportunities and challenges*, Land Forces Academy Review, vol. XXVI, No. 2(102)
5. Marta Bistron, Zbigniew Piotrowski, (2021), *Artificial intelligence application in military systems and their influence on sens of security of citizens*, Electronics, 10 (7), 871. https://doi.org/10.3390/electronics10070871
6. Jorgen Frohm, Veronica Lindstrom, Johan Stahre and Mats Winroth, *Levels of automation in manufacturing*, (2008), Ergonomia – International journal of ergonomics and human factor, vol. 30, issue 3, https://www.researchgate.net/publication/255793362_Levels_of_Automation_in_Manufacturing
7. https://www.oed.com/viewdictionaryentry/Entry/271625
8. Jose Luis Garcia Virgil, *Reflection on ethics, human intelligence and artificial intelligence (AI)*, (2020), Journal of Biology and Today's World 2020, Vol. 9, Issue 11, 001-002
9. *https://www.elementsofai.com/*
10. Natalie M. Scala, James P. Howard II, *Handbook of military and defence operations research,* (2020), CRC Press by Taylor & Francis Group, ISBN – 13:978-1-138-60733-0
11. *https://dictionary.cambridge.org/dictionary/english/autonomy*
12. Lawrence Lewis, *AI and Autonomy in War: Understanding and mitigating risks*, (2018), CAN Analysis & Solutions, http://www.cna.org/CAN_files/PDF/DOP-2018-U-018296-Final.pdf
13. Peter Burt, *None too clever? Military applications of artificial intelligence*, (2021), Drone Wars UK, https://dronewars.net/wp-content/uploads/2021/12/DW-None-too-clever-full-web.pdf
14. *https://orangedatamining.com/*
15. Zoubin Ghahramani, *Probabilistic machine learning and artificial intelligence*, (2015), Nature 521 (7553):452-459, DOI: 10.1038/nature14541

THE SECURITY CULTURE WITHIN ORGANIZATIONS AND ITS RELATIONSHIP WITH INDIVIDUAL SECURITY OF EMPLOYEES IN THE CYBERSPACE

Gârdan S. Daniel Adrian, Uță M. Cristian, Hurloiu M. Lăcrămiora-Rodica, Hurloiu I. Ion-Iulian, Ghiorghiță V. Eugen

Economics Department, Spiru Haret University,Bucharest, Romania, se_gardand@spiruharet.ro,

***Abstract**: The concept reffering to information security represents a very complex one today, taking into account the tremendous changes that are occurring with high speed in the socio-economic environment. When we are talking about the security of data and information we cant afford to resume it only to the safety of the information content itself and the preservation of the value of information. We have to become more and more aware about the dangers, difficulties and challenges related to personal, individual security of the employees work and outcomes of their activities within organizations. The present paper tries to emcompass this very issue – how the presence of the employees into the cyberspace, along with the one of the organizations needs to be securized in front of all the complex form of cyber-attacks and other forms of dangers that can affect not only the productiveness of the employees but the very security of the company itself. The two dimensions of individual and organizational security are entangled and have to be considered in an equal manner a priority for the modern organizations management.*

***Keywords**: security* culture, individual employees security, security perceptions, cyber-space

Introduction

The strength and stability of an organization are the result of the effective protection of general values such as: information, resources, products and, last but not least, personnel. Thus, the protection of personnel is approached through the prism of the formation of competences, skills, the accumulation of experiences, as well as the image projected in the public space. Strategic resources of the companies in terms of intellectual capital and resources to innovate and make efficient research and development activities are relying on the quality of the human resources involved in such activities, but, in an equal measure on the capacity of the organization to develop and apply strong and efficient security information policies, standards and practices.

Research in the field shows that, while security attacks are either internal or external, 66% of computer attacks for example in Greece come from employees within organizations (Siponen, M., Pahnila, S. &Mahmood, A. 2007).

So becomes clear that, in order to assure information security is essential to deal with a certain type of behavior and involvement of the employees on this matter. Thus the success of information security appears to depend, in part, upon the effective behavior and understanding of the individuals involved in its use. From this point of view, every organization have to encourage an constructive behavior of the end users and system administrators that can improve the effectiveness of information security.

Human behavior is complex and multi-faceted, and this becomes more complicated in organizations whereas their culture defies the expectations for control and predictability that developers routinely assume for technology. Many factors like the lack of information security awareness, ignorance, negligence, apathy, mischief, and resistance are the root of users' mistakes that can affect the level of infor-

mation security within the organization. The present paper highlight the fact that investments in security information systems, procedures and resources has to be combined with a constant effort to build awareness of the employees regarding the need of information security and other measures meant to assure also the protection for the individual employee in front of cyber-attacks and other forms of dangers presented in the cyberspace.

1. Information security culture – a necessity for modern organizations

Modern organizations are confronted with many negative factors from the internal or external business environment. Amongst them, elements that can affect the information security are diversified and need a proper analysis in order for companies to be able to manage and contain their negative effects at the level of their performance.

An interesting approach that affords companies management to integrate security policies and actions within the general business strategy refers to the development of a certain information security culture. Information security culture can be considered embedded into the corporate culture and defines the way in which employees see the organization from the point of view of security policies issues (Hacker, J. V., et al, 2019).

A lot of scientific authors that are dealing with organizational culture share the common belief that a strong organizational culture can enhance the organizational performance (Koskosas, I., 2008). This hypothesis stem from the idea that an organization with a well defined and clear transmitted organizational norms and values, will have the neccesarry prerequisites for a superior performance. This can be achievedthrough:

- The enhancement of coordination and control within the organization
- The improvement of goal alignment between organization and its members
- The improvement of employee efforts

Taking account of all the above we can presume that, the organizational culture implies an entire system of learned behavior which will be reflected in a certain level of end-user awareness and which will have an effect on the success or failure of the information security process. Different research shows that users employees are considering that an approach that is more user-involving is much more efficient when it comes to rise the user awareness and behavior regarding information security (Dhillon, G., Smith, K., & Dissanayaka, I., 2021).

Al-Emran et all suggests that proper security gains can be obtained through strengthening security culture, a fact that is influencing in the same time the employees security behavior (Al-Emran, M., 2018).

There can be different approaches when we talk about improving the quality of policies in information security governance: organizations can have the solution based on outsourcing the security information management with the augment of security procedures (Benishek, L. E., & Lazzara, E. H., 2019). or to implement a model based on the Direct-Control Cycle for improving the quality of organization security.

An equal importance has the software development phase, in which, a proper approach can gain improvements in the information security for the company as a direct results of the work made by software developers (Diesch, R., Pfaff, M., & Krcmar, H., 2020).

In their effort to improve information security activities, companies can adhere to a model that highlights the importance of information security policies for the employees starting from the threat appraisal, importance of self-efficacy and response efficacy when employees are trying to comply with information security policies (Eling, M., McShane, M., & Nguyen, T., 2021).

Culture is a perception of organizational norms and values and so it exists within the organizations, not in the individual. To this end, individuals with different backgrounds or at different levels in the organization may tend to describe the organization in similar way. Security culture is used to describe how members perceive security within the organization. Since security and risk minimization are

embedded into the organizational culture, all employees, managers and end-users must be concerned of security issues in their planning, managing and operational activities (Nasir, A., et al, 2019).

The capacity of the organization to put in place a system capable to ensure effective and proactive information security, is dependend by the degree in which all staff is able to actively participate and not to resume to be a rather passive observer of information security. In doing so, staff must strongly held and widely share the norms and values of the organizational culture in terms of information security perception activities.

If the respective organization is managing classified information, the behavior of the staff must fall within the standards, guidelines and procedures established by the security policy. From this point of view, an important role is played by the security culture, the correct sizing of which must take into account a dynamic and continuously developing information environment, marked by misinformation, manipulation, intoxication, cyber espionage, media campaigns, etc.

The security culture is strengthened through the education of each individual, regardless of the position occupied by him in the hierarchy of an organization.

Awareness establishes a common basis for understanding security throughout the organization and focuses on security elements and challenges that employees need to understand and internalize. Each employee must understand their security responsibilities as well as vulnerabilities that can generate loss, fraud or unauthorized activity. All members of the organization, from senior management to interns, must have the same level of understanding of security issues. The awareness program must be in agreement with the security policy and the incident response plan so as to allow the evaluation of the effectiveness of the damage reduction procedures in crisis situations.

The degree of development of the security culture is also dependable on the type of informational system used by the organization along with the information one. The difference and common elements of the two types of essential systems can be seen in the table below:

Table 1. Information system vs informational system at the level of modern organization

Criteria	Information system	Informational system
Components	-hardware equipment for data storage and processing (computers); - software programs necessary for processing and disseminating information within the organization (data transmission systems); - processed data; - the theories underlying processing algorithms, etc	- data and information - the primary components of IS; - information flows - the amount of information; - informational circuits - the route that information takes; - informational procedures - the set and sequence of data processing elements; - information processing means - technical elements - data entry materials.
Features	- contains procedures and techniques for obtaining and disseminating information; - allows automatic data processing; - the IT system intervenes between the decision-making and the operational system.	- generate data and information; - ensures a rule at organizational and managerial level; - integrates the IT system and the organization's resources.
Beneficiaries	- the direct beneficiaries of the system; - the specialized staff who design/implement it.	- the organizational system; - the managerial system
Types of systems	- centralized IT system; - decentralized computer system, etc.	Systems of: - management of classic administrative processes; - administration of contracts; - meeting management; - human resources management; - quality management; - procurement management;

		- document management, etc.
The report information system - computer system	The information system is an essential component of the informational system, being the computer solution and the hardware components	The information system includes the computer system.
The role in the organizational framework	role of organizing internal activities within the prescribed functionalities	- generates and provides data and information for top management regarding the activities carried out in the organization - contributes to efficient internal organization (from the perspective of human, financial, economic resources, etc.); - has a complex of functions and adaptable options

Source: adaptation from (Petrov, C. C., & Petrov, A. (2017). Necesitatea sistemelor informaţionale in activitatea de succes a organizaţiei. In Teoria şi practica administrării publice (pp. 504-512).)

The new challenges of technology

If employees do not understand the need to apply security policies and standards, they will not feel compelled to apply them. The verification of the level of awareness, training and security education necessary at the level of the organization must be carried out constantly, based on specific criteria. Training efforts must be updated and correlated to the way the organization evolves over time, adopting new methods and means of work. Currently, the training of an organization's staff must be updated in accordance with the evolution of online communication technologies, because, in addition to the advantages that the Internet offers us, we must be prepared to face certain challenges characteristic of this field, which has become an integral part of professional activities, but also those carried out during free time. From this perspective, security education does not only aim at the professional activity carried out for the benefit of the organization, but also at the behavior that must be adopted outside the program hours.

Regardless of the place or the devices used when we navigate in virtual space, the projective behavior must remain as rigorous.

Threats for individuals security within the cyberspace

Dark Web dangers

The security environment is strongly influenced by the informational development that we have been going through in recent years, which is accompanied by unconventional challenges.

Among the new vulnerabilities, risks and threats are those propagated in the Dark Net or Dark Web area. If this part of the Internet can be a source of knowledge through data and information useful to mental government organizations or researchers in various fields, it can also become a source of security challenges due to the anonymity it offers.

A major challenge is using the Dark Web, though. accessed out of mere curiosity, to avoid tracking users by websites or to access web pages blocked in a certain country. However, just like the visible network, we must always remain vigilant and follow basic security rules, such as: updating the operating system and applications or avoiding opening or downloading some files whose origin we do not know. Also, we must not reveal personal or sensitive information in the dark web environment. The Dark Web is www (World Wide Web) content available on networks that can only be accessed using specialized browsers. Dark Web pages and sites are not indexed. by standard search engines and used by users who, for various reasons, want their Internet activities to remain anonymous.

Illegal markets and espionage

In general, the Dark Web is associated with illegal activities, an example being DarkMarket, the largest illegal market in the virtual environment, which had approximately 500.000 users in 2020. It was closed after a joint international action by the authorities in Germany, Australia, Denmark, Moldova, Ukraine, Great Britain and the USA. The German authorities have identified 20 servers of this trading platform, located in the Republic of Moldova and Ukraine. This market was also used by Romanian citizens. The case of a fellow countryman who purchased drugs from Belgium and the Netherlands through DarkMarket and who was caught in the act following an action by the police and DIICOT prosecutors is known. in February 2019.

Cyber espionage can also be included in the field of activities found in the hidden area of the Internet.

In November 2014, a cyber security company made public the results of an investigation into the DarkHotel group, a complex network of cyber espionage targeting hotel tourists. The attacks targeted the business environment, but also politicians, with the aim of stealing information of strategic importance for a certain state, state secrets and data with high commercial value.

The DarkHotel operation, which took place around the globe for about 10 years, aimed both at obtaining substantial financial gains and at stealing classified information. in this case, the hackers exploited the facilities of the Wi-Fi service made available to customers by hotel units from several countries. Under the guise of updating widespread applications, cybercriminals would deliver seemingly legitimate packages that had malicious code attached. The hackers had managed to break even the certificates that guaranteed that the data came from a reliable source.

The way in which this operation is carried out highlights the vulnerabilities that appear in the absence of connecting to the Internet through a secure source.

Safe navigation

It is very important that appropriate security measures are taken when accessing a site from the Dark Web, but it should be known that, regardless of these, guaranteeing anonymity is unlikely.

One of the necessary measures is subscribing to a VPN (Virtual Private Network) service and using secure servers, which help preserve online privacy, protect identity and data transmitted from a device. The VPN service should meet some minimum criteria: come from a country that does not require data retention (for example, NordVPN from Panama or SurfShark from the Virgin Islands), be compatible with the majority of online devices and platforms, ensure good encryption and have no logging policies. Another measure is to use a private browser, protected by a digital signature, which is constantly updated. However, using such a browser, although it masks the entity, does not hide the location.

Disposable e-mail addresses should also be used, such as those provided by the services ProtonMail, TORbox, Eluda, etc.

Special attention must be paid to the content distributed on the Dark Web, because a malicious code can be hidden very easily in any type of file. To increase the safety of the user, it is necessary to use a virtual machine (a program that simulates the operation mode and architecture of a computer) to isolate the downloaded files from the rest of the operating system.

Hidden information

The Dark Web can be used to find a court case from a certain state or academic journals, to support investigations related to the trade in narcotics, firearms, medicines, etc. or on human trafficking, in hidden websites and wiki-lists. But, regardless of the reasons that lead us to navigate the Dark Web, we must be aware of the fact that there are many dangers in this environment, and the experience of accessing some content can be even traumatic.

The operations carried out by the authorities in the Dark Web area allow the monitoring of cyber-crime, but also the identification of new technologies and methods used in other criminal activities.

The attention we pay in real life to the things we do or say must be kept to the same extent in the virtual environment, regardless of whether it is in the visible or the hidden part of the network.

The Internet is part of the daily reality of our lives, and our communication and interactions must be adapted to protect general security values. From this perspective, the Dark Web must be used knowingly and with great discernment.

References

1. Al-Emran, M., Mezhuyev, V., Kamaludin, A., & Shaalan, K. (2018). The impact of knowledge management processes on information systems: A systematic review. International Journal of Information Management, 43, 173-187. https://doi.org/10.1016/j.ijinfomgt.2018.08.001
2. Benishek, L. E., & Lazzara, E. H. (2019). Teams in a new era: Some considerations and implications. Frontiers in psychology, 10, 1006. https://doi.org/10.3389/fpsyg.2019.01006
3. Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. The Journal of Strategic Information Systems, 30(4), 101693. https://doi.org/10.1016/j.jsis.2021.101693
4. Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. Computers & Security, 92, 101747. https://doi.org/10.1016/j.cose.2020.101747
5. Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. Risk Management and Insurance Review, 24(1), 93-125. https://doi.org/10.1111/rmir.12169
6. Hacker, J. V., Johnson, M., Saunders, C., & Thayer, A. L. (2019). Trust in virtual teams: A multidisciplinary review and integration. Australasian Journal of Information Systems, 23. https://doi.org/10.3127/ajis.v23i0.1757
7. Koskosas, I. (2008). Goal setting and trust in a security management context. Information Security Journal: A Global Perspective, 17(3), 151-161. https://doi.org/10.1080/19393550802290337
8. Nasir, A., Arshah, R. A., Ab Hamid, M. R., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. Journal of Information Security and Applications, 44, 12-22. https://doi.org/10.1016/j.jisa.2018.11.003
9. Petrov, C. C., & Petrov, A. (2017). Necesitatea sistemelor informaţ ionale in activitatea de succes a organizaţ iei. In Teoria şi practica administrării publice ,pp. 504-512
10. Siponen, M., Pahnila, S. and Mahmood, A. 2007 Employees' Adherence to Information Security Policies: An Empirical Study, In: IFIP International Federation for Information Processing, Vol. 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Eloff, M.,Labuschagne, L., Eloff, J. von Solms, R., (Boston: Springer), pp. 133-144

THE ROLE OF MOTIVATED EMPLOYEES IN CREATION OF COMPETITIVE ADVANTAGES THROUGH INFORMATION SECURITY WITHIN MODERN ORGANIZATIONS

Gârdan S. Daniel Adrian, Duda I. Iordan Gheorghe Iosif, Gârdan I. Iuliana Petronela, Andronie I. Mihai

Economics Department, Spiru Haret University, Bucharest, Romania, se_gardand@spiruharet.ro,

***Abstract**: We face all togheter tremendous challenges today due to the technological development on one hand and due to many complex and interlinked social, political, economical and even biological events and factors on the other hand. Mankind is forced to find creative solutions capable to bring peace, safe environment and equilibrium for the future generations to come. From the point of view of IT development and implementation of modern digital interfaces within different organizations we can highlight the importance of the information security in every form that we can talk about – preservation of data integrity, secure channels of comunication, security protocols, and maybe the most important one – the staff involvement and the integration of information security within the organizational culture.*

Any organization is involved in a particular environment in which develops diversified relations with other actors. From the point of view of business type organizations, these relationships are coaggulated around the idea of exchange and market integration, the need to develop competitive advantges being a constant one. Employees that are fully motivated and implied in a organizational culture that embraces the importance of information security can contribute substantially to the creation and preseration of competitive advantges build or relied on the sensible, confidential business information.

***Keywords**: data security, competitive advantages,employee motivvation, organizational culture*

Introduction

Inovation becomes a necessity for every organization in XXI century because of the high level of competition, undefined types of customers, the large range of products available on the market, and the tremendous speed of information. Actually within their efforts to preserve their customers loyalty, and a certain positioning on the market, companies are forced to search, identify, develop and maintain a range of competitive advantges in front of the competition. The term competitive advantage was first used by Porter in 1985 (Rua, O. L., & Santos, C., 2022). Despite the popularity that this concept has gained over time and the huge amount of scientific literature reffering to it, still it is problematic to be defined because of the complexity of factors that can be taken into consideration.

We may consider that a specific competitive advantage for an organization is achieved when that organization has the capability to develop or to gain a specific set of elements (being attributes or actions) that put it into the position to outperform its competitors (Ma, H., 2000). Thus, competitive advantage becomes clear when the output of a certain specific organization is more profitable that those of the competitors from its market, meaning that this organization is able to be better in terms of market share, product quality or technological advancement (Ávila, M. M., 2022).

Modern organizations can find various sources of competitive advantages – some of them relying with the production process, very innovative materials or energy sources; others with the supply chain – new and improved ways to transport products, delivery methods; others when it comes to the marketing communication techniques or sales strategies. Despite the large area of these possible sources of competitiveness, innovation and the proper integration off strategic resources with a specific human resources management strategy remains a powerfull source of sustainable competitiveness. (Urban, J., 2022). Encouraging the employee involvement in every process that can use their creativity and new approaches makes the organization capable to grasp a lot of data that can be used for applied innovation, that finally can be transformed into competitive advantages. The business objectives and the strategic short, medium and long objectives can be achieved through the implementation of a human resources management approach that is structured as follows (Urban, J., 2022):

- Long term human resources vision relying on basic values and credo of the company – used as the basis for the employees motivation and communication strategy
- Medium-term human resources prerequisites that can achieve the strategic business goals of the company
- Critical analysis of the current human resources status of the organization highlighting the strenghts and weaknesses of the organization as well as the development trends
- Specific human resources management goals for the company, along with human resources policies, different variants and the proper way to evaluate these
- A tactical plan, with specific sub-tasks, deadlines and responsabilities associated with them. Ussualy these sub-tasks being assigned to individual departments and persons

In the present time, organizations may vary as regarding their approach and particular focus of their human resources management system. Thus we can talk about organizations that are emphasizing control or commitment (Madhani, P. M., 2021).

In the first case, actually we have a traditional type of human resources management system based on rules, procedures, extrinsic types of motivation – reward or punishment, close employees monitoring. In the second case, human resources management systems that are emphasizing the commitment are considered high-performance work systems capable to invest in training, career opportunities, higher wages, and employee benefits. We cannot consider control type human resources management systems as being by default obsolete and with a low level of efficiency, but many organizations that are stick with this type of system are having a kind of vicious circle – they are not capable to improve profit margins and market position because they do not invest in trening and other benefits that could stimulate employees to develop eventualy more intrinsic motivation while doing their tasks. Commitment based organisations are communicating to the employees the fact that they have long term carrer opportunities and not merely short-term engagement like internships, so they engagement could rise exponentially. In this way also the turnover rates are reducing and the costs with identification of new proper employees are lower (Madhani, P. M., 2022).

In order that engagement of the employees and their motivations transform in sources of competitive advantages, organizations actually have to empower these employees. The process of empowerment is reffering to giving to the employees the power, authority, responsibility, resources, freedom to take decisions and to find out the solution to the work-related problems in the organisation (Sunny, K. G., & Yajurvedi, N., 2022).

The present aticle stressed out the ideea that one source of sustainable competitive advantages for modern companies is the involvement of employees in the process of information security that allows for the company a strict control over confidential business information, decisional outcomes, promotional strategies or other instruments needed to gain advantages on the market.

Data security and its importance in modern organizations

Nowadays, the recognition of the omnipresence of information in human activities is a common fact. Information and communication technology, from the personal computer to the Internet, from the mobile phone to the global communication networks, is in full development and is transforming our lives, relationships, and the organization of society.

We can talk about the birth and development of a entirely new space based on all these technologies and factors that are managing the flow of information: the virtual space – cyberspace. The notion of cyberspace was launched for the first time by William Gibson - Canadian science fiction writer - in 1982, through the short story Burning Chrome, published in Omni magazine (Stepanov, E., 2016).

The emergence of the alternative space, called cyberspace, replaced traditional activities and generated certain principles of action, virtual navigation and use of online opportunities, which, all together, formed the so-called cyberculture.

Cyberculture is a global phenomenon that represents the totality of relations in the field of IT technologies, which includes, among others, the culture of information dissemination and assimilation, as well as the culture of communication through virtual networks. Due to its psychosociological importance and relevance, it has become an object of study for the social sciences. În principle, cyberspace should not be confused with the real Internet (as a network), but should be seen as summing up the psychological and social aspects that the individual human psyche and society as a whole give to it through use.

Therefore, cyberspace includes the identities and objects that exist in computer networks used by human individuals for various purposes. For example, a website can be said to be in cyberspace when the activities carried out by the people who access it online, detached from its physical geographical location, become online events, therefore of cyberspace. Events in cyberspace interact closely with events in the real world, as individuals and supra-individual entities such as corporations, organizations, and institutions inform, communicate, organize, work, and make decisions about real life online. The use of communication networks by human individuals clearly gives cyberspace, in addition to its purely operative and organizational component, oriented towards solving certain tasks, an emotional valence, which humanizes it.

Currently, there is an increasingly accentuated dependence of socioeconomic entities, public and governmental institutions on the IT systems that largely manage their resources, but especially the communication of information essential to organizational existence and development, making them increasingly vulnerable to the impact that cyber threats can have against IT environments.

Most frequently, computer crimes are aimed at:

- the private life of social individuals: affecting their personal data;
- the economic field: affecting the activity, security and economic competitiveness of firms and companies;
- national security: affecting the operation of critical infrastructures, government, defense and national security networks and systems.

Simultaneously with the increase in the use of ICT, the number of threats, attacks, frauds, computer crimes, the number of affected organizations and persons, who express their dissatisfaction and who are interested in the safe operation of the terminals connected in such networks, also increases considerably.

Networked corporations and individuals face various major difficulties, risks and challenges, including (Bragaru, T., Malcoci, V., & Galaicu, V., 2017):

- The modern informational infrastructure, based on computer networks, is becoming more and more complex.
- The increased level of inter-dependence of businesses and people on modern ICT, can lead to the situation in which a possible failure in the field of ICT can cause business failure. The viability time of any processes and activities when the ICT services are down has been considerably reduced.

- The ease with which data can be processed, transported and intercepted in networks; anonymity of activities in the network; the immaterial character of the information; the independence of supporting data, the possibilities of malicious manipulation of systems, applications and data in networks, etc.

So it becomes obvious that, in order to manage in an efficient way all these possible threats and challenges related with the security of data, the companies need a proper system that can assure not only the integrity and security of physical information but also safe procedures, safe transfer of the data and safe acces of the right employees to different categories of information.

In the conditions of fierce competition, which currently exists on the market, at different levels, organizations aim to improve the efficiency of internal organization, trade, transaction, communication and other types of activities, more general or more specific, by using information systems, as management levers. Each company, depending on needs and priorities, implements and develops information systems in order to automate the processes of operating with data, providing data and information, so useful in the conditions of a modern society. Most of the time, companies opt for easily adaptable information systems from a technical and operational point of view, in order to be able to make changes and complete with new functionalities at any time depending on the new circumstances and needs of the organization (Bragaru, T., Malcoci, V., & Galaicu, V., 2017).

In order to remain competitive, large industrial companies, banks, government institutions, telecommunications, media, Internet providers or companies with headquarters distributed in the territory, need a perfect integration of the various branches and warehouses with the central offices. major investment in information technology and communications infrastructure leads to an increase in performance indicators that measure profit, work efficiency, return on investment and service quality. Productivity and revenues resulting from the sale of products and services increase significantly. The integration of different production centers within an organization reduces the total maintenance costs, and the improvement of accounting procedures and the systematization of resources lead to the improvement of the market position. Information and communication technologies, in general, and information systems, in particular, have become widely used tools by today's organizations. In the existing competitive environment, companies advocate for mechanisms to make their activity more efficient. Management processes are combined with information systems, which play a supporting role for decision-making and execution activities.

Employees motivation – strategic tool for competitiveness

The bond between employees motivation and company competitiveness is certified by an extensive body of scientific literature. In order to fully ascertain this aspect is imperative first to defne employees motivation within the organizations accordingly. Thus, seen from a procedural perspective, motivation is a concept that refers directly to a series of "stages" of the manifestation of human behavior in action. In this context, we are talking about motivation seen as a corollary of the factors that determine the initiation of a certain behavior, direct this behavior, establish a certain intensity of it and a certain degree of persistence over time (Bernstein, D.A., et al., 2008).

Also, motivation can be formally defined as representing an indicator measuring the intensity of the constant effort made by a person to achieve a goal (Johns, G., & Saks, M.A., 2007).

It can be observed that both in the presented definitions and in other approaches, the psychology specialists have identified three fundamental elements that help us conceptualize motivation and in perspective the motivation process - persistence, seen as a basic characteristic of motivation - the ability of individuals to it constantly manifests in the direction of motivation, the intensity of behavior, another defining characteristic for motivation, and the direction and objectives - elements of a qualitative nature also present at the level of any motivational process (Pânişoară, G., & Pânişoară, I.O., 2005).

The three dimensions that are the basis of motivation will directly contribute in a synthetic form to the coagulation of individuals' efforts in the direction of reaching a level of performance corresponding to the proposed objectives. Performance can be simply defined as a measure of the degree to which a

member of an organization contributes to the achievement of the objectives of the organization in question.

The relationship between motivation and performance can be highlighted in the figure below:

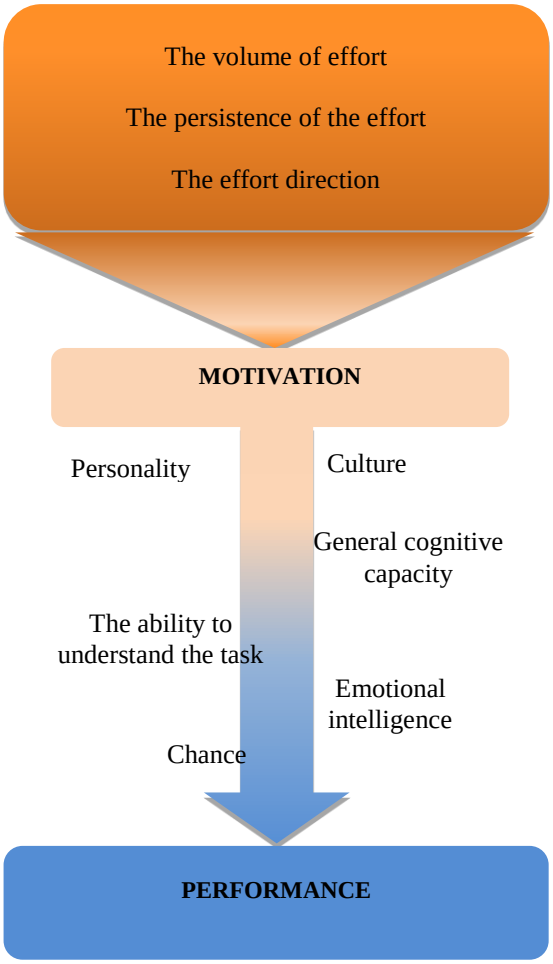


Figure 1: Factors contributing to individual work performance

Source: Johns, G., & Saks, M.A. (2007). Organizational behavior: understanding and managing life at work, seventh edition, Toronto: Pearson Prentice Hall, p. 137

As a conclusion we can highlight some observations regarding the motivation of individuals within organizations:

- the motivation must be in a direct proportional relationship with the employee's skills (without their real foundation, the motivation can represent a process without finality, without tangible results);
- the existing individual differences must be taken into account when choosing reasons within motivation programs;
- direct and indirect motivations must be clearly defined through experimentation;
- the dynamic nature of the reasons must be taken into account (employees face new situations, they can progress or regress);
- eliminating or reevaluating stereotypes regarding motivation.

In the current competitive context in which, for many markets, each company has access to approximately the same types of technology, resources, etc., the capacity for competitive differentiation is very based on the ability to attract and maintain quality human resources.

Human capital optimization is virtually one of the essential goals for each company,

The behavior of the employees is decisively influenced by the culture specific to the organization in which they operate. Organizational culture has been defined as a model of values and beliefs shared by the members of an organization that confer meaning and provide for them the norms of behavior within the organization. If the organizational culture is oriented toward the direction of competitiveness and employees stimulation this can create a proper background for a constant process of developing competitive strategic advantages for the company as a direct consequence of the employees involvement.

According to Aaker, competitive advantages can have two main sources (Aaker, D. A., & Moorman, C., 2017):

1. Exceptional abilities – that actually are in close relation with exceptional competencies of companies' employees ;

2. Exceptional resources – the ones that other organizations do not have.

A competitive advantage can be achieved with a qualified labour force in an organization that encourages competition considering market changes, production and service quality. Thus, the success of any organization depends on the ways in which employee management and strategic business objectives are synchronized. Research in the field have determined some essential features of the management staff characteristics for obtaining competitive advantages (Batarlienė, N., et al., 2017):

- responsible attitude to work and company's image,
- integrity,
- self-criticism,
- the pursuit of quality in performing assigned tasks,
- diligence,
- flexibility.
- A quick and flexible response to innovations and teamwork that can facilitate organizations to respond quickly to customers' interests and competitors' challenges

The same authors are concluding that for majority of companies the main sources of competitive advantages are:quality of services, customer service and competent employees.

Employees involvement in creation of competitivity advantages based on information security

Commitment is defined as a state of mind that holds people and organizations in line of behaviour and encompasses psychological factors that force individuals to take action in effect to information security planning. The successful development of an information system has long been believed to depend on the commitment to a certain project that is dealing with this task. In the situation in which individual and group goals are congruent, group members will be committed to increasing group performance. In the situation in which inside the organization we have low awareness levels, we can ascertain a major need for effective information security. Thus this need to increase security awareness in the perception of all employees and users at all levels, is manifested in terms of task knowledge and familiarity to information security.

In case of modern companies, people are able to make the difference between information technology and security and the specific training that is reffering to the ethical, legal and security aspects of information technology usage that should be ongoing at all levels within organizations. Since people react differently to poorly constructed security messages, communication will broken down and may be confusing from the point of view of task knowledge and security risk awareness among the employees. Thus, the main implication for information security management is to focus on changing attitudes and human behaviour which are part of the organizational culture in order to enhance awareness among the employees about information security task related tasks (Koskosas, I., Kakoulidis, K., & Siomos, C., 2011).

In order to obtain a proper level of protection for the integrity, confidentiality, and availability of information used within its business activities, modern company has to ensure that every person from within the organization is capable to understand correctly his/her roles and responsibilities, and receives accordingly a specific training in order to perform them.

Actually at the level of ISO/IEC 17799 (2000) standards, all employees of the organization and, where relevant, third party users, should receive appropriate training. This training content should include specific information regarding security requirements, legal responsibilities and modalities for business controls. Besides this knowledge, in order to ensure the required efficiency, the training has to be clear about the correct use of information processing facilities, long enough the access to information or services is granted (ISO/IEC 17799, 2000, p.9). It would make sense for an organization's security educational program to cover all the controls specified by the specific information security standard used by the organization. However, it is clearly unreasonable to expect each and every end-user to be educated about all the controls specified by a standard such as the ISO/IEC 17799. Each employee should know his or her role and responsibility, his or her contribution to IT security, and should share the IT security vision.

In the process of training, many times, managers are confronting themselves with a kind of employee resitance to new information. In order to change a learner's values, beliefs, attitudes, or psychological states of mind, more than just education will be required. Adults have well established values, beliefs, and opinions, as opposed to the formative beliefs, values, and opinions of children. In addition to this, adults may have had differing education, varying years of experience, and a wealth of previously learned information (Van Niekerk, J., & Von Solms, R., 2005).

Information security depends on both human knowledge, and human cooperation. A lack of knowledge can generally be addressed through education, whilst a lack of cooperation can be addressed through the fostering of an organizational sub-culture of information security in the organization. However, if employees have adequate knowledge, but lack the required attitude they will not necessarily behave securely. Conversely, employees who have the correct attitude, but do not have the necessary knowledge, will not be able to behave securely. This co-dependency between knowledge and attitude would mean that neither of these factors should be addressed in isolation. Overall, information security should support the mission of the organizations, it must be cost effective and fit into the organizations' culture seamlessly, that is integrate technology, processes and people.

References

1. Aaker, D.A., & Moorman, C. (2017). *Strategic market management,* New York: John Wiley & Sons.
2. Ávila, M.M. (2022). Competitive advantage and knowledge absorptive capacity: The mediating role of innovative capability. *Journal of the Knowledge Economy, 13(1),* 185-210. https://doi.org/10.1007/s13132-020-00708-3
3. Batarlienė, N., Čižiūnienė, K., Vaičiūtė, K., Šapalaitė, I., & Jarašūnienė, A. (2017). The impact of human resource management on the competitiveness of transport companies. *Procedia Engineering, 187,* 110-116. https://doi.org/10.1016/j.proeng.2017.04.356
4. Bernstein, D.A., Penner, L.A., Clarke-Stewart, A., & Roy. E. J. (2008). *Psychology* (8thed.), Boston: Houghton Mifflin Company.
5. Bragaru, T., Malcoci, V., & Galaicu, V. (2017). *Securitatea reţ elelor informatice. Studia Universi-tatis Moldaviae, Seria Ştiinţe Exacte şi Economice, 107(7),* 166-179.
6. Johns, G., & Saks, M.A. (2007). *Organizational behavior: understanding and managing life at work*, seventh edition, Toronto: Pearson Prentice Hall.

7. Koskosas, I., Kakoulidis, K., & Siomos, C. (2011). Information security: Corporate culture and organizational commitment. *International Journal of Humanities and Social Science, 1(3),* 192-195. www.ijhssnet.com
8. Ma, H. (2000). Competitive advantage and firm performance. *Competitiveness Review, 10(2),* 15-32. https://doi.org/10.1108/eb046396
9. Madhani, P. M. (2021). Lean Six Sigma in finance and accounting services for enhancing business performance. *International Journal of Service Science, Management, Engineering, and Technology, 12(6),* 141-165. https://doi.org/10.4018/IJSSMET.2021110109
10. Madhani, P. M. (2022). The "High-Road" Approach to Compensation and Benefits Practices: Enhancing Competitive Advantages. *International Journal of Applied Management Sciences and Engineering, 9(1),* 1-21. https://doi.org/10.4018/IJAMSE.286179
11. Pânişoară, G., & Pânişoară, Ion-Ovidiu (2005). *Motivarea eficientă: ghid practic,* Iaşi: Editura Polirom.
12. Rua, O. L., & Santos, C. (2022). Linking brand and competitive advantage: The mediating effect of positioning and market orientation. *European Research on Management and Business Economics*, *28*(2), 100194. https://doi.org/10.1016/j.iedeen.2021.100194
13. Stepanov, E. (2016). Oportunităţ ile ş i pericolele ciberspaţ iului: abordări conceptuale. In *Valori ale mass-mediei în epoca contemporană*, 176-182. https://ibn.idsi.md/vizualizare_articol/139267#
14. Sunny, K. G., & Yajurvedi, N. (2022). Enhancing The Efficacy of Organisational Competitive Advantage Through Employee Empowerment. *Journal of Positive School Psychology, 6(3),* 5457-5465. https://journalppw.com/index.php/jpsp/article/download/3108/2033
15. Urban, J. (2022). Human Resource Management Strategy as a Small Business Competitive Advantage Tool. In SHS Web of Conferences (Vol. 135). EDP Sciences. https://www.proquest.com/docview/2634542055?pq-origsite=gscholar&fromopenview=true
16. Van Niekerk, J., & Von Solms, R. (2005, July). A holistic framework for the fostering of an information security sub-culture in organizations. In *Issa, 1(13*). https://digifors.cs.up.ac.za/issa/2005/Proceedings/Full/041_Article.pdf

MODERN POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS

Zhaneta N. Savova, Rosen A. Bogdanov

**Department of Computer Systems and Technogies, Faculty of Artilery, Air Defence and Communication and Information Systems/National Military University, Shumen, Bulgaria, zh.savova@mail.bg*
***Department of Communication and Information Systems, Faculty of Artilery, Air Defence and Communication and Information Systems/National Military University, Shumen, Bulgaria, RAB61@abv.bg*

***Abstract**: A foreseeable quantum future capable of breaking the current cybersecurity infrastructure requires the standardization of new post-quantum algorithms. The paper presents the stages of selection of asymmetric cryptographic algorithms in the post-quantum cryptography standardization project announced by NIST in 2016. The four post-quantum cryptographic algorithms selected for standardization are analyzed and their main characteristics are compared in the article.*

***Keywords**: Post-Quantum Cryptography, Public Key Algorithm, Lattice Problem, Stateless Hash-based Signature*

СЪВРЕМЕННИ ПОСТКВАНТОВИ КРИПТОГРАФСКИ АЛГОРИТМИ

Жанета Н. Савова, Росен А. Богданов

Въведение

Едно от големите технически постижения на 21 век е преминаването от теоретични разработки към практически реализации на квантови компютри. Основното предимство на квантовите компютри в сравнение с обикновените е в способността им да извършват многократно по-голям брой паралелни изчисления, като изчислителният им потенциал се увеличава в геометрична прогресия с увеличаването на броя на използваните кюбити. Това ги прави особено подходящи за използване при решаване на задачи в областта на ктиптографията и криптоанализа. Проведените експерименти показват, че квантов компютър, разполагащ с подходящи алгоритми може да разбие за секунди считани за непробиваеми със сегашното ниво на техниката шифри и пароли. Това налага да бъдат изследвани принципите на построение, функциониране, техническите параметри и приложимостта на съвременните криптографски алгоритми, проектирани за изпълнение от квантови машини.

Националният институт по стандарти и технологии NIST към Министерството на търговията на САЩ избра първата група алгоритми за криптиране, които са проектирани да издържат на атаката на бъдещ квантов компютър, който потенциално може да пробие сигурността, използвана за защита на поверителността в цифровите системи, които се използват всекидневно, като софтуер за онлайн банкиране и имейл криптиране. Избрани са четирите алгоритъма за криптиране, които ще станат част от пост-квантовия криптографски стандарт на NIST, който се очаква да бъде финализиран след около две години [20].

През 2016 г. NIST обяви проект за стандартизация на постквантовата криптография, в който призова световните криптографи да разработят и изпробват нови алгоритми за криптиране, които

биха могли да устоят на атака от бъдещ квантов компютър, доста по-мощен от сравнително ограничените изчислителни машини, налични днес [18].

Етапи на избор на кандидатите за постквантови криптографски алгоритми

Обявеният през 2016 г. проект за нови криптографски стандарти с публичен ключ очаква да определи един или повече допълнителни алгоритми за цифрови подписи, криптиране с публичен ключ и алгоритми за обмяна на ключове. Целта е тези алгоритми да разширят стандарта за цифров подпис DSS (FIPS 186-4), както и специални публикации като препоръки за схеми за обмяна на ключове по двойки, използващи криптография с дискретен логаритъм (SP 800-56A Rev 2) и тези, използващи факторизиране на цели числа (SP 800-56B).

През ноември 2017 г. 82 кандидат-алгоритъма бяха изпратени до NIST за разглеждане. Сред тях 69 отговаряха както на минималните критерии за приемане и изискванията за подаване и бяха приети като кандидати за първи кръг на процеса за подбор на 20 декември 2017 г., отбелязвайки началото на първия кръг от процеса на стандартизация на постквантовата криптография на NIST. От тези 69 алгоритъма на основата на обявени критерии за оценка и процеса на подбор въз основа на обществена обратна връзка и преглед от NIST на 30 януари 2019 г. са избрани 26 алгоритъма за преминаване към втория кръг на конкурса [3].

През юли 2020 г. са обявени избраните алгоритми за криптиране с публичен ключ и установяване на ключове от втория кръг на конкурса: Classic McEliece, CRYSTALS-KYBER, NTRU и SABER. Финалистите за третия кръг за цифрови подписи са CRYSTALS-DILITHIUM, FALCON и Rainbow. В допълнение, осем алтернативни кандидат алгоритъма също ще преминат към третия кръг: BIKE, FrodoKEM, HQC, NTRU Prime, SIKE, GeMSS, Picnic и SPHINCS+. [4]

През юли 2022 г. от подадените 15 кандидата за трети кръг на конкурса са идентифицирани алгоритмите, избрани за стандартизация, и тези, които ще продължат да бъдат оценявани в четвъртия кръг. От групата на алгоритмите за криптиране с публичен ключ и установяване на ключ ще бъде стандартизиран CRYSTALS–KYBER. Алгоритмите за цифрови подписи, които ще бъдат стандартизирани, са CRYSTALS–Dilithium, FALCON и SPHINCS+. В допълнение, други четири алтернативни алгоритми за установяване на ключове преминават към четвърти кръг за оценка: BIKE, Classic McEliece, HQC и SIKE [2]. В момента е обявена нова покана на NIST за предложения за алгоритми за цифров подпис с публичен ключ [19].

Избрани за стандартизация постквантови криптографски алгоритми

Както бе споменато в предходната секция, през юли тази година са избрани четири постквантови криптографски алгоритми за стандартизация от NIST, един за криптиране с публичен ключ и установяване на ключ и три алгоритъма за цифров подпис. В секцията последователно ще бъдат разгледани и сравнени техните основни характеристики.

CRYSTALS-Kyber

CRYSTALS-Kyber [6] е неразличим при атака с адаптивно избран шифрован текст IND-CCA2 (INDistinguishability under adaptive Chosen Ciphertext Attack) сигурен механизъм за капсулиране на ключове KEM (Key Encapsulation Mechanism), чиято сигурност се основава на трудността на решаването на проблема с обучение с грешки LWE (Learning-With-Errors) върху решетки по модул. Алгоритъмът предоставя на потребителите три различни множества от параметри, насочени към различни нива на сигурност. По-конкретно, Kyber-512 осигурява сигурност, приблизително еквивалентна на AES-128, Kyber-768 цели сигурност, приблизително еквивалентна на AES-192, а Kyber-1024 осигурява сигурност, приблизително еквивалентна на AES-256.

Дизайнът на Kyber има своите корени в основната LWE-базирана схема за криптиране, предложена от Regev [21]. След оригиналната работа на Regev, практическата ефективност на схемите за криптиране на LWE е подобрена чрез наблюдение, че тайната в LWE може да дойде от същото разпределение като шума [5] и също така забелязването, че "LWE-подобни" схеми могат да бъдат изградени с помощта на квадратна (по-скоро отколкото правоъгълна) матрица като публичен ключ [16]. Друго подобрение беше прилагането на идея, първоначално използвана в криптосистемата NTRU за дефиниране на проблемите Ring-LWE [17] и Module-LWE [14], които използват полиномиални пръстени, а не цели числа. Защитеният от CCA KEM Kyber е изграден върху криптосистема защитена от атака с избран открит текст CPA (Chosen Plaintext Attack). Сигурността на криптосистемата се базира на устойчивостта на Module-LWE проблема. Повече информация относно математическите основи на алгоритъма, неговата същност и криптоанализ е налична в публикацията [10].

CRYSTALS-Dilithium

Dilithium е схема за цифров подпис, която е силно защитена при избрани атаки на съобщения въз основа на трудността при решаване на проблеми над решетки по модул. Идеята за сигурност означава, че противник, който има достъп до подписващия съобщението, не може да генерира подпис на съобщението, чийто подпис все още не е видял, нито да произведе различен подпис на съобщение, което вече е видял подписано.

Дизайнът на Dilithium се основава на техниката „Fiat-Shamir with Aborts" на Любашевски [15], която използва вземане на проби за отхвърляне, за да направи базираните на решетка схеми Fiat-Shamir компактни и сигурни. Схемата с най-малки размери на сигнатурата, използваща този подход, е тази на Ducas, Durmus, Lepoint и Lyubashevsky[11], която се основава на допускането на NTRU и изключително използва вземане на проби по Гаус за създаване на сигнатури. Тъй като вземането на проби по Гаус е трудно за сигурно и ефективно прилагане, се използва само равномерно разпределение. Dilithium подобрява най-ефективната схема, която използва само равномерно разпределение, благодарение на Bai и Galbraith [7], като използва нова техника, която свива публичния ключ с повече от коефициент 2. Доколкото е известно, Dilithium има най-малкия публичен ключ + размер на подписа на всяка схема за подпис, базирана на решетка, която използва само равномерно разпределение при вземане на проби.

Falcon

Falcon е схема за цифров подпис над NTRU базирана на бързо преобразование на Фурие. Falcon е съкращение произлизащо от подчертаните символи в името на алгоритъма Fast Fourier Lattice-based compact signatures over NTRU.

Falcon се основава на теоретичната рамка за базирани на решетка схеми за подписване, предложена през 2008 от Gentry, Peikert и Vaikuntanathan [12]. Авторите на алгоритъма Falcon прилагат тази рамка върху NTRU решетки [13], с така нареченото „вземане на проби с бързо преобразование на Фурие". Основният проблем, определящ сигурността на схемата за цифров подпис е проблемът за намиране на кратко цяло число SIS (Short integer solution) [1] върху NTRU решетки, за който в момента не е известен ефективен алгоритъм за решаване в общия случай, дори с помощта на квантови компютри. Основната цел на проектираната схема за цифров подпис е минимизиране на общата дължина на публичния ключ и цифровия подпис.

SPHINCS+

SPHINCS+ е схема за цифров подпис, базирана на хеш функции. Принципно SPHINCS+ работи подобно на първата схема за цифров подпис без състояния SPHINCS, предложена през 2015 г. [8]. Основната идея е да се удостовери автентичността на огромен брой двойки ключове за малко временни подписи FTS (Few-Time Signature), използвайки така нареченото хипердърво. FTS схемите са схеми за подпис, които позволяват от двойка ключове да се генерират малък брой подписи, например от порядъка на десет в SPHINCS+. За всяко ново съобщение се избира псевдослучайна двойка FTS ключове, с която се подписва съобщението. Подписът се състои от подписа на FTS и информацията за удостоверяване за тези FTS двойка ключове. Информацията за удостоверяване е подпис използващ дърво за сертифициране на подписи с дърво на Merkle. [9]

Информацията за удостоверяване за FTS двойката ключове се състои от d MTS (Many-Time Signatures) подписи, които изграждат път от двойката ключове FTS до върха на MTS дървото. MTS подписът е класически подпис с дърво на Меркел в случая на SPHINCS+. Той се състои от еднократен подпис OTS (One-Time Signature) върху даденото съобщение плюс пътя за удостоверяване в него двоичното хеш-дърво, удостоверяващо автентичността на N OTS двойки ключове на една MTS двойка ключове. Публичният ключ на SPHINCS+ на практика е публичния ключ на MTS от най-високо ниво, който е само възелът-корен на неговото двоично хеш дърво и следователно, една хеш стойност.

Секретният ключ на SPHINCS+ е само една секретна начална стойност. От нея по псевдослучаен начин се генерират всички OTS и FTS секретни ключове. Заедно секретните OTS и FTS ключове напълно определят цялата виртуална структура на двойките ключове в SPHINCS+.

Предложени са 3 схеми на подписване: SPHINCS+-SHAKE256, SPHINCS+-SHA-256 и SPHINCS+-Haraka, които се получават чрез прилагане на конструкцията SPHINCS+ със SHAKE256, SHA-256 и Haraka, съответно.

Като се има предвид гореизложеното, основните характеристики на избраните за стандартизация постквантови криптографски алгоритми могат да се обобщят в таблица 1.

Таблица 1. *Сравнение на характеристиките на съвременните постквантови криптографски алгоритми*

Алгоритъм	Приложение	Математически проблем определящ сигурността	Сигурност и характеристики
CRYSTALS-Kyber	криптиране с публичен ключ и установяване на ключ	трудност на проблема с обучение с грешки LWE над решетки по модул	Kyber-512 ≈ AES-128 Kyber-768 ≈ AES-192 Kyber-1024 ≈ AES-256
CRYSTALS-Dilithium	схема за цифров подпис	трудност на проблеми в решетки над решетки по модул	най-малък публичен ключ + размер на подписа
Falcon	схема за цифров подпис	проблемът за намиране на кратко цяло число SIS	малък публичен ключ + размер на подписа
SPHINCS+	схема за цифров подпис	използване на еднопосочни хеш функции	схемата е без състояния, което й позволява да бъде заместваща за текущата схеми за подписване на съобщения

Заключение

Квантовото бъдеще, характеризиращо се с нарастващ брой теоретични разработки, свързани с квантовите изчисления, и опитите за техните практически приложения в реализации на все помощни и бързодействащи квантови компютри, е способно да разбие настоящата инфраструктура

за киберсигурност. В резултат от необходимостта от стандартизация на нова постквантовата криптография, са избрани 4 алгоритми за асиметрична криптография, които могат да устоят на атака от бъдещ квантов компютър. От анализа на техните основни характеристики може да се направят следните изводи:

1. По-податливи на атаки с квантови изчисления са асиметричните криптографски алгоритми. Затова за стандартизация са избрани един алгоритъм за криптиране с публичен ключ и установяване на ключове CRYSTALS-Kyber и три за схеми за цифров подпис: CRYSTALS-Dilithium, Falcon и SPHINCS+.
2. Новите постквантови алгоритми са базирани основно на два нерешими математически проблема: решетки по модул и прилагане на еднопосочни хеш функции, които определят и направленията за развитие на криптографията.
3. Предложеният асиметричен алгоритъм за криптиране CRYSTALS-Kyber осигурява сигурност, съизмерима със симетричния AES алгоритъм.
4. Изследванията при проектиране на схеми за цифров подпис са насочени към осигуряване на приемлива сигурност при малък общ размер на публичния ключ и на подписа.

References

1. Ajtai, M. (1996, July). Generating hard instances of lattice problems. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 99-108)
2. Alagic G., et al. NIST IR 8413, Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, July 2022, Retrieved from https://doi.org/10.6028/NIST.IR.8413
3. Alagic G., et al. NISTIR 8240, Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process, 2019, Retrieved from https://doi.org/10.6028/NIST.IR.8240
4. Alagic G., et al. NISTIR 8309. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, July 2020, Retrieved from https://doi.org/10.6028/NIST.IR.8309
5. Applebaum, B., Cash, D., Peikert, C., & Sahai, A. (2009, August). Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In Annual International Cryptology Conference (pp. 595-618). Springer, Berlin, Heidelberg
6. Avanzi, R., et al. CRYSTALS-Kyber, Algorithm Specifications And Supporting Documentation (version 3.02), 2021, Retrieved from https://pq-crystals.org/kyber/data/kyber-specification-round3-20210804.pdf
7. Bai, S., & Galbraith, S. D. (2014, February). An improved compression technique for signatures based on learning with errors. In *Cryptographers' Track at the RSA Conference* (pp. 28-47). Springer, Cham
8. Bernstein, D. J., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., ... & Wilcox-O'Hearn, Z. (2015, April). SPHINCS: practical stateless hash-based signatures. In *Annual international conference on the theory and applications of cryptographic techniques* (pp. 368-397). Springer, Berlin, Heidelberg
9. Bernstein, D., et. al., SPHINCS+, (November 2017), Retrieved from https://sphincs.org/data/sphincs+-specification.pdf
10. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., ... & Stehlé, D. (2018, April). CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In 2018 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 353-367). IEEE
11. Ducas, L., et al. (2013, August). Lattice signatures and bimodal Gaussians. In *Annual Cryptology Conference* (pp. 40-56). Springer, Berlin, Heidelberg

12. Gentry, C., Peikert, C., & Vaikuntanathan, V. (2008, May). Trapdoors for hard lattices and new cryptographic constructions. In Proceedings of the fortieth annual ACM symposium on Theory of computing (pp. 197-206)
13. Hoffstein, J., Pipher, J., & Silverman, J. H. (1998, June). NTRU: A ring-based public key cryptosystem. In International algorithmic number theory symposium (pp. 267-288). Springer, Berlin, Heidelberg
14. Langlois, A., & Stehlé, D. (2015). Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography, 75(3), 565-599
15. Lyubashevsky, V. (2009, December). Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 598-616). Springer, Berlin, Heidelberg
16. Lyubashevsky, V., Palacio, A., & Segev, G. (2010, February). Public-key cryptographic primitives provably as secure as subset sum. In Theory of Cryptography Conference (pp. 382-400). Springer, Berlin, Heidelberg
17. Lyubashevsky, V., Peikert, C., & Regev, O. (2010, May). On ideal lattices and learning with errors over rings. In Annual international conference on the theory and applications of cryptographic techniques (pp. 1-23). Springer, Berlin, Heidelberg
18. NIST, Created January 03, 2017, Updated September 06, 2022, Post-Quantum Cryptography Standardization, Retrieved from https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization
19. NIST, Guidelines for submitting tweaks for Fourth Round Candidates, Retrieved from https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/guidelines-for-submitting-tweaks-fourth-round.pdf
20. NIST, NIST Announces First Four Quantum-Resistant Cryptographic Algorithms, July 05, 2022, Retrieved from https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
21. Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6), 1-40

GLOBAL RELIABILITY FOR INFORMATION STORAGE VIA SOLID STATE DRIVE

Daniel R. Denev

Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Bulgaria, d.denev@shu.bg

***Abstract**: This paper presents the first large-scale field study of NAND-based SSDs in global storage systems. The study is based on a very comprehensive set of field data covering 1.4 million SSDs of a major storage vendor (NetApp). The devices consist of three different manufacturers, 18 different models, 12 different capacities and all major flash technologies (SLC, cMLC, eMLC, 3D-TLC). The data allows us to explore a large number of factors that have not been explored in previous studies, including the effect of firmware versions, TLC NAND reliability, and correlations between drives in a RAID system. This paper presents our analysis, together with a number of practical implications arising from it.*

***Keywords**: Firmware, RAID system, SSD*

ГЛОБАЛНА НАДЕЖДНОСТ ЗА СЪХРАНЕНИЕ НА ИНФОРМАЦИЯ ЧРЕЗ SOLID STATE DRIVE

Даниел Р. Денев

Факултет по технически науки, Шуменски университет „Епископ Константин Преславски", България, d.denev@shu.bg

Въведение

Надеждността на системата може би е един от най-важните аспекти на системата за съхранение и като такъв съществува голям брой изследвания по темата за надеждността на устройствата за съхранение. Голяма част от по-старата работа е фокусирана върху твърдите дискове (HDD), но тъй като повече данни се съхраняват на твърди дискове (SSD), наскоро фокусът се измести към надеждността на SSD. В допълнение към голямото количество работа върху SSD в лабораторни условия при контролирани експерименти, напоследък се появиха първите полеви проучвания, докладващи за надеждността на SSD в разгърнати производствени системи. Тези проучвания се основават на данни, събрани в центрове за данни във Facebook, Microsoft, Google и Alibaba, където устройствата се внедряват като част от големи разпределени системи за съхранение. Въпреки това наблюдаваме, че все още има редица критични пропуски в съществуващата литература, които тази работа се стреми да преодолее: Няма проучвания, които да се фокусират върху корпоративните системи за съхранение (фиг. 1).

Фиг. 1. Solid State Drive устройства

Устройствата, работните натоварвания и механизмите за надеждност в тези системи могат да се различават значително от тези в облачните центрове за данни. Например устройствата, използвани в корпоративните системи за съхранение, включват устройства от висок клас и надеждността се осигурява чрез (единичен, двоен или троен паритет) RAID, вместо репликация или кодове за разпределено съхранение. По-конкретно, SSD популацията на нашето проучване се състои от почти 1,4 милиона устройства и включва устройства от трима различни производителя, 18 различни модела, 12 различни капацитета и четири различни флаш технологии, т.е. SLC, cMLC (потребителска класа), eMLC (корпоративна класа), и 3D-TLC. Данните, събрани за тези дискове, са много богати и включват информация за замени на дискове (включително причини за смяна), лоши блокове, използване, възраст на дискове, версии на фърмуера, роля на дискове (напр. данни, паритет или резервни), сред редица други неща. Тази статия представя резултатите от нашия анализ с фокус върху отстраняването на пропуските в съществуващата работа [1, 4].

1. ОПИСАНИЕ НА СИСТЕМИТЕ И ДАННИТЕ

Основата на нашето проучване са телеметрични данни от голяма популация NetApp системи за съхранение, внедрени на място. Системите, наричани още файлове, използват файловата система WAFL и операционната система Data ONTAP на NetApp, която използва софтуерен RAID, за да осигури устойчивост срещу откази на дискове. Подсистемата RAID може да бъде конфигурирана да използва SSD в конфигурация Raid-TEC (троен паритет), RAID-DP (двоен паритет) или RAID-4 (единичен паритет). SSD в рамките на RAID група са хомогенни (един и същ производител, модел и капацитет); времето за разгръщане на устройствата може да варира (от няколко месеца до няколко години), но повечето SSD в рамките на RAID група са били разгърнати по едно и също време [2]. По-голямата част от всички системи на NetApp изпращат в полето ежеседмични пакети NetApp Active IQ (преди наричани AutoSupport), които проследяват много голям набор от параметри на системата и устройството, но не съдържат копия на действителните данни на клиентите. Тази информация се събира и автоматично се анализира за коригиращи действия и за откриване на потенциални проблеми.

2. СТАТИСТИКИ

В този раздел представяме базова статистика за характеристиките на дисковете в нашата популация и обобщена статистика за различни показатели за надеждност.

2.1. Характеристики на дисковете

Първите шест колони в Таблица 1 описват ключовите характеристики на различните фамилии устройства в SSD популацията, включително производител и модел (в анонимна форма), капацитет (вариращ от 200GB до 15,3TB), интерфейс (SAS срещу SATA), флаш технология (SLC, cMLC, eMLC, 3D-TLC), литография и лимитът на цикъла на програмно изтриване (PE) на модела, т.е. максималният брой PE цикли, за които е оценен (вариращи от 10K до 100K). Всяко семейство устройства съдържа няколко хиляди до стотици хиляди SSD. И накрая, както е показано в таблица 1, популацията обхваща голям брой конфигурации, които са често срещани на практика през последните години.

2.2. Показатели за живот

Последните три колони в таблица 1 предоставят статистически данни за три различни показателя за изправност и надеждност на устройствата. По-конкретно: Процент на изразходвани резервни блокове: Всяко устройство резервира област (което е равна на 2,5% от общия капацитет на устройството за SSD в това проучване) за пренасочване на съдържанието на блокове, които устройството вътрешно декларира при наличие лоши сектори поради прекомерен брой грешки. Процентът на консумираните резервни блокове отчита какъв процент от полезната област е бил консумиран..

2.3. Наблюдения на високо ниво

По-долу правим редица първи наблюдения въз основа на Таблица 1, преди да се задълбочим в по-подробен анализ на нашия набор от данни в останалата част от този документ: Средният ARR за цялата популация е 0,22%, но процентите варират значително в зависимост от модела на задвижването, от само 0,07% до почти 1,2%. Тези числа са значително по-ниски от числата, докладвани по-рано в други статии. Например, дори най-лошият модел в нашето проучване (ARR от 1,2%) е в долния край на диапазона, отчетен за SSD в центровете за данни на Google (диапазон от 1-2,5%).

3. ПРИЧИНИ ЗА ЗАМЕНИ

Има различни причини, които могат да задействат подмяната на SSD, както и различни подсистеми в йерархията за съхранението, които могат да открият проблеми, и да задействат подмяната на устройства. Например проблеми могат да бъдат докладвани от самото устройство, слоя за съхранение или файловата система. Таблица 1 описва различните типове причини, които могат да предизвикат подмяна на устройство, заедно с тяхната честота, действието за възстановяване, предприето от системата (т.е. копиране на данни от устройството, което трябва да бъде заменено, срещу възстановяване на данните с помощта на RAID паритети) и обхвата на проблема (т.е. риск от частична загуба на данни, риск от пълна загуба на устройство или липса на непосредствени проблеми).Когато изследваме честотата, с която се съобщават отделните типове причини за замяна, ние забелязваме, че единственият най-често срещан тип причина са SCSI грешки, които са отговорни за 33% от всички замени и за съжаление също са едни от най-тежките типове причини. Другата сериозна причина за смяна на устройство е това че напълно не реагира, и се съобщава че това е 0,60%. Останалите две категории са приблизително еднакво често срещани и двете имат потенциал за частична загуба на данни, ако RAID реконструкцията на засегнатите данни се окаже неуспешна. Първата категория (C) се отнася до прекъснати и изтекли команди и съставлява 19% от всички типове причини. Другата категория (B) се отнася за изгубени записи.

Таблица 1. Описание на видовете причини, които могат да предизвикат подмяна

Катег.	Тип	%	ARR (%)	Описание	Реакц. възстан.	Обхват
A	SCSI Epop	32:78%	0:055	Слоят SCSI открива хардуерна грешка, докладвана от SSD, която е достатъчно сериозна, за да се задейства незабавна подмяна на устройството и реконструкция на данните. Например, тези грешки могат да се дължат на ECC грешки, произтичащи от DRAM на устройството, които му пречат да функционира правилно.	RAID Разпозн.	Пълно
	Не реагиращ диск	0:60%	0:001	Дискът напълно се повреди и престана да реагира.	RAID Разпозн.	Пълно
B	Изгубени записи	13:54%	0:023	Загубен запис се открива, когато съдържанието на 4K WAFL блок е несъвместимо въз основа на неговия подпис, който включва атрибути и номер на версия. Тъй като има много потенциални причини със този симптом, се използва евристика, за да се реши дали дискът да се повреди или не. Ако се появят множество такива грешки в рамките на един SSD и няма грешки в друг SSD, тогава предишният SSD се маркира като неуспешен	RAID Разпозн.	Част.
C	Прекратени Команди	13:56%	0:023	Тази грешка се генерира поради прекратена команда и се докладва или от самия SSD, или от слоя за съхранение. Например, тази грешка може да възникне, когато хостът изпрати някои команди за запис към устройството, но действителните данни никога не достигат до устройството поради проблем на хоста или поради проблеми с връзката.	RAID Разпозн.	Част.
	Собственост на диска I/O грешки	3:27%	0:005	Тази грешка е свързана с отговорната подсистема, която следи кой възел притежава диск. В случай, че възникне грешка по време на комуникацията с тази подсистема, тогава SSD веднага се маркира като неуспешен.	RAID Разпозн.	Част.
D	Предсказуеми Провали	12:78%	0:021	SSD отчита тази грешка въз основа на модел от възстановени грешки, възникнали вътрешно, като използва собствени прагове и критерии, както е посочено от съответния производител.	RAID Разпозн.	Част.
	Превишаващ праг	12:73%	0:020	Подсистемата Storage Health Monitor следи различни параметри за всяко SSD и в случай, че прагът (напр. на броя на медийните грешки) бъде надвишен, SSD се заменя проактивно.	Копие на диск	нулево

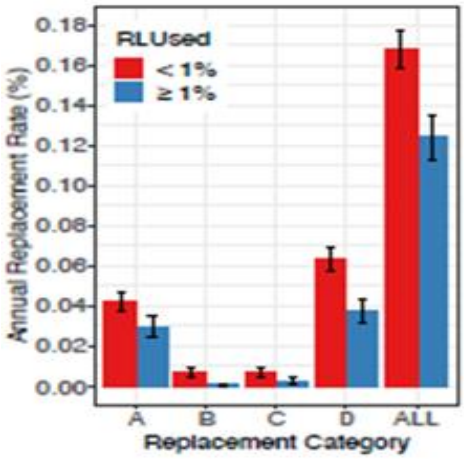
Констатация: Една трета от подмените са свързани с един от най-сериозните типове причини (т.е. SCSI грешки), но от друга страна, една трета от подмените на устройства са просто превантивни въз основа на прогнози

4. ФАКТОРИ, ВЛИЯЩИ ВЪРХУ КОЕФИЦИЕНТА НА ЗАМЕНЯНЕ

В този раздел ние оценяваме как различните фактори влияят върху годишния процент на подмяна на SSD в нашия набор от данни. Извършваме нашия анализ на eMLC и 3D-TLC SSD и изключваме cMLC и SLC устройства поради недостатъчни данни.

4.1. Използване и възраст

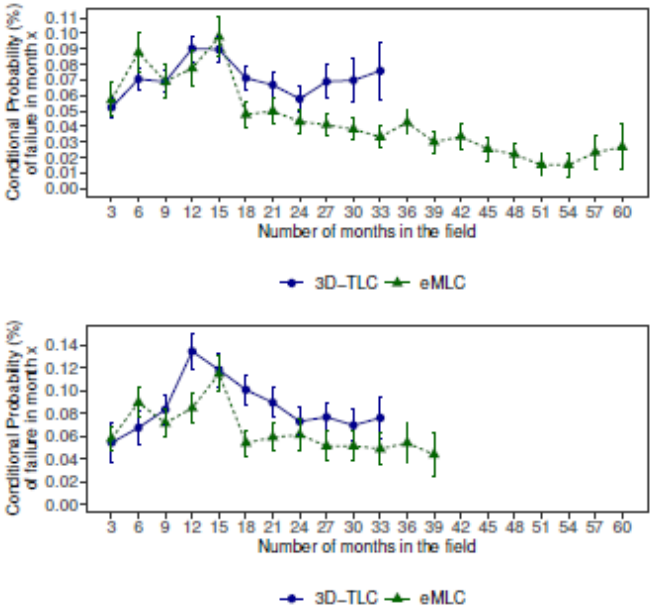
Използването и износването на флаш клетките, което идва с работата, е добре известно, че влияе върху надеждността на базираните на флаш SSD дискове; задвижванията са гарантирани да останат функционални само за определен брой PE цикли. В този набор от данни SLC устройствата имат ограничение за PE цикли от 100K, докато ограничението на повечето cMLC, eMLC и 3D-TLC устройства е равно на 10K цикъла, с изключение на няколко фамилии eMLC устройства с ограничение от 30K PE цикъла (фиг. 2). Всяко устройство отчита броя PE цикли, които е претърпяло, като процент от лимита на PE цикъла, което ни позволява да проучим как употребата влияе върху нивата на подмяна. За съжаление, номиналният използван живот се отчита само като съкратено цяло число и значителна част от дисковете отчитат нула за този показател, което показва, че е използван по-малко от 1% от техния номинален живот.



Фиг. 2. Годишен процент на подмяна за тип флаш въз основа на процента на устройствата

Също така разгледахме отделно задвижванията, които се използват широко (повече от 50% от техните PE цикли) и техните типични причини за подмяна. Виждаме, че тенденцията на намаляване на процента на загубени записи продължава тук, тъй като не наблюдаваме нито един случай, свързан със загубени записи сред тези устройства. Едно възможно обяснение е, че загубените записи може да са свързани с грешки във фърмуера и тъй като фърмуерът се актуализира до подобрени версии в течение на живота на устройството, процентът на загубени записи намалява. Възможно е също така проблемите, водещи до загубени записи, обикновено да станат очевидни в началото на живота на устройството и то да бъде заменено, преди да достигне повече от 1% или 50% от номиналния си живот.

Констатация 2: Наблюдаваме много продължителен период на ниска смъртност на дискове, който може да продължи повече от година и да видим нива на успех 2-3 пъти по-високи, отколкото в по-късни части от неговия в живот (фиг. 3).

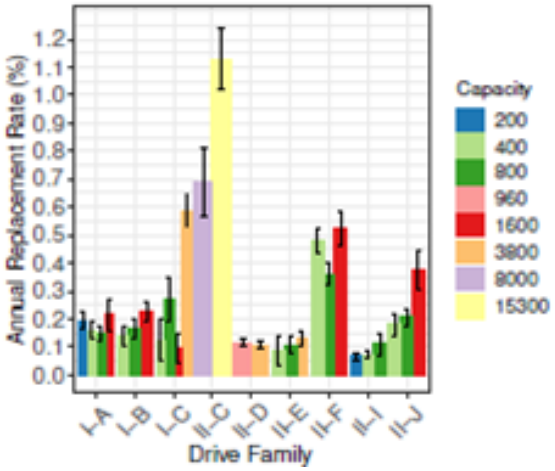


Фиг. 3. Условна вероятност за повреда въз основа на възрастта на устройството

4.2. Тип задвижване

Моделите на задвижване в нашето проучване се различават по типа флаш, на който са базирани, т.е. по това колко бита са кодирани в една флаш клетка. Например устройствата с едно ниво на клетка (SLC) кодират само един бит на клетка, докато устройствата с много нива на клетка (MLC) кодират два бита в една клетка за по-висока плътност на данните и следователно по-ниска обща цена, но потенциално са по-висока склонност към грешки. Най-новото поколение флаш е базирано на тристепенна клетка (3D-TLC) с три бита.

Констатация 3: Като цяло, най-високите нива на замяна в нашето проучване са свързани с 3D-TLC SSD. Въпреки това нито един флаш тип няма забележимо по-висок процент на заместване от другите типове флаш, изследвани в тази работа, което показва, че други фактори, като капацитет или литография, могат да имат по-голямо влияние върху надеждността (фиг. 4).



Фиг. 4. Показва годишните нива на подмяна за дискове, доставени с множествен капацитет

ЗАКЛЮЧЕНИЕ

Нашите наблюдения подчертават важността на актуализациите на фърмуера, тъй като по-ранните версии на фърмуера могат да бъдат свързани със значително по-високи нива на неуспех. И все пак наблюдаваме, че 70% от дисковете в нашето проучване остават с една и съща версия на фърмуера през цялото времетраене на нашето проучване. Следователно ние насърчаваме доставчиците на корпоративни хранилища да правят надстройките на фърмуера възможно най-лесни и безболезнени, така че клиентите да прилагат надстройките без притеснения относно проблеми със стабилността. Въпрос, който често възниква при конфигурирането на RAID групи е: Как размерът на групата, по отношение на броя на устройствата, ще повлияе на нейната надеждност? В края на краищата, интуитивно, повече устройства създават повече потенциал за повреди. Нашите наблюдения показват, че по-големите RAID групи може да не са толкова лоши, колкото често се смята [3, 4].

References

1. Alan T. Arnholt and Ben Evans. BSDA: Basic Statistics and Data Analysis, 2017. R package version 1.2.0.
2. Konstantinova E., Tsankov Ts. Modern SSDs: A high-tech solution to the obsolete HDD systems. Proceedings of the Ninth student scientific conference “Ecology and environment”, 2021, ISSN 2367-5209, pp. 133-140.

3. Matias Bjørling. From Open-Channel SSDs to Zoned Namespaces. In Linux Storage and Filesystems Confer-ence (Vault 19), 2019.
4. Tonchev T., Yankova-Yordanova Y., Tsankov Ts. Comparative Analysis Between Hard Disk Drive and Solid-State Drive, Journal of Physics and Technology, Plovdiv university press "Paisii Hilendarski", Plovdiv, 2018, ISSN 2535-0536.

ANALYZING DATA AND TESTING THE SINGLE WIRE HANDOVER CAPABILITIES OF CATEGORY 8 CABLES

Daniel R. Denev, Tsvetoslav S. Tsankov

Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Bulgaria, d.denev@shu.bg

АНАЛИЗИРАНЕ НА ДАННИ И ПРОВЕРКА НА ВЪЗМОЖНОСТИТЕ ЗА ПРЕДАВАНЕ НА КАБЕЛИ ПО ЕДИН ПРОВОДНИК ОТ КАТЕГОРИЯ 8

Даниел Р. Денев, Цветослав С. Цанков

Факултет по технически науки, Шуменски университет „Епископ Константин Преславски", България, d.denev@shu.bg

***Abstract**: Standards organizations are advancing the development of test requirements and specification limits for Category 8 cable components for frequencies up to 2 GHz. Prior to Category 8 cable specifications, test procedures for measurement and data transmission were based on 2-port Vector Network Analyzers (VNAs) and conventional balun (balanced-unbalanced) transformers. These baluns were used to connect the unbalanced ports of the VNA to the differential device under test. The scope of this article is to compare and analyze Category 8 cable transmission data obtained from a 4-port VNA with data and obtained from a 2-port VNA system with baluns. The advantages and disadvantages of both testing methods will be discussed.*

***Keywords**: Balun, Cat 8, TLT, VNA*

Въведение

Категория 8 (Cat 8) е най-новият стандарт в Ethernet медните мрежови кабели. Дефиниран и пуснат от ANSI/TIA 568. 2016 Cat 8 кабелът е с характеристики от следващо поколение и се превръща в най-новата итерация на Ethernet категорията кабели. Едно нещо, което трябва да се отбележи е, че има различни стандарти за Cat 8 Ethernet кабели. Тъй като ISO SC25 WG3 е разработил оригиналния стандарт той, предоставя две опции за Cat8 — Клас Cat 8.1 и Клас Cat 8.2.

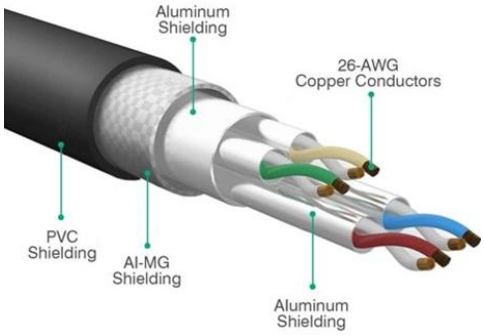
- Cat8.1 Ethernet кабелът използва RJ45 съединители, за да бъде съвместим с Cat6a и предишните Ethernet кабели;
- Ethernet кабелът Cat8.2 използва съединители, различни от RJ45, по-специално TERA или GG45, за да се свързва с кабели Cat7.

Приликата с неговия предшественик от категория 8 е екранирането. Поради това те имат по-строги изисквания за кросоувъри и устойчивост на смущения и шум и имат по-добра способност за електромагнитни смущения (EMI). Разликите между двата стандарта са многобройни. Кабелът Cat7 използва конектори GG45 или TERA, кабелите Cat 8 имат два стандарта, така че са налични обикновени конектори RJ45 и конектори, които не са RJ45. Cat7 има четири усукани двойки мед-

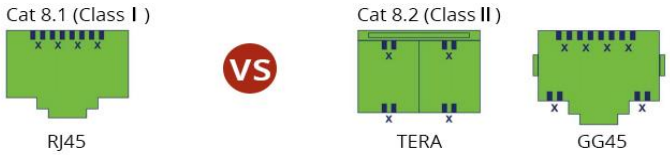
ни проводници, Cat8 идва с две усукани двойки. Cat 7 има отлични предимства в поддържането на шум. Cat7 е дефиниран до 600 MHz, докато Cat8 поддържа честота на предаване от 2000 MHz. Фиг. 1 показва кабел от категория 8, по подобен начин фиг. 2 показва конекторите за същата категория. Формула (1) показва изчислението за предаване и обработка на кадри в кабели CAT 8.

$$(Frame\ Size\ 6^2 x\ Frame\ Rate\ 6^2)\ +\ (Frame\ Size\ 6^2 x\ Frame\ Rate\ 6^2) \quad (1)$$

40GBase-T пренася данни със скорост от 40Gbps по 4 чифта кабели при категория 8. Честотата на изпитване за кабелни компоненти от категория 8 е 2 GHz. Тази честота е 4 пъти по-висока от тестовата честота за кабелни компоненти от категория 6A, която е 500 MHz. Тестването на 2 GHz носи предизвикателства, които не се срещат при тестване на по-ниски честоти. Подготовката на кабела, кабелните устройства за свързване на системата към векторния мрежов анализатор, стандартите за калибриране на s-параметрите са някои от тези предизвикателства. Преди категория 8 балуните бяха основният компонент, използван за свързване на балансираните усукани двойки към дисбалансните изходни портове на VNA. Тестването с балуни е подробно описано в параграфа за тестване на усукана двойка. С увеличаването на тестовата честота до 2 GHz друг подход за тестване на усукани двойки става много актуален. Този друг подход за тестване се основава на небалансираните данни на отделните проводници, измерени с 4-портов VNA. Всеки край на двата проводника на двойката е свързан към VNA порт. Всички останали проводници на изпитвания 4-чифтов кабел трябва да бъдат правилно терминирани. В следващите раздели ще предоставим подробно описание на тези два метода за изпитване [1, 3, 4].



Фиг. 1. Кабели категория 8

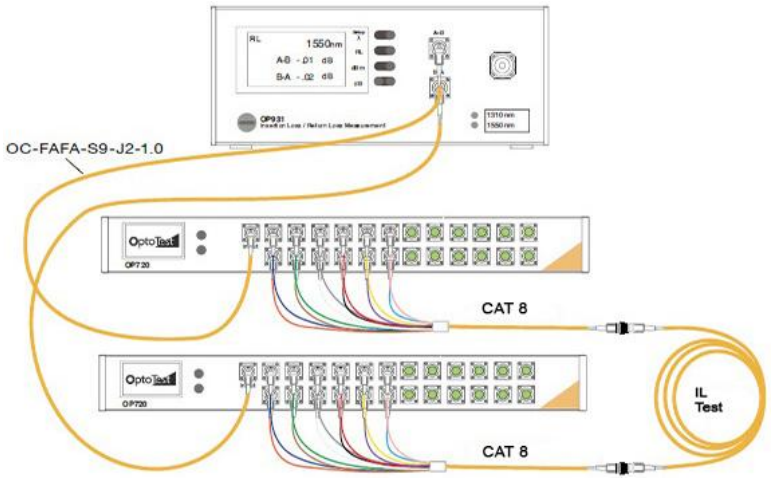


Фиг. 2. Конектори за кабел от категория 8

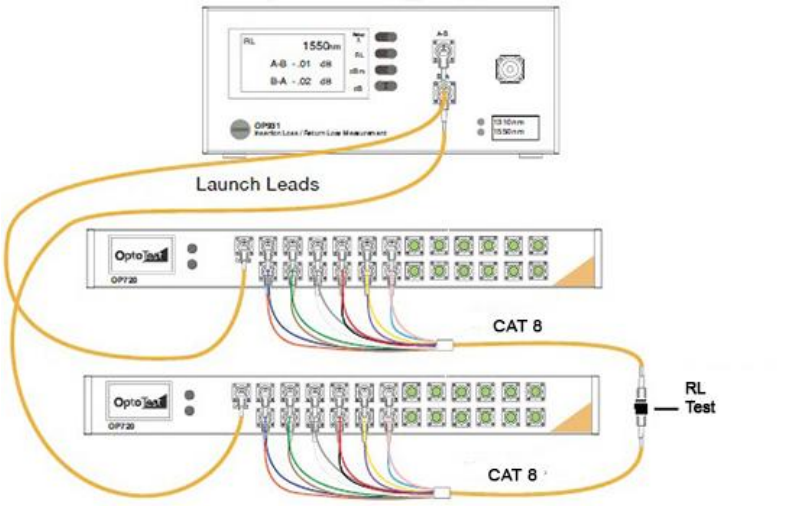
1. Балунно измерване

Балуните се използват за свързване на небалансираните портове на VNA към балансираните усукани двойки. В допълнение към осигуряването на баланс за дебалансиране на интерфейсните балуни, също така те осигуряват трансформация на импеданса. Следователно тези балуни осигуряват интерфейса между 50 Ω небалансиран порт на VNA към 100 Ω импеданс на балансираната усукана двойка. Има два типа балуни: конвенционални балуни, базирани на намотки, и трансформаторни балуни, базирани на преносна линия или TLT. Балун с конвенционални намотки тип трансформатор не е възможно да се получи честотната лента от 1 MHz до 2 GHz, необходима за

тестване на кабели от категория 8. Поради това балуните TLT се използват за тестване на кабели от категория 8 в необходимата честотна лента. Използваните TLT са направени от коаксиални предавателни линии с известен импеданс, конфигурирани да осигурят съвпадение на импеданса от 50 Ω до 100 Ω. За тестовете в тази статия бяха използвани фино настроени и оптимизирани TLT балуни, работещи на 2,2 GHz. Продукт за тестване на кабели от типа DCM ES-2G с автоматичен превключвател беше използван за автоматизиране на вмъкнатите загуби, загубите при връщане, кръстосаните смущения в близкия край и кръстосаните смущения в далечния край на тестваните кабели от категория 8. Превключвателят ES-2G беше свързан към 2-портов E 5071B VNA. Превключвателят ES-2G е определен от 1 MHz до 2,2 GHz. Минималното ниво на шума за тестване на кръстосани смущения е по-добро от 90 dB при 2,2 GHz. Превключвателят ES-2G е способен да извършва измерване на обратна загуба до 35 dB в честотния диапазон от 1 MHz до 2,2 GHz. Фиг. 3 и 4 показват конфигурациите за измерване на балун. Всички двойки, които не се тестват, се прекратяват в диференциален и общ режим. Традиционното калибриране на SOLT се използва за измервания на балуна в точката на свързване на кабела [2, 6].



Фиг. 3. IL Тестова конфигурация



Фиг. 4. RL Тестова конфигурация

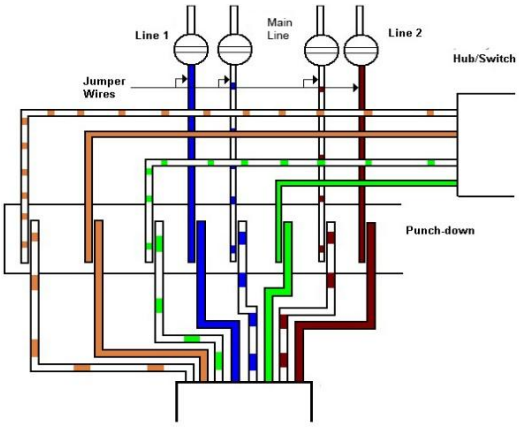
2. CAT 8 Ethernet кабели

Cat 8 Ethernet кабел не се препоръчва в повечето сценарии. Мрежите Cat 8 за дома и малкия до среден бизнес (SMB) са доста редки случаи. От една страна, Cat8 25Gbps/40Gbps достъп до скорост на данни е примамлив, но в повечето случаи ненужен за домашна и SMB употреба. От друга страна, разполагането на Cat 8 Ethernet кабели изисква съществуващата мрежова инфраструктура да бъде съвместима с Cat8 кабелите или клиентът трябва да надстрои своето мрежово оборудване и устройства, за да поддържат Cat 8. Изборът на по-евтиния и по-точен Cat 6a може да отговори на изискването за използване на домашни и малки бизнес мрежи с по-висока производителност, като междинни 2.5GbE, 5GbE и 10GBASE-T. Най-високата скорост и други характеристики с висока производителност правят Ethernet кабела Cat 8 най подходящ за вискоскоростни центрове за данни и сървърни стаи, където разстоянието на медна връзка между сървъри и комутатори е кратко. Малки до средни центрове за данни, които търсят 25G надстройка от 10G или 1G на ръба, ще бъдат особено идеални за внедряване на кабели Cat 8. В обичайния случай за домашна мрежа Cat 8 може да се използва за игри и стрийминг. Уравнението показва изчислението за предаване и обработка на кадри в кабели CAT 8, въз основа на което е създаден алгоритъм за съвместимост в устройствата, показан в (2).

$$C^{SD} = \quad k=P \quad \frac{tp^2+ut^{DT} \quad i=0 \quad p=0(\quad 0=P\, z^j + \quad 1=P\, z^j)w_i}{tp-ut^{DT} \quad i=0 \quad p=0(\quad 0=P\, z^j + \quad 1=P\, z^j)w_i} \tag{2}$$

3. Автоматична конфигурация за превключване

В тази тестова конфигурация всяка тестова позиция използва независим балун. Всеки VNA порт се превключва към всички тествани двойки посредством многополюсни RF коаксиални превключватели. Всеки път за измерване се калибрира с помощта на диференциално SOLT калибриране в точката на свързване на кабела. Пълен 2-портов модел за калибриране в алгоритъма за коригиране на грешки е добавен. Всички стандарти за диференциално калибриране са проверени до 2,2 GHz с помощта на NIST проследим VNA. Фиг. 5 показва автоматичен превключвател за сдвояване, а фиг. 6 показва система за автоматично превключване.



Фиг. 5. Двойков автоматичен превключвател

Калибрираните пътища със сигнали се основават на базата на реда на Фурие и чрез система от тригонометрични функции. Всякакви периодични калибрирани пътища със сигнали могат да бъдат представени като сбор от безкраен брой данни с множество основни честоти

$\omega_0 = \frac{2\pi}{T} = 2\pi f_0$. За целта един период от сигнала трябва да се разложи в ред на Фурие със стъпка, равна на основната честота $f_0 = \frac{1}{T}$ на сигнала:

$$S\ t\ = \frac{a_0}{2} + \ \sum_{i=1}^{k}\ a_i cos 2\pi\ if_0 t + b_i sin 2\pi\ if_0 t\ ; K \to \infty \tag{3}$$

$$a_i = 2f_0 \int_{-\frac{T}{2}}^{\frac{T}{2}} S(t) \cos\ 2\pi i f_0 t\ dt = \frac{2}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} S(t) \cos\ 2\pi i f_0 t\ dt \tag{4}$$

$$b_i = 2f_0 \int_{-\frac{T}{2}}^{\frac{T}{2}} S(t) \sin\ 2\pi i f_0 t\ dt = \frac{2}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} S(t) \sin\ 2\pi i f_0 t\ dt \tag{5}$$

Фиг. 6. ES- 2G Система за автоматично превключване

Броят на членовете K в редицата на Фурие е практически ограничен от допустимата грешка при апроксимирането на функцията $S(t)$. Изразът (2) може да се представи в следния по-компактен вид:

$$S\ t\ = \frac{a_0}{2} + \ \sum_{i=1}^{k} A_i \cos\ 2\pi i f_0 t + \varphi \tag{6}$$

$$A_I = \ \sqrt{a_i^2 + b_i^2} \tag{7}$$

$$\varphi = -arg tg\ \frac{a_i}{b_i} \tag{8}$$

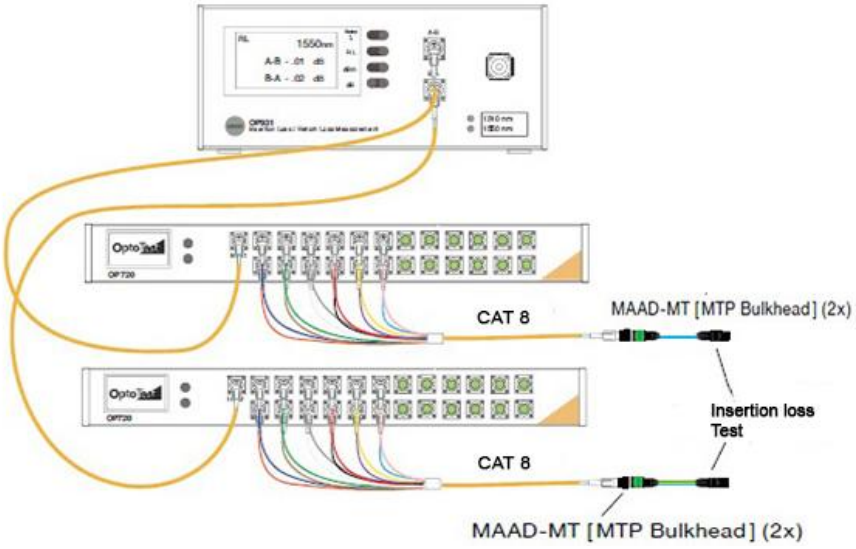
Ползата от използването на код на Грей е, че малките нестабилности (в рамките $\pm 1/2\delta$) на аналоговия сигнал S(t) в интервала на предаване на данни Δt от влакното предизвикват изкривяване най-много в един бит от двоично число, образувано на изхода след измерване . Това се обяснява от таблица 1.

Таблица 1. Обикновен двоичен код и код на Грей

№ на ниво квантуване	Обикновен двоичен код	Код на Грей	№ на ниво квантуване	Обикновен двоичен код	Код на Грей
0	0000	0000	8	1000	1100
1	0001	0001	9	1001	1101
2	0010	0011	10	1010	1111
3	0011	0010	11	1011	1110
4	0100	0110	12	1100	1010
5	0101	0111	13	1101	1011
6	0110	0101	14	1110	1001
7	0111	0100	15	1111	1000

4. Конфигурация за тестване на един проводник

Необходим е 4-портов мрежов анализатор за извършване на тестване на един проводник. Връзката между анализираната мрежа и изпитваната двойка се осъществява чрез два отделни коаксиални пътя с импеданс 50 Ohm. Всеки проводник от двойките, които не са подложени на тест, се завършва с коаксиален товар от 50 ома. Мрежовият анализатор извършва всички измервания на единичен проводник и всички изчисления, необходими за предоставяне на резултатите в диференциален формат [5, 8, 9].



Фиг. 7. Конфигурация на теста за вмъкване на загуби

Броят на термините K за единичен кабел в серията на Фурие е представен в следната форма:

$$S\ t\ = \frac{a_0 - 1}{2} + \ \sum_{i=1}^{k} A_i \cos -1\ \ 2\pi i f_0 t + \varphi - 1 \tag{9}$$

$$A_I = \ \overline{-a_i^2 + (-b_i^2)} \tag{10}$$

$$\varphi = -argcotg\ \ \frac{a_i - 1}{b_i - 1} \tag{11}$$

5. Измервания на кабели

Тази точка описва основите на настройката за измерване. В настоящото изследване фокусът е върху типа кабели

- U/FTP без обвивка Категория 8.2 (30 метра)
- При измерване на кабели основно внимание се обръща на следните основни параметри
- Честотен диапазон
- Брой точки
- Честотна лента
- Промяна на честотата
- Ниво на мощност
- Температура на кабела

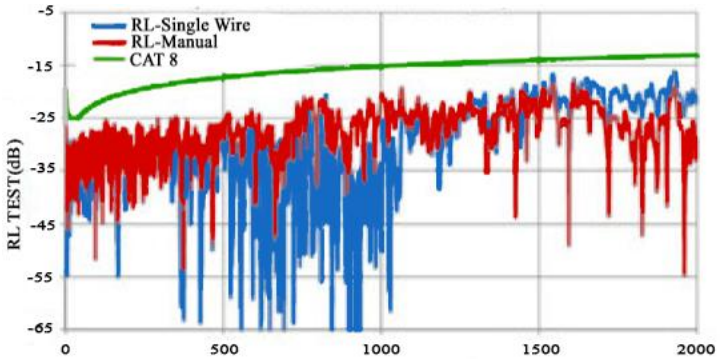
Таблица 2 показва настройките за измерване, параметрите и стойностите

Таблица 2. Настройка на измерването

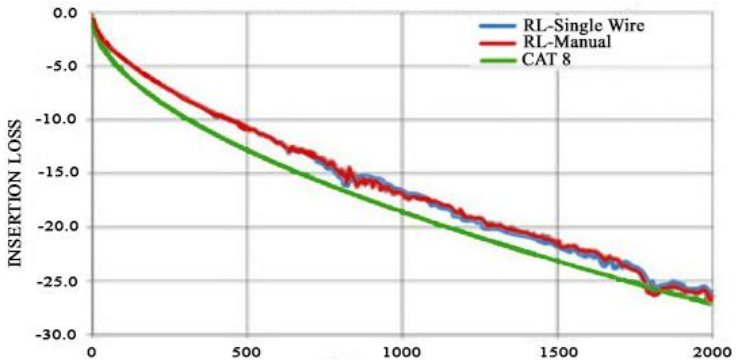
Параметри	Стойности
Честотен диапазон	1 MHz to 2000 MHz
Брой точки	1601 IF
Честотна лента	300 Hz
Промяна на честотата	$Linear$
Ниво на мощност	10o dB
Температура на кабела	23° C

6. Резултати от теста на кабела

В тази точка са показани графиките на резултатите от измерването на кабели от категория Cat 8. По-конкретно резултатите от теста ще бъдат оценени в параграф 8. Основният акцент е върху зеления цветен сигнал, който описва предаването на информация за определен период от време. Прави впечатление, че не е податлив на външни смущения



Фиг. 8. Връщане на загуби в метода Балун



Фиг. 9. Вмъкване на загуби в метода Балун

7. Оценка на резултатите от теста

1) Директно измерване на балун:

Следват типични лабораторни техники за тестване на LAN кабели.

Кабелното свързване беше извършено с помощта на монтаж на печатна платка (PCB), прикрепен директно към TLT балун с SMB конектори.

Импедансно съгласувани печатни платки свързват IC гнездата към SMB конекторите.

2) Автоматични измервания на балун:

Изисква разпръскване на изпитваните двойки

Свързването на изпитваната двойка се извършва с помощта на крайни кубове, които се свързват директно към 50 Ohm контактна пътечка.

Екранираните чаши се използват за постигане на висока изолация между тестовите позиции

3) Вмъкната загуба:

Измерванията на загубите при вмъкване на единичен проводник вмъкване показват добра корелация.

Изборът на THRU стандарт е от решаващо значение за получаване на по-гладко и безпроблемно измерване на вмъкната загуба.

Ефектът на обратната загуба върху внесената загуба е по-очевиден при по-къси кабели

4) Загуба при връщане:

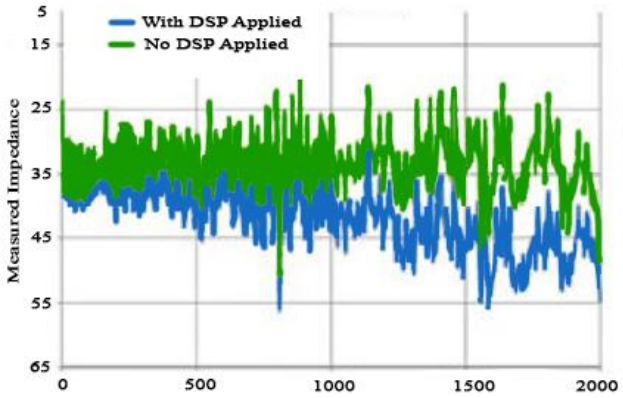
Резултатите са сравними и при двата метода.

Подготовката и манипулирането на кабела е много важно, особено при автоматичните измервания.

Този ефект се премахва лесно с помощта на DSP техники [6, 7].

Отстраняване на ефектите в края на кабела от подготовката за отразителните тестовете

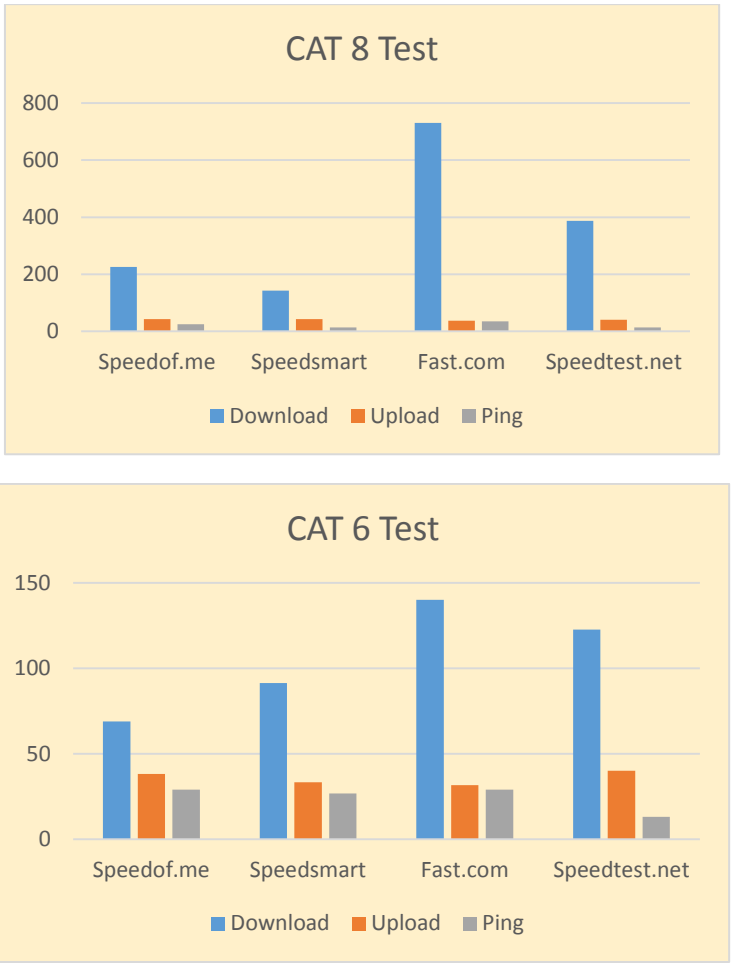
Добре известно е, че дължината на обвивката, отстранена по време на подготовката на LAN кабела за тестване, влияе върху резултатите от теста за импеданса и обратната загуба. С увеличаването на честотата и ефектът на опашката се вижда при тези измервания на отражението. Тъй като дължината на свалената обвивка се скъсява, честотата, при която се вижда ефектът на опашката, се увеличава. Винаги обаче ще е необходимо да премахне част от обвивката на кабела; следователно винаги ще има ефект на опашка поради дължината на свалената обвивка. Това може да е много обърквашо за производителите на кабели, тъй като те могат да отхвърлят добър кабел или да пропуснат лош кабел поради грешки в резултатите от теста за отражение. Резултатите от теста за отражение показва че е засегната производителността, тъй като краят на кабела е подготвен от различни лица, това осигурява различни резултати от теста за отражение. Техническият доклад на IEC IEC/TR 61156-1-5 описва процес за елиминиране на този ефект чрез отстраняване на обвивката. Процесът се основава на преобразуването на резултатите от честотната област във времевата област, където се използват техники за цифрова обработка на сигнала (DSP) и за премахване на ефекта на обвивката върху резултатите. След като ефектите бъдат премахнати, данните се преобразуват обратно в честотните резултати. Преобразуването на данните от честотен домейн във времеви домейн и обратно в честотен домейн се извършва с помощта на обратна бърза трансформация на Фурие (IFFT), а преобразуването обратно в честотен домейн се извършва с помощта на бърза трансформация на Фурие (FFT).



Фиг. 10. Премахване на ефекта на опашката с DSP

Сравнителен анализ на скоростите с кабели Cat 8 и Cat 6

Въз основа на изследванията до тук е извършено допълнително измерване на категорията кабели Cat 8 и Cat 6 и техните технически възможности, чрез което е направен сравнителен анализ на тяхната скорост. За извършване на изследването са използвани кабели Cat 8 и Cat 6. Проведено е на тренировъчна мрежа и са използвани параметрите и скоростите им. Измерването на скоростта се извършва индиректно чрез платформи за измерване на трафика. Фиг. 11 показва резултатите.



Фиг. 11. Скорост на изтегляне, качване и пинг

Заключение

Добре известно е, че технологията с 4 порта позволява възможността за тестване на балансирани двойки без ограниченията на честотния диапазон на балуните. Балуните с TLT технология обаче могат да предложат честотни ленти, които са в състояние да покрият диапазона от честоти на предложената категория 8. Тъй като стандартите за кабелите от категория 8 продължават да напредват към ратифициране, съществува и необходимост от по-нататъшен напредък в изискванията и насоките за изпитване, за да се отговори на нуждите на тези по-високи честоти. Значителни технически изисквания за точни измервания и фиксиране са реда на Фурие и косвеното калибриране. Със завършеното сравнително тестване в тази статия, калибрирането и корекцията чрез ред на Фурие са причинители някои от най-видимите ефекти и разлики между измерванията с балун. Калибрирането предлага простота и точност, но е трудно за прилагане в комутирана система и все пак изисква допълнителни процедури за премахване на ефектите от тестовото приспособление. Някои по-сложни техники за калибриране може да изискват и по-високо ниво на мре-

жовите анализатори. Техниките за късо и отворено калибриране също представляват собствени предизвикателства. По-специално, калибрираният резистор за натоварване трябва да бъде както внимателно избран, така и характеризиран, а качеството на свързване на резистора към приспособлението играе измерима роля при измерванията на загуби. Прилагането DSP техника за 4-портови еднопроводни измервания трябва да бъде проучено допълнително и вероятно ще играе важна роля в тестовите стандарти, тъй като честотата на тестване се разширява.

References

1. Базин Ш. Основи на мрежовата сигурност. ДуоДизайн, С., 2004
2. Ганчев, И. Компютърни мрежи и комуникации. Пловдив, ИМН, 1999.
3. Генков Д., Основи на компютърните мрежи, Габрово, 2014, ISBN 978-619-7071-61-0
4. Кент, П. Да научим Netscape Комуникатори 4. С., ИнфоДар, 1998.
5. Макмилън, Т. Cisco: Компютърни мрежи – основи, Алекссофт, 2016
6. Мизин, И. А., В. А. Богатырев, А. П. Кулешов. Сети коммутации пакетов. Москва, Радио и связь, 1986
7. Clayton R. Paul Analysis of Multiconductor Transmission Lines, Wiley
8. Cross Jon, Koichi Yanagawa, Modal Decomposition Measurement Technique. IWCS 1995 proceedings
9. Chao H, Chen Y, Wu J, Power saving for machine to machine communications in cellular networks. In: 2011 IEEE GLOBECOM workshops (GC Wkshps), Dec 2011, pp 389–393

APPROACHES FOR BUILDING AUTOMATED MANAGEMENT AND MONITORING SOFTWARE ARCHITECTURES OF RF SPECTRUM

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

ПОДХОДИ ЗА ИЗГРАЖДАНЕ НА СОФТУЕРНИ АРХИТЕКТУРИ ЗА АВТОМАТИЗИРАНО СЛЕДЕНЕ И УПРАВЛЕНИЕ НА РАДИОЧЕСТОТНИЯ СПЕКТЪР

Мирослав Г. Неделчев

Катедра „Компютърни системи и технологии", Факултет „Артилерия, противовъздушна отбрана, комуникационни и информационни системи", гр. Шумен, България

nedel4ew@abv.bg

Abstract: *RF management and monitoring of frequency resources has an essential role in the planning, implementation and allocation of frequency bands, issuing of licenses and permits, as well as control over the provided resources by national and regional regulatory authorities. The dynamics of these processes require the use of software architectures to optimize the operation of systems as a whole, creating opportunities for shared use of common resources.*

Keywords*: RF management and monitoring, RF monitoring software architecture*

Въведение

Често при издаване на лицензи и разрешителни за използване на подходящите за безжична комуникация честотни ленти, възникват въпроси относно натовареността на съответната лента в конкретен географски район; ефекта от разполагане на нови източници [1] на електромагнитна енергия и все по – често използваните еднократни или многократни импулсни електромагнитни въздействия за борба с безпилотни летателни апарати [2], вида на терена, нивата на емисиите и нивата на смущения, икономическият ефект от това и други.

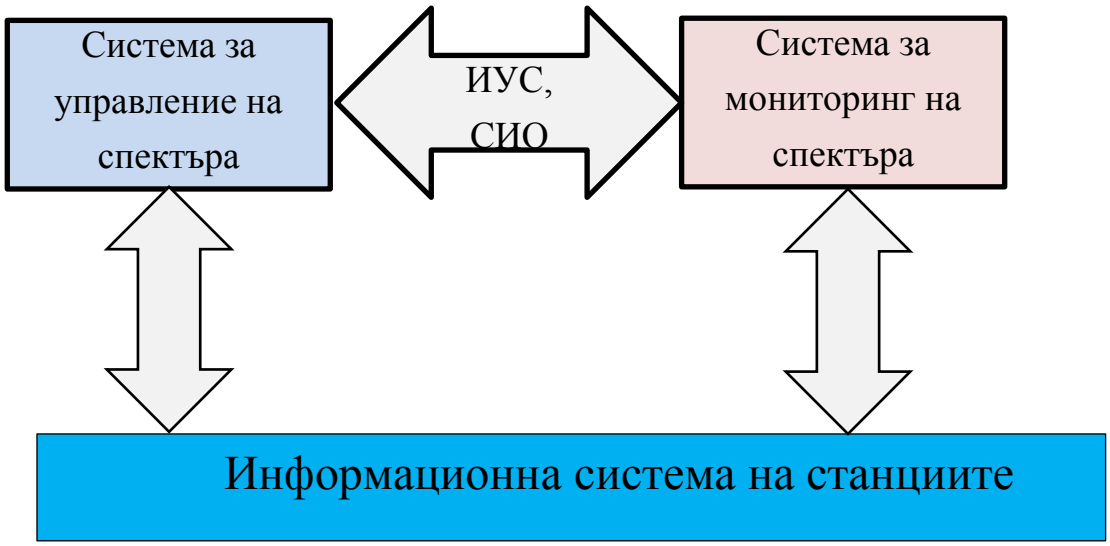
Съществуващите софтуерни архитектури за автоматизирано следене и управление на радиочестотния спектър не са в състояние да отговорят на съвременните разбирания за динамичен достъп до честотни ресурси и/или споделено използване на честотни ленти в различни географски области, обект на контрол от национални и международни регулаторни органи.

Функционални изисквания към софтуерната архитектура

С оглед тяхното надграждане и в съответствие с препоръките на ITU-R към тях се описват и изисквания към функционалността на съвместимите бази данни, на които трябва да отговарят. Такива могат да са:

- Отдалечен достъп до системни ресурси;
- Автоматично откриване на нарушения;
- Назначаване на честоти и лицензиране;
- Интегриране на инструмент(и) за подпомагане на планирането и внедряването;
- Автоматизирано измерване на параметрите на сигнали;
- Автоматизирани измервания на заетостта и/или определяне на посока;
- Автоматизиран обмен на данни;
- Поддържане на графичен интерфейс.

Общ вид на софтуерна архитектура за автоматизирано следене и управление на радиочестотния спектър е показан на фиг. 1.



Фиг. 1. Обща софтуерна архитектура за изграждане на система за управление на спектъра [3]

- **Система за информационен обмен (СИО)** - определя структура на данните и вида на командите към системата за наблюдение чрез системата за управление.
- **Интерфейс за управление на спектъра (ИУС)** осигурява цялата структура от данни и команди, за да позволи на системата за наблюдение да има достъп до данни съхранявани в базата данни на системата за управление на спектъра.
- **Система за управление на спектъра** - поради отворения интерфейс осигурява възможност за интегриране на всяка отделна система за управление на спектъра .
- **Система за наблюдение** - обслужва всички задачи за измерване, необходими за управлението на спектъра и предоставя оптимално използване на ограничения честотния спектър.
- **Информационна система на станциите (ИСС)** – компонент към информационната система за предоставяне на актуална информация относно текущото състояние на станциите за наблюдение. Измерват се аналогови, цифрови и импулсни сигнали и се различават следните режими:
  - **Автоматично измерване** – осигурява постоянно или циклично измерване на зададен набор от параметри в определена част от деня или годината;

Автоматично разпознава отклонение от зададени диапазони и възможност за задействане на аларма и последващо измерване с оборудване предоставящо по – голяма точност.

– **Интерактивен режим на измерване** - режимът на интерактивно измерване се използва за получаване на обща карта с възможности за анализ на сигнали, определяне местоположението на предаватели, измерване на покритието в дадена точка, откриване на нарушения и идентифициране на електромагнитни емисии.

Възможен е и статистически анализ на заетостта на честотните ленти и канали, стойности на измерването, кои потребители използват най-често дадена лента и др.

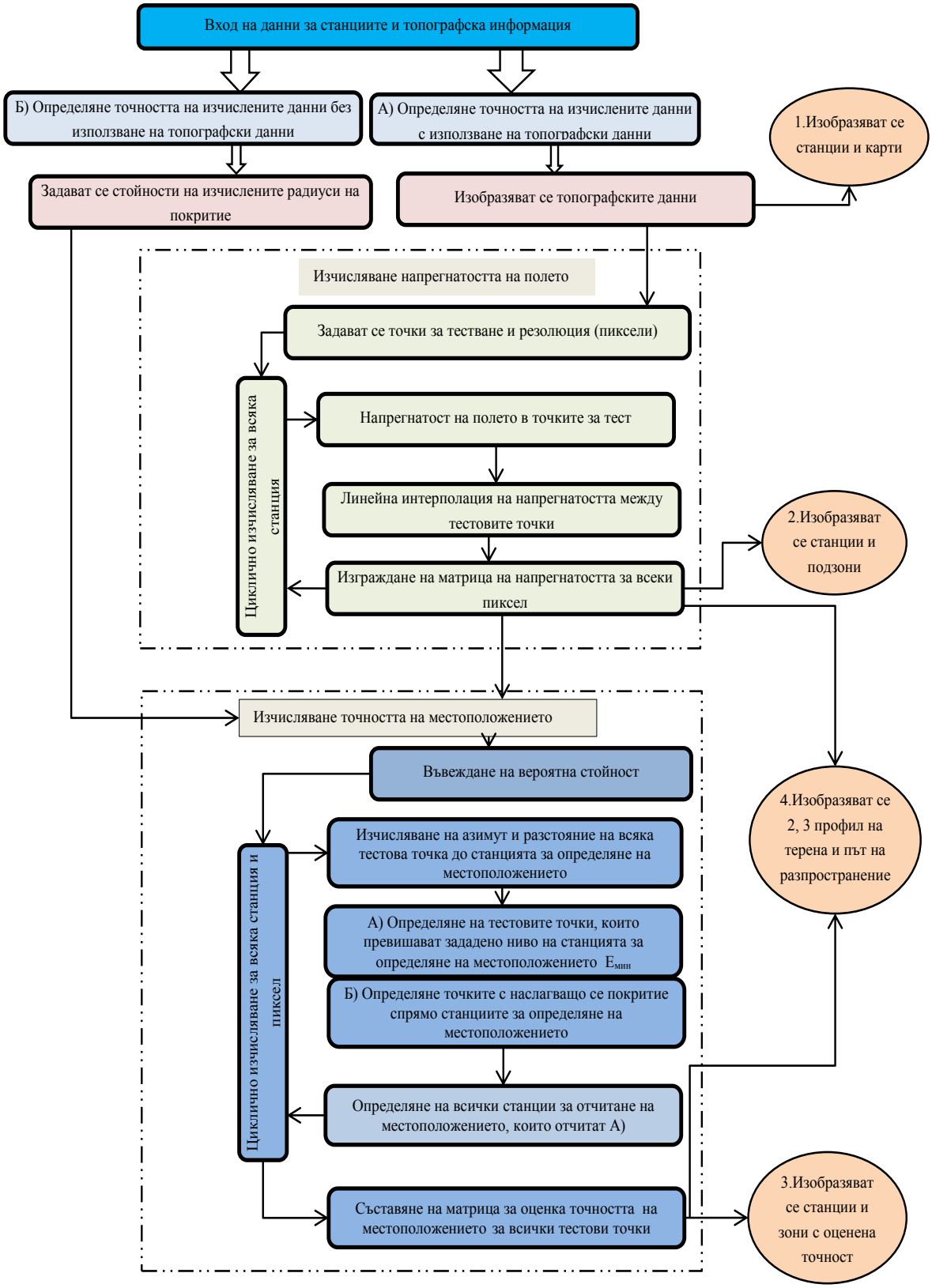
– **Режим за определяне на местоположението** - използва различни техники (AoA, TDOA) за точно намиране на предавател.

Софтуер за наблюдение и оптимизиране използването на спектъра, базиран на оценка ъглите на постъпване

Софтуер за наблюдение и оптимизиране използването на спектърар базиран на оценка ъглите на постъпванер първоначално е предложен през 2005 г. [5] и подобрен през 2012 г. [4]. Позволява създаване на карти на покритието за УКВ мобилни потребители,определяне на условията на взаимодействие със фиксирани станции и:

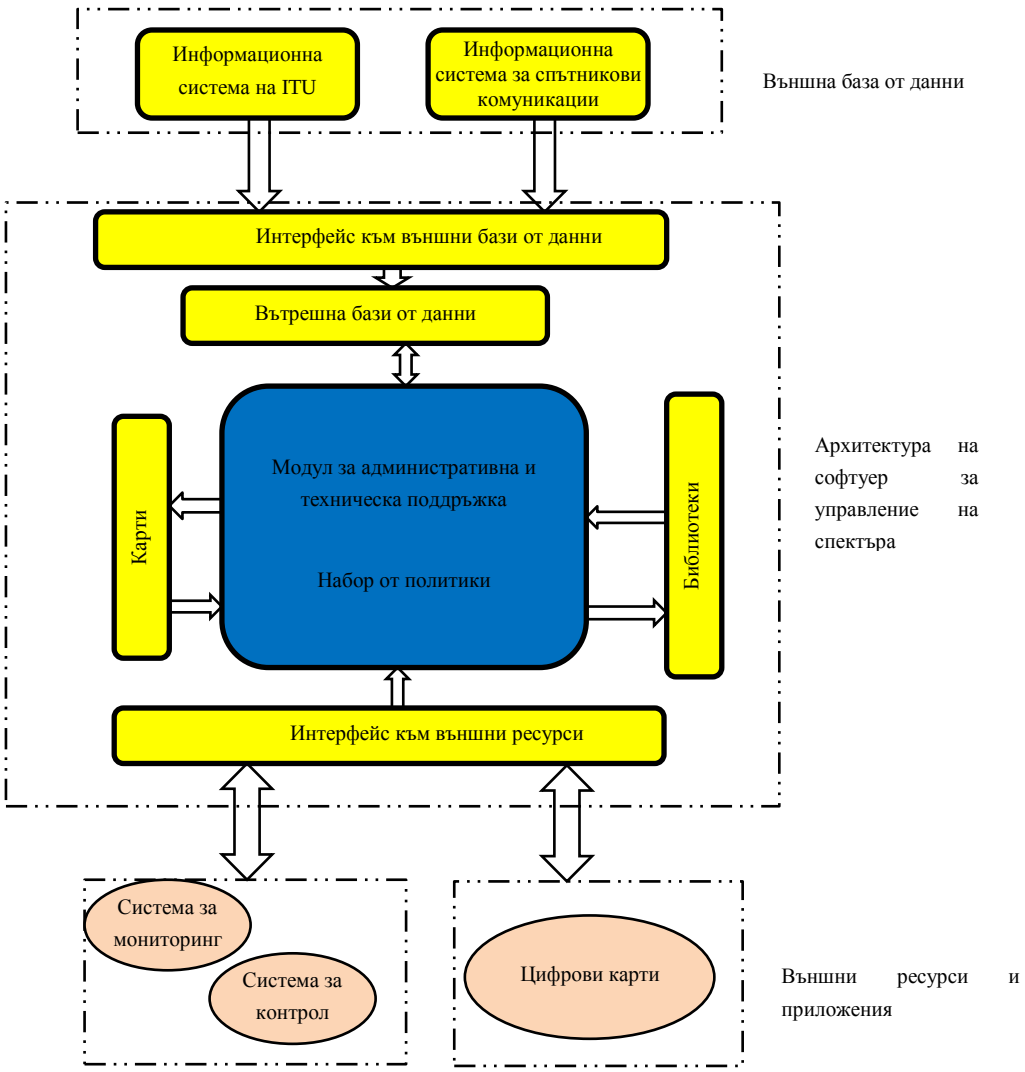
- точна количествена информация за реалната електромагнитна обстановка;
- измерване на параметрите на средата и определяне на местоположение чрез триангулация;
- изобразяване на подробни карти на мониторинговото покритие при различни честоти в диапазона 30-3 000 MHz ;
- оценка на различни варианти и ползите от надграждане на системата за мониторинг (чувствителност на приемниците, методите за определяне на местоположение,промяна на височини на антените);
- да се идентифицират области, в които една или друга функция за наблюдение не допринася значително за цялостния мониторинг и възможностите за използване в друга зона;
- да се разработват технически и икономически обосновани планове за надграждане и разширяване на съществуващите мрежи за наблюдение;
- да се оптимизира работата на мобилни станции при планиране на техния маршрут на базата на данни от предишни наблюдения;

Общ вид на архитектура с отчитане на оценката от ъглите на постъпване е показана на фиг. 2 с осигуряване на възможности за използване на топографски данни и задаване на радиуса на покритие. При това е възможно да се определи напрегнатостта на полето в конкретни тестови точки със съответната зададена средно вероятна точност на местоположението и зададения профил на терена и път за разпространение за конкретния поддиапазон.



Фиг. 2. Структура на система за оптимално планиране и проектиране на мрежи за наблюдение на спектъра базиран на оценка ъглите на постъпване [3]

С оглед унифициране процеса на регулиране и осигуряване на възможности за динамичен достъп ITU разработва и насърчава използването на компютърно подпомагано управление на спектъра от администрациите на развиващите се страни. Софтуера е базиран на Windows (WinBASMS) и представлява сложен софтуерен продукт с възможност за отчитане на множество технически характеристики и функции. Софтуерната архитектура показана на фиг.3 е предложена от ITU [6] и осигурява графично и контекстно меню и възможности за взаимодействие с външни бази от данни,ресурси и карти, които могат да бъдат растерни и векторни карти (политически, крайбрежни, регионални, морски).



Фиг. 3. Архитектура на софтуер за компютърно подпомагано управление на спектъра

Заключение

В настоящия доклад са представени подходи за изграждане на софтуерни архитектури с възможности за контрол, мониторинг, планиране, разпределение, споделяне и управление на спектъра чрез използване на компютърно подпомагани техники, така че да не се оказва съществено влияние върху работата на други потребители. Предоставя възможностите за уплътняване на спектъра и неговото по равномерно натоварване за даден географски район с отчитане на възможно повече фактори, влияещи върху качеството на услугите.

References

[1] Кацев И., (2021), "Analysis of the opportunities for employment unmanned aerial vehicles class mini in artillery formation", *Proceedings of International Scientific Conference "Defense Technologies" DefTech 2021, Faculty "Artillery, AD and CIS", Shumen, Bulgaria pp 116-123*

[2] Чанев С., „Активни направления за повишаване на възможностите за противодействие на БЛА на бойното поле" *Сборник научни трудове на Международната научна конференция „Отбранителни технологии" DefTech 2021, Факултет "Артилерия, ПВО и КИС"*, *стр. 92-99*

[3] ITU-R (2015), *Handbook on computer aided techniques for spectrum management (eds.) Chapter 3 Spectrum management data and database management, pp129-136*

[4] Krutova O , Pavlyuk A.,(2012) "Planning procedures for spectrum monitoring networks in the VHF/UHF frequency range," *International Symposium on Electromagnetic Compatibility - EMC EUROPE,* pp. 1-6, *doi: 10.1109/EMCEurope.2012.6396919.*

[5] Krutova O. E., Kogan V. V. and. Pavliouk A. P,(2005) "Advanced software for planning and optimization of spectrum monitoring networks," *IEEE 6th International Symposium on Electromagnetic Compatibility and Electromagnetic Ecology,* pp. 76-79, doi: 10.1109/EMCECO.2005.1513067.

[6] Report ITU-R SM.2356-2 (06/2018), Procedures for planning and optimization of spectrum-monitoring networks in the VHF/UHF frequency range

ANALYSIS OF SPECTRUM MANAGEMENT AND MONITORING 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

АНАЛИЗ НА СИСТЕМИТЕ ЗА УПРАВЛЕНИЕ И МОНИТОРИНГ НА СПЕКТЪРА

Мирослав Г. Неделчев

Катедра „Компютърни системи и технологии", факултет „Артилерия, противовъздушна отбрана, комуникационни и информационни системи", гр. Шумен, България
nedel4ew@abv.bg

Abstract: *Automated spectrum management plays an important role in the entry of new wireless services and provides opportunities for spectrum trading, leasing and sharing.*
This paper presents some of the spectrum monitoring and management systems and their capabilities for reliable and fast resource management.

Keywords*: RF management and monitoring, RF monitoring systems*

Въведение

Необходимостта от използване на компютърно подпомагани техники за управление и мониторинг на радиочестотния спектър е осъзната и възприета от повечето национални регулаторни органи още през 70-те години на XX в.

Развитието на микропроцесорната и полупроводна техника доведе до значително понижаване на цената на безжичните радиоелектронни средства и допринесе за тяхната широка употреба. Концепциите за „умен дом" и IoT още повече утежняват проблема с използване на радиочестотния спектър.

От друга страна, строгото регулиране и ограничаване на достъпа до подходящи честоти представлява ограничение за навлизане и използването на нови технологии. Въпреки това изследванията показват, че части от честотния спектър в определени времеви интервали и на определени места за лицензираните честоти се наблюдават така наречените „бели места или дупки" – т.е честоти, които не се използват [17]. Това ясно показва, че традиционния подход за регулиране на честотните не отговаря на съвременните предизвикателства пред безжичните системи за комуникация и налага използване на подходи [1], които ще доведат до по - ефективно [17] използване на радиочестотния спектър, т.е неговото максимално уплътняване.

Към настоящия момент такива решения са политиката за назначаване на честоти WAPECS - Wireless Access Policy for Electronic Communications Services – предложена от European

Conference of Postal and Telecommunications Administrations(CEPT) [4],[6] и, и техниките за споделен и отворен достъп до спектъра [14] в частност лицензирания споделен достъп [15] .

При WAPECS се цели ограничаване на смущенията и възможност за конкуренция между отделните радио инфраструктури за заемане на конкретни ленти основаващи се на присвояване на честотни блокове, вместо метода за присвояване на канали при неутрални изисквания към предоставяните услуги и използваната технология.

Оторизираният споделен достъп е регулаторен подход, целящ да улесни въвеждането на радиокомуникационни системи, управлявани от ограничен брой лицензополучатели при индивидуален лицензионен режим във честотна лента, която вече е определена или се очаква да бъде присвоена на един или повече действащи потребители.

При подхода на лицензирания споделен достъп (LSA) допълнителните потребители са оправомощени да използват спектъра (или част от спектъра) в съответствие с правилата за споделяне, включени в техните права за използване на спектър, като по този начин позволяват на всички оторизирани потребители, включително присъстващите, за осигуряване на определено качество на услугата (QoS) "

Оторизираният споделен достъп и лицензираният споделен достъп са централизирани модели, които позволяват споделяне на спектър при предварително зададени условия, които могат да бъдат статични (време и местоположение) или динамични (време, местоположение, честота, ниво на мощност, трафик на първични потребители и т.н.).

Описаните по-горе решения за интелигентно управление на спектъра[14], [18] налагат усъвършенстване на компютърно подпомаганите техники за следене и управление на спектъра [3]. В съответствие с препоръките на ITU-R са разработени редица софтуерни архитектури за автоматизирано следене и управление на радиочестотния спектър. Такива са [2],[1] „Интелигентна система за управление на спектъра (SMI)", „Автоматизирана система за управление на спектъра (SIRIUS)", „Софтуер за управление на носещи услуги (RAKURS)", „Автоматизирана система за управление на спектъра (ICS)"," Система за автоматизирано управление (IRIS), "Интегрирана автоматизирана система за управление на спектъра (SPECTRA)", "Система за автоматизирано управление и наблюдение (TCI).

1. Интелигентна система за управление на спектъра (SMI)

Модулна система с функционално-географско разделяне между сървъра на базата данни [16] и различните модули за приложения. Разработена е от националната агенция за радиоизследвания [11] на Република Корея и е предназначена да извършва всички необходими дейности по управление на честотния план [5].

Мащабируемата архитектура позволява модификация и основни системни конфигурации лесно могат да бъдат разширявани и надграждани до по-сложни и цялостни конфигурации.

Основната система се състои от подсистема за анализ на излъчвания в наземни мрежи и съвместимост между устройствата. Допълнителните подсистеми осигуряват възможност за анализ на сателитни мрежи и споделяне на честотни ресурси. Системата може да обработва различни видове слоеве в режим на симулация с топографски карти и използване на данни за гъстотата на населението.

Подсистемата за мрежов анализ (планиране) и координация на аналогови и цифрови излъчвания има следните функции:

- анализ на покритието за излъчващи станции;
- анализ на смущения;
- анализ на наличните канали;
- споделяне и регистрация на излъчваните честоти.

Подсистема за анализ на излъчвания в наземни мрежи се използва при планирането и координацията на фиксирани и наземни мобилни услуги, като клетъчните мрежи от четвърто и пето

поколение, включително и груповите радио комуникационни системи. Функциите съвпадат с тези на подсистемата за мрежов анализ (планиране) и координация на аналогови и цифрови излъчвания, но отчитат мобилните потребители.

Подсистемата за анализ на сателитни мрежи е предназначена за координация на орбитите на сателитните ретранслатори, разположение на наземните станции и ограничаване на интерференцията, както между спътниковите, така и наземни услуги посредством системата за споделяне на честотни ресурси

2. Автоматизирана система за управление на спектъра (SIRIUS)

Предложена е от Република Киргизстан. и представлява опростена система за управление [9] на не голям набор от честоти на базата на технология клиент-сървър в съответствие с препоръките на ITU-R за методи за оценка и анализ на EMC.

Системата се състои от модул за управление,административен и инженерен модули. Основни функции които се предоставят са :

- лицензиране на честотни назначения;
- вътрешна и международна координация (уведомяване);
- планиране използването на спектъра;
- аналитични методи за оценка на SNR и EMC;
- инструменти за инженерен анализ с общо предназначение за изчисляване на смущения и зони за покритие, анализ на трасета и др., посредством цифрови данни за терена;
- регистриране на събития (заявки, конфликти, решения);
- събиране и анализ на данни за мониторинг на спектъра;
- анализ на измерванията и сравнение с базата данни;
- съхранение на данни за вътрешни и международни таблици за разпределение на честотите;
- импортиране и експортиране на данни;
- архивиране и възстановяване на данни;
- регистрация на потребители на системата, одити.
- За управление на отделните модули са предвидени следните инструменти:
- планиране на спектъра;
- аналитични инструменти за излъчване, мобилни и фиксирани услуги;
- аналитична оценка на EMC между станциите с различни услуги;
- инженерни инструменти с общо предназначение ;
- прогнозни модели за разпространение;
- поддръжка на национални и международни таблици за разпределение на честоти, включително и услуги ;
- инструмент за редактиране на планове и разпределение на канали;
- гъвкава система за отчитане на таблици с честотни разпределения (показване в графичен и табличен вид);
- проверка на честотните задания и съответствие им с честотните таблици;
- инструмент за оценка въздействието на съществуващите и бъдещи станции - за всяко географско местоположение в зоната на обслужване на станцията (услуга) чрез изчисления, базирани на данни за терена;
- инструмент за оценка на междуканалните смущения ;
- анализ на интермодулационните смущения
- индексирано търсене на станция в базата данни - резултатите се показват с избрани от потребителя слоеве;

- изчисляване и графично изображение на зоните на покритие и зоните на смущения за дадена станция,използвайки различни модели на разпространение ;
- Показване на профили на трасето и стойности на затихване при разпространение (в зависимост от модела на разпространение).

За улесняване на прогнозирането са въведени различни типови модели на разпространение в свободно пространство - еднородна и неоднородна повърхност; Окумура-Хата;модифициран модел за разпространение в свободното пространство и модели по препоръки на ITU-R.

3. Софтуер за управление на носещи услуги RAKURS

Софтуерният инструмент RAKURS [8] е проектиран и разработен в Русия в края на 70-те години на миналия век в интерес на контрол радиоразпръскването на аналогови услуги .

Към настоящият момент включва софтуерно ядро, база от данни и пакет за приложения и се използва за честотно планиране на телевизионно и радио излъчване в VHF и UHF обхват и смекчаване на проблема с електромагнитната съвместимост в Беларус, Армения,Молдова и Узбекистан и осигурява следните основни възможности:

- оценка на характеристиките на честотните задания; разработване на препоръки относно избор на честотен канал за нови или модифицирани честотни назначения;
- гранична (двустранна, многостранна) международна координация на разпределенията на честоти;
- изчисляване на зоните на обслужване за единични станции за телевизионно излъчване на стандарти DVB-T, DVB-T2,DVB-H и T-DAB;
- изчисляване на смущения внасяни от LTE мрежи;
- определяне на взаимни смущения между различни станции;
- приблизително изчисляване на разходите на компоненти за проектираната мрежа ;
- автоматизирано генериране на мрежа за оптимално покритие на даден регион.

При изчисляването на EMC се използва единен интерфейс и се отчитат модела на разпространение; надморска височина; параметри за повърхността; предявявани изисквания; възможностите за сортиране на смущения за станцията според различни бази данни; водни пространства;ъгли и просвет; комбиниране на смущения за различни бази данни

4. Автоматизирана система за управление на спектъра ICS

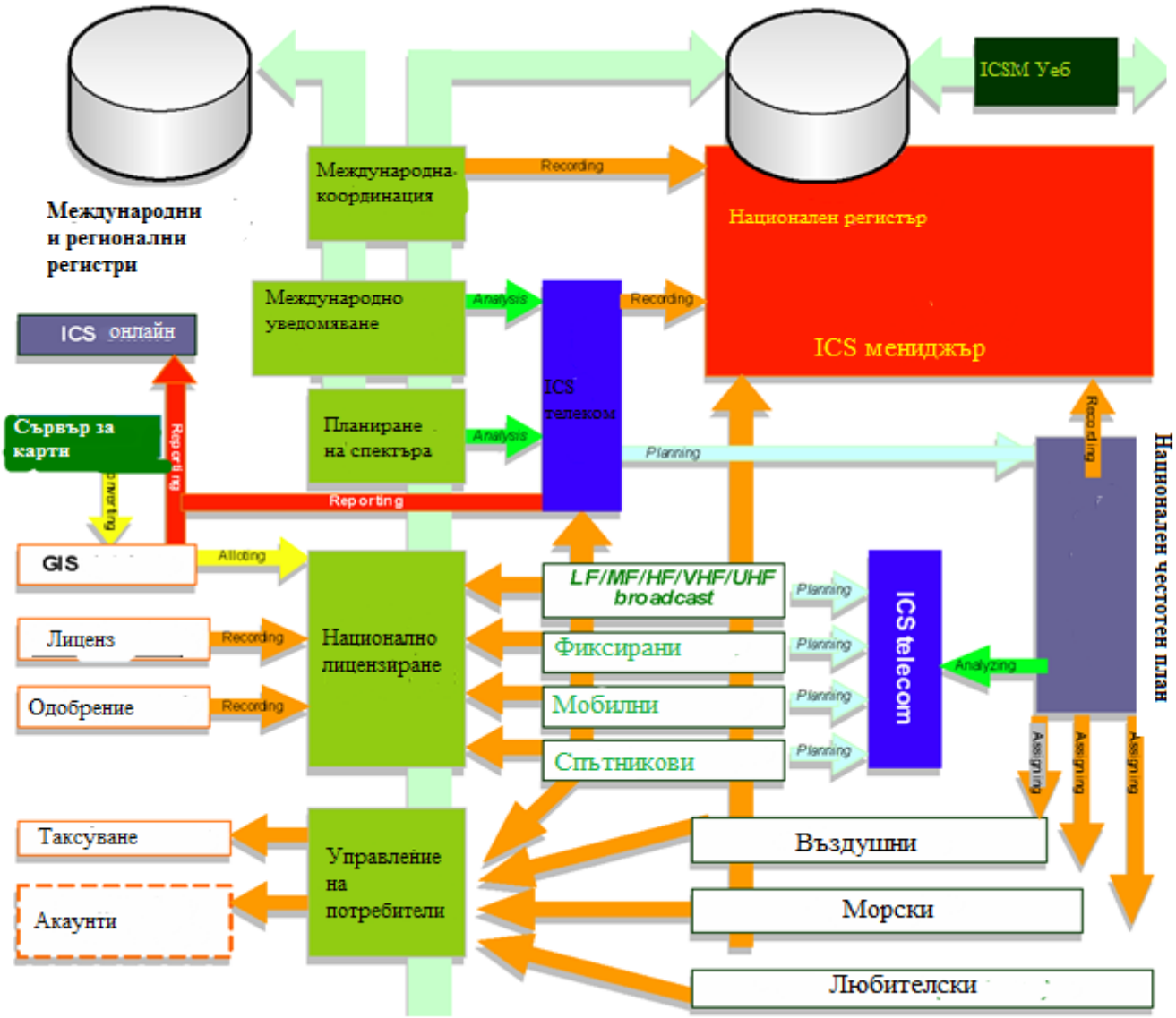
ICS е разработена от Франция и се използва от множество национални и международни регулаторни органи [7]. Архитектурата позволява работа от типа клиент-сървър; вграждане в друга система и уеб базирани програми за управление на някои услуги.

Автоматизираната система за управление на спектъра се състои от три подсистемни приложения [10]:

ICS мениджър - софтуер за управление на спектъра;

ICS телеком - софтуер за радиопланиране и управление на спектъра;

ICS онлайн - инструмент за публикуване, позволяващ споделяне на онлайн доклади.



Фиг. 1. Архитектура на автоматизирана система ICS

Основните характеристики на ICS мениджъра са:

– управление на административни процедури (управление на лицензи, оперативно управление) в съответствие с действащите национални, регионални и международни правила ;

– изчисляване на таксите в съответствие с техническите и административни параметри на честотите и задания на лицензи.

– генериране на документи (отчет, фактури, разписки), фактуриране и проследяване на плащанията;

– международна нотификация, международна координация;

– планиране на спектъра, честотни задания;

– зонални разпределения;

– интерфейс със системите за мониторинг на спектъра;

– разпределения, приложни радиоинтерфейси и права за управление на ползването;

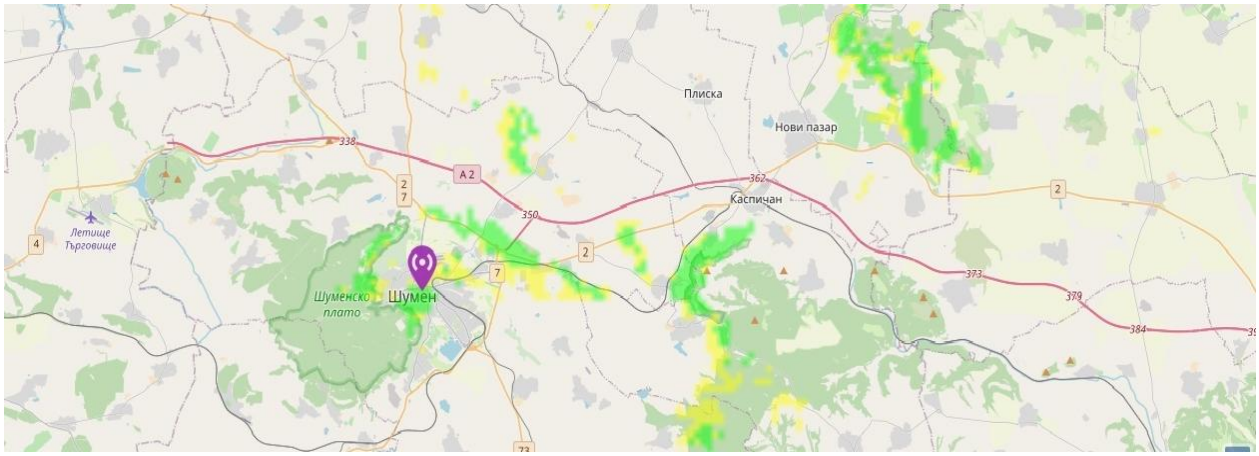
– оперативно управление за всички услуги (технически, административни, честотни, местоположение, антени и параметри на оборудването);

– управление на известия към ITU по препоръка на ITU-R SM.1370.

ICS телеком позволява инженерно планиране и моделиране, развитие и управление на радиокомуникационни мрежи. Осъществява координация между националните честотни планове и фиксираните, мобилни, сателитни, любителски и други потребители, изпълнява функции по оптимизиране и наблюдение на спектъра, оценява съвместимостта на нови и съществуващи мрежи и подпомага управлението на спектъра за аналогови и цифрови, ТВ сигнали, клетъчни мрежи, интелигентни мрежи и безпилотни летателни апарати.

5. Radio Mobile

Представлява свободна за употреба софтуерна платформа [12] (сорс кода не е отворен),предназначена за създаване на детайлни модели на разпространение на електромагнитните вълни при отчитане на множество фактори и особености на терена. Ограничена е до използване на честотни ленти за свободна употреба от ползвателите на любителско радио. Налични са две версии – за инсталиране и онлайн. При първата е възможно да се използват карти с отчитане на височините на терена и GPS данни. Възможно е да работи само в режим офлайн, но само чрез Windows операционни системи, докато втората версия поддържа всякакъв тип операционни системи.



Фиг. 2. Изчисляване на покритието за района на град Шумен

Заключение

Компютърно подпомаганите техники за управление достъпа до честотните ресурси не решават проблема с фрагментацията на честотния спектър поради невъзможността от точно предсказване на електромагнитната обстановка, дължащо се на множество променливи взаимно зависими технически параметри, но предоставят база за реализиране на лицензиран и оторизиран споделен достъп, както и политиката за безжичен достъп предложена от CEPT, т.е по-ефективно управление на честотните ресурси от широк кръг ползватели.

References

[1] Banerjee, I, Seneviratne, K.,(2005) Public service broadcasting: a best practices sourcebook, UNESCO

[2] Brock, G. L. ; Bedford, T. L. ; Grange, G. M. "An overview of the intrasystem EMC analysis program with graphics"

[3] Burns J., Marks P., LeBorgne F., Rudd R.,(2013) Study on Spectrum Management in the field of Broadcasting, FINAL REPORT Implications of Digital Switchover for Spectrum Management

[4] Electronic Communications Committee, (2008), "Report from CEPT to the European Commission in response to the Mandate to develop least restrictive technical conditions for frequency bands addressed in the context of WAPECS Final Report"

[5] ETRI, (April 2018) Case study on spectrum management and monitoring in Korea

[6] European Commission (2013)," Radio Spectrum Policy Group", RSPG13-538

[7] https://atdi.com/

[8] https://rakurs.niir.ru/index_EN.html

[9] https://ursi.org/proceedings/procGA05/pdf/CP5.12(0253).pdf

[10] https://www.lstelcom.com/en/products/spectrum-management/spectra/

[11] https://www.rra.go.kr/en/intro/history.do

[12] https://www.ve2dbe.com/english1.html

[13] ITU-R (2015), *Handbook on computer aided techniques for spectrum management (eds.) (2015)* Chapter 3 Spectrum management data and database management, 129-136

[14] Olanrewaju B.S., Osunade O. (2012), "Survey of Related Technologies for Improved Spectrum Efficiency", IOSR Journal of Engineering (IOSRJEN), e-ISSN: 2250-3021, p-ISSN: 2278-8719, www.iosrjen.org, Volume 2, Issue 11, November 2012, pp 25-33.

[15] Onidare S.O, Navaie K., Ni Q. (2019), "On the Spectrum and Energy Efficiency in Dynamic Licensed Shared Access Systems: A Multiobjective Optimization Approach", Vol.7, Digital Object Identifier 10.1109/ACCESS.2019.2952686

[16] Recommendation ITU-R SM.1537-1, (08/2013), Automation and integration of spectrum monitoring systems with automated spectrum management

[17] Vinogrdov E., (2016), State of the art- Ways for increasing spectrum efficiency and implementation of new radio technologies, Information technology and telecommunication vol.4 №1, pp 68-78

[18] Woolsey, R. B. [2000] Automatic Tools for Telemetry Test Range Spectrum Management.,Proc. ITC/USA 2000,
https://repository.arizona.edu/bitstream/handle/10150/606489/ITC_2000_00-03-4.pdf?sequence=1&isAllowed=y

PREDICTIONS AND EVALUATION WITH AI IN CYBERSECURITY

Angela R. Borisova

"Artillery, Air Defense and CIS" Faculty" - Shumen,
National Military University "Vasil Levski", Bulgaria, arborisova@nvu.bg

Abstract: *The use of artificial intelligence in cybersecurity systems is a trend for the reason that it enables organizations to meet and respond adequately against the growing computer threats and attacks. For this purpose, computational algorithms developed with the help of Machine Learning are included in the software intended for protection. In order for the trained machines to work correctly, it is necessary to constantly make predictions and accordingly evaluate the state of the network traffic, which verifies whether the software can pass safely or to be blocked. This review paper examines forecasts and assessments without whose collaboration the detection and prevention of a cyberincident would be extremely hard.*

Keywords:. *Cybersecurity, Artificial Intelligence, Machine Learning*

ВЪЗМОЖНОСТИ ЗА ПРОГНОЗИ И ОЦЕНКИ ПРИ ИЗПОЛЗВАНЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ В КИБЕРСИГУРНОСТТА

Ангела Р. Борисова

Факултет „Артилерия, ПВО и КИС"- гр. Шумен,
Национален военен университет „Васил Левски", България, arborisova@nvu.bg

1. Прогнозиране на кибератаки чрез използване на AI

В днешно време различните организации плащат милиарди долари, за да бъдат разработени най-добрите машини, използващи изкуствен интелект за осигуряване на киберсигурност. Изкуствения интелект (ИИ, Artificial Intelligence, AI) се явява решение за изграждане на умни и добре защитени комуникационно-информационни системи със значително намаляване на вероятността от човешки грешки, чрез възможността да бъдат прогнозирани и откривани злонамерени интернет дейности, като фишинг, неоторизирани мрежови инструкции и несанкционирана доставка на вредоносен код към междинни и крайни терминали-жертва. Осъществяването на внедряване на ИИ изисква създаването на алгоритми, които да засичат и обезвреждат интернет заплахите. Киберсигурността е област, подкрепена от изкуствения интелект, което от своя страна позволява подобрение в процесите на управление на информацията. С напредване на тази технология обаче се увеличават и цифровите заплахи. Колкото повече се използват комуникационни технологии с помощта на компютърни мрежи, чипове и данни [5], толкова повече проблеми възникват.

Много от наличните антивирусни софтуери, които се предоставят с безплатно разпространение, не могат да отговорят адекватно на нарастващите киберзаплахи [2]. Много често тези софту-

ери считат даден файл за безопасен, когато всъщност той не е такъв. Това е грешка, която се нарича „false negative", което е причина все повече институции да предвиждат използването на ИИ (AI и в частност Machine learning) с цел минимизиране на некоректните дефиниции за вирусите. Един от методите за откриване на проникване е базиран на т.н. „размита мрежа" (Fuzzy Network), като той използва асоциативно претърсване в генетично програмирана мрежа. Този метод доказва свойства на гъвкавост и ефективност при откриване на аномалии в мрежите и е способен да работи със смесени бази данни [4].

На таблица 1 са представени 4-те положения при прогнозиране дали даден софтуер е злонамерен или не, като те са:

- **True** positive – когато съответната програма за отчитане на зловреден софтуер направи прогноза, че даден файл е опасен и той наистина се окаже такъв.
- **True** negative - когато съответната програма за отчитане на зловреден софтуер направи прогноза, че даден файл е безопасен и той наистина се окаже такъв.
- **False** positive - когато съответната програма за отчитане за зловреден софтуер направи прогноза, че даден файл е опасен, а същевременно се окаже, че не е такъв.
- **False** negative - когато съответната програма за отчитане за зловреден софтуер направи прогноза, че даден файл е безопасен, а същевременно се окаже, че не е такъв.

Таблица 1. Матрица на грешките (таблица на истинност, confusion matrix)

Прогнозиране			
Действителен резултат		Злонамерен софтуер	Безопасен софтуер
	Злонамерен софтуер	True positive	False negative
	Безопасен софтуер	False Positive	True negative

Пример, отнасящ се до прогнозиране състоянието на кибератака, дали предсказанието е вярно или не е посочен в таблица 2.

Таблица 2. Примерна статистика при прогнозиране

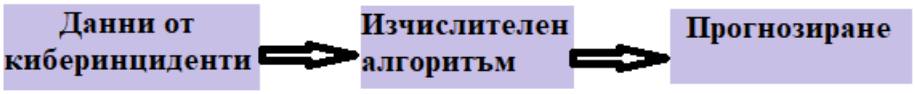
Прогнозиране при 1000000 реализации			
Взети решения		Злонамерен софтуер	Безопасен софтуер
	Злонамерен софтуер	1000	900
	Безопасен софтуер	900	997.200

Имайки данните от таблица 2 може да се заключи, че статистически проверявания софтуер е наистина злонамерен. Проблем обаче е еднаквата вероятност за „false negative" и „false positive". Най-често прогнозните резултати изглеждат по посочения на таблица 2 начин, защото програмите за откриване на атаки все още не са 100 % надеждни. От примера се вижда, че са открити 1000 заразени файла, измежду 1 млн. проверени пакети например и това е действителен резултат. В редовете "false positive" и "false negative" се среща числото 900 и в този случай се оказва, че самата прогноза е лоша. Когато програмата покаже, че 900 измежду 1000 файла например са безопасни, а те всъщност не са, тогава вече е налице фалшива прогноза и 900 е изключително лош

резултат, а това може да се дължи на факта, че атакуващия пакет е нов и самата програма не се е срещала с него до този момент.

В механизмите на AI е внедрена способност да се идентифицира, да се отговори на атака и дори да се предприемат мерки по защита на дадена система от анормално поведение. Този процес открива злонамерен софтуер или мрежови аномалии. За защита на дадена корпорация от атаки се използват различни похвати за идентифицирането им, като: хеш функции (цифров отпечатък на файл, който се основава на съдържанието на файла), специфични сегменти от вътрешния код, характеристики на поведението, когато се изпълнява файл или приложение. Всички тези методи към днешна дата обаче осигуряват минимална защита от киберзаплахи и са по-известни още като атаки с т.нар. Zero-day (Това са такива атаки, които никога не са били засичани като опасни. Поради тази причина вероятността съществуващите способи за защита да ги разпознаят като заплаха е нищожна).

Вредният софтуер може да причини големи повреди, от извеждане на съобщения, през причиняване на хаотична работа на програмите, криптиране на файлове и искания за откуп за тяхното дешифриране, до разрушаване на данните или твърдите дискове [1]. На фигура 1 са изброени стъпките, през които преминава процеса на засичане и съответно прогнозиране на киберзаплахите, като данните от киберинциденти могат да бъдат стотици и дори хиляди на брой. Това е причината хора да не могат да се справят с обработката на такъв обем информация, а компютрите с инсталирани адекватни алгоритми за ИИ имат тази възможност. При внедряването на ИИ добра практика се явява използването на многослойна изкуствена невронна мрежа (МНМ, MNN – всяка невронна мрежа може да бъде разработена в средата Матлаб [6]), на която да се подадат наличните огромни количества данни, а изчислителния алгоритъм да си свърши работата и да подготви системата за извършване на прогнозиране.



Фигура 1. Стъпки за осъществяване на прогнозиране

2. Примери за изчислителни алгоритми

Изчислителните алгоритми в ML се делят на 3 основни вида:

- обследвани (с надзор/контролирано обучение, supervised);
- непроследявани (без надзор/неконтролирано обучение, unsupervised);
- Reinforcement (обучение с утвърждение).

Примери за обследвани алгоритми са:

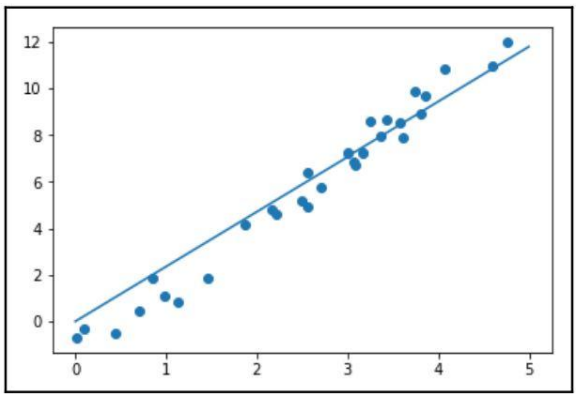
- с използване на регресия (линейна функция и логистична задача);
- алгоритъм K на най-близкия съсед (k-Nearest Neighbors, k-NNs);
- метод на опорните вектори (Support vector machines, SVMs);
- дърво на решенията и гори за произволни решения (Decision trees and random forests);
- невронни мрежи (Neural networks, NNs)

На фигура 2 е представен един от най-широко разпространените обследвани алгоритми, а именно линейна регресия, като са използвани библиотеки: scikit-learn, numpy и matplotlib на езикът Pyton. Посоченият модел на фиг. 2 е за прогнозиране на данни, които не са известни на алгоритъма до момента, като за тази цел е използван методът predict (). Данните, които се използват за обучение на мрежата са разпределени посредством линеен модел, имащ следния вид: $\boldsymbol{y = 3x + 2}$ [3].

```
%matplotlib inline
import matplotlib.pyplot as plt
import numpy as np
from sklearn.linear_model import LinearRegression

pool = np.random.RandomState(10)
x = 5 * pool.rand(30)
y = 3 * x - 2 + pool.randn(30)
# y = 3x - 2;

lregr = LinearRegression(fit_intercept=False)
X = x[:, np.newaxis]
lregr.fit(X, y)
lspace = np.linspace(0, 5)
X_regr = lspace[:, np.newaxis]
y_regr = lregr.predict(X_regr)
plt.scatter(x, y);
plt.plot(X_regr, y_regr);
```

Фиг. 2. Прогнозиране на данни чрез линейна регресия [3]

На фигура 3 е представен изчислителния модел на линейна регресия, показващ приблизителното разпределение на пробни данни.



Фигура 3. Диаграма на линейна регресия след обучение [3]

Примери за непроследявани алгоритми са:

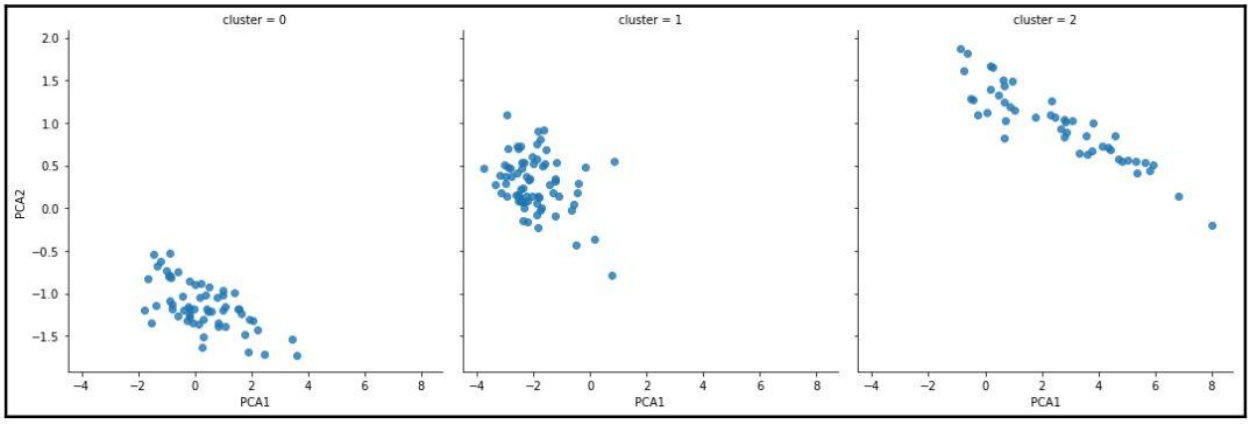
- намаляване на измеренията (Dimensionality reduction):
  - анализ на главните компоненти (Principal component analysis, PCA);
  - PCA ядро (PCA Kernel);
- клъстериране (Clustering):
  - клъстериране на k (k групиране, k-means);
  - йерархичен клъстерен анализ (Hierarchical cluster analysis, HCA).

На фигура 4 е представен код на алгоритъм за клъстериране, като е извършено свиване на размера на данни и след това чрез гаусова функция тези данни са класифицирани спрямо предназначението им.

```
import pandas as pd
import seaborn as sns

data_df = pd.read_csv("../datasets/clustering.csv")
data_df.describe()
X_data = data_df.drop('class_1', axis=1)
y_data = data_df['class_1']

from sklearn.decomposition import PCA

pca = PCA(n_components=2)
pca.fit(X_data)
X_2D = pca.transform(X_data)
data_df['PCA1'] = X_2D[:, 0]
data_df['PCA2'] = X_2D[:, 1]

from sklearn.mixture import GaussianMixture

gm = GaussianMixture(n_components=3, covariance_type='full')
gm.fit(X_data)
y_gm = gm.predict(X_data)
data_df['cluster'] = y_gm
sns.lmplot("PCA1", "PCA2", data=data_df, col='cluster', fit_reg=False)
```

Фигура 4. Клъстериране чрез използване на смесени модели на Гаус [3]

На фигура 5 е посочена диаграма, на която се вижда, че алгоритъма за клъстериране е успял автоматично да класифицира наличните данните по правилен начин, като се е позовавал единствено на собствена преценка, тъй като предварително получени данни за обучение не са предоставени.



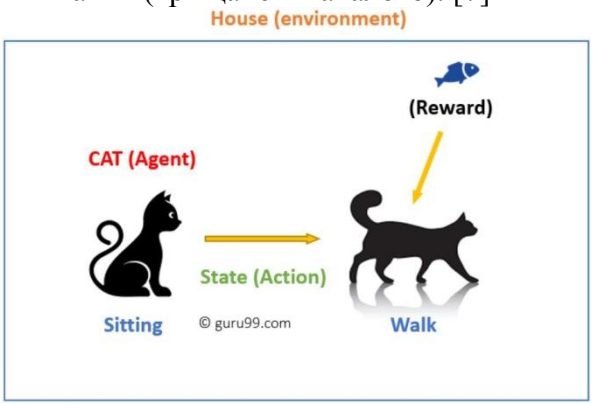
Фигура 5. Диаграма на клъстериране на данни след обучение [3]

Примери за “reinforcement” алгоритми са:

- Вериги на Марков (Markov process);
- Q-обучение (Q-learning);
- Обучение с времеви разлики (Temporal difference methods, TD)
- Методи на Монте Карло (Експерименти на Монте Карло, Monte Carlo methods) [3].

На фигура 6 е представен модел, в който се акцентира върху това как работи обучението с утвърждение. За тази цел е изследвано поведението на агент, който е изложен на въздействието на околната среда, в случая къщата, в която агента (домашен любимец - котка) живее, като за изпълнение на същинската част на обучението се подават команди от човек (собственика). Тъй като котката не разбира човешки език, не е възможно да и бъде казано директно какво да прави, затова се симулира ситуация и се наблюдава поведението на животното. Ако реакцията и е правилна, тя ще получи поощрение, а при втори подобен опит, котката ще изпълни сходно действие, но с по-голям ентусиазъм. Така домашния любимиц се учи какво трябва да направи

от положителни преживявания (награда - получена храна) и какво не трябва да прави, съответно от негативни преживявания (връщане в началото). [7]



Фигура 6. Извършване на reinforcement обучение [7]

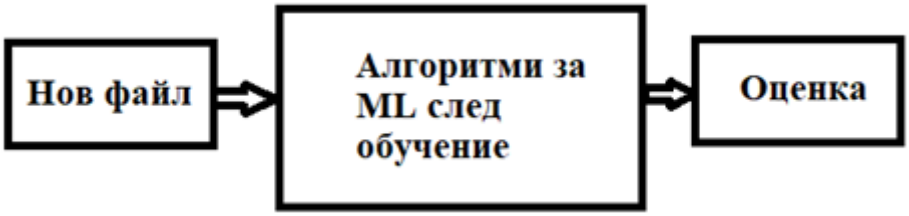
Резултатът от reinforcement обучението е:

- Агентът реагира на подадена му команда, като променя позицията си, преминавайки от статично състояние в динамично състояние, т.е извършва движение.
- Реакцията на агента е извършеното действие, а поведението му стратегия за избор на даденото действие, като се очаква да бъдат реализирани по-добри резултати в по нататъчни изследователски постановки.
- При успешно преминаване, агента получава награда (за да бъде стимулиран), а ако не успее да изпълни необходимото придвижване, получава наказание (трябва да започне отначало) [7].

Обучението с утвърждение изследва поведението на софтуерни агенти, в конкретния случай поведението на живо същество, като самото обучение представлява последователност от примерни действия, на които агента реагира по най-подходящия начин - чрез насърчаване и избягва неподходящите решения на проблема - чрез санкция.

3. Системи за оценка и вземане на решения

За да бъде прогнозата по-точна и алгоритъмът за ИИ да е коректен, се използват подалгоритми за машинно обучение (ML). Машинното обучение изисква предварително подготвени данни да се подадат към алгоритъма и той да се обучи кога вземането на решение ще е правилно и кога – не. В началото на обучението се задават различни параметри, които се настройват и впоследствие модифицират въз основа на получените резултати от вземане на решение. По-нататък започва самото обучение на мрежата за откриване на злонамерен софтуер, като се идентифицират връзките между кода и прогнозата. Най-често на алгоритмите за обучение се предоставят данни, които имат форма на написан програмен код на съответен, работен за системата, език. След като мрежата вече е обучена, всеки нов файл се представя на алгоритъма на ML за оценка, която удостоверява, дали софтуера може да премине (ако е безопасен) или не (фиг. 7). Веднъж „научен" софтуера за машинно обучение лесно и бързо може да идентифицира вида на атаката. Това е дълъг процес и изисква изследване на огромен брой файлове. Самият Artificial Intelligence налага ново обучение всеки път когато се появи необичаен, несрещнат до този момент проблем.



Фигура 7. Блок-схема на оценка с ML

След обучение невронните мрежи се използват в различни системи за осъщесвяване на киберзащита: За да се предвиди дали дадена система ще бъде атакувана или не от злонамерен софтуер, могат да бъдат използвани редица различни входни данни, които са асоциирани за дадена корпоративна мрежа, като например: IP адрес, географско местоположение, дата и час, операционна система, версия на операционната система, брой на отворените портове и техния тип, вид на атаката, естество на работния процес. На самия изход трябва да се направи прогнозиране или класификация.

Заключение

Включването на AI към киберсигурността към днешна дата е експериментална област, в която все още са налице множество проблеми, но постигнатите положителни резултати към настоящия момент са обнадеждаващи и обещаващи, като в близкото бъдеще използването му ще става обичайна практика, както по отношение на нови възможности за работа, така и по отношение на нови предизвикателства. Компаниите и организациите ще трябва да инвестират все повече в автоматизирани инструменти за анализ, прогнозиране и оценка, които позволяват бърз и адекватен отговор на настоящите и бъдещите провокации към киберсигурността. Сценарият, който се задава е комбинация от умения, между човешки оператори и машини.

References

[1] Грег, М. & Сантос, О., Сертифициран етичен хакер, Алекс Софт, 2020, ISBN 9546563935, стр. 247

[2] Проучване на Генезис Ривас, 2021, Is an Antivirus and Firewall enough to be cyber-protected?, URL: https://www.gb-advisors.com/is-an-antivirus-and-firewall-enough-to-be-cyber-protected/

[3] Parisi, A., Hands–On Artificial Intelligence for Cybersecurity, Packt, 2019, ISBN 978-1-78980-402-7, p.p. 12-20

[4] Николов, Л., Киберсигурност на КИС, НВУ „В. Левски", Шумен, 2021, ISBN: 978-619-7531-22-0, стр. 174.

[5] Mihail Iliev, Borislav Bedzhev, Monika Bedzheva, Plamen Yanakiev. A Method for Synthesis of Nearly Ideal Phase Manipulated Signals. IN: Proceedings of the 2020 IEEE International Conference on Information Technologies, BULGARIA, 2020, pp. 2

[6] Slavyanov, K. & Minchev, Ch., An Algorithm of Fuzzy Inference System for ISAR Image Classification, 2017, ISSN 1691-5402, pp.1

[7] Проучване на Даниел Джонсън, 2022, Reinforcement Learning: What is, Algorithms, Types & Examples, URL: https://www.guru99.com/reinforcement-learning-tutorial.html#what-is-reinforcement-learning

CYBERSECURITY ASSESSMENT METHODOLOGY FOR E-LEARNING PLATFORMS

Radostin S. Dimov, Linko G. Nikolov, Dimitar S. Dimov

Computer Systems and Technologies Department, Artillery, Air Defense Communication and Information Systems Faculty, National Military University „V. Levski", Shumen, Bulgaria, rsdimov95@gmail.com, linko.nikolov@aadcf.nvu.bg, dimovds99@gmail.com

***Abstract**: E-learning platforms trend to increase their impact across educational institutions. On one hand, it appears as an improovement and evolution of educational process. But on the other hand, as an online service, the cybersecurity risk is imposed. Lots of vulnerabilities may be found while performing online education. This research paper proposes necessary steps for cybersecurity tests of e-learning processess.*

***Keywords**: Cybersecurity Assessment, Penetration Testing, E-learning platforms, Hacking*

Introduction

In the last few years, due to Covid-19, there has been a trend towards increasing the use of e-learning platforms. At the same time, ensuring the online security of students and teachers is a major issue. For example, in March 26, 2022, personal data for roughly 820,000 current and former New York City public school students were compromised in the hack of a widely used online grading and attendance system, revealing what could be the largest-ever breach of K-12 student data in the U.S. Another example is on May 07, 2020, where „Unacademy", one of the largest online learning platforms in India, has faced a data breach and details of 22 million users, reported available for sale later. According to security firm Cyble Inc, a hacker is offering this users database, containing 21,909,707 records - $ 2,000. Furthermore, in 21 Sep 2020, while ransomware attacks against the education sector are common, experts say threat actors are actively targeting schools as classrooms switch to remote learning. As for writing this research paper, a brand new vulnerability found on 14.09.2022 is a clear text MS Teams token, kept in Window and Linux machines. It is presented at [3]. Very famous attack was the one, interrupted an EU meeting, fig. 1.

Fig. 1. Data breach in EU online meeting [4]

In such an insecure online environment, penetration tests are fundamental method for assessing the cyber security of communication and information systems. As the hackers are trying to gain unauthor-

ized access to the systems, these tests perform the same methods, attacks, and procedures to estimate the cyberhealth of the targeted e-learning environments for tests. The evolution in cyber defence system offers Artificial Intelligence (AI) with Machine Learning and Deep Learning [7] but such systems undergo further development.

1. E-learning model

Beig part of an educational institution and a partner in an European educational project, the NMU is using an online, or a.k.a „distance learning center" [5], developed and implemented in 2012. Requirements, proposed in [6] are followed but security issues are an area of interest. For the e-learning model, a system of user students and a system of didactic materials may be implemented in order to test (assurance of) the software quality (QA) such as the proposed analysis for indication which teaching technologies can be implemented in short-term courses [8].

The proposed methodology defines the main tasks in performing the analysis and assessment of cyber security of e-learning platforms. Due to security measures the tests should be performed in a secure controlled virtual environment. An example topology is presented on fig. 1. The model contains three separate subnets:

1. Management Network – Include the core services of the e-learning platform.
2. Cadet's Battalion Subnetwork – Physical subnet connected to the central management router. It is an everyday network used by the students.
3. Shumen Faculty Network – A separate network physically located in a different geographical location, used by students from a different faculty of the same university. They are supposed to connect to the e-learning platform through the Internet.

The model shown on figure 1 is just an example. In practice, the real structure of these kind of networks is much larger, including hundreds of end terminals, wide variety of nodes and different support services. The simulated environment may not be extended that much, as for educational purposes the number of end nodes will not necessarily result in manipulating the received results from the assessment tests.

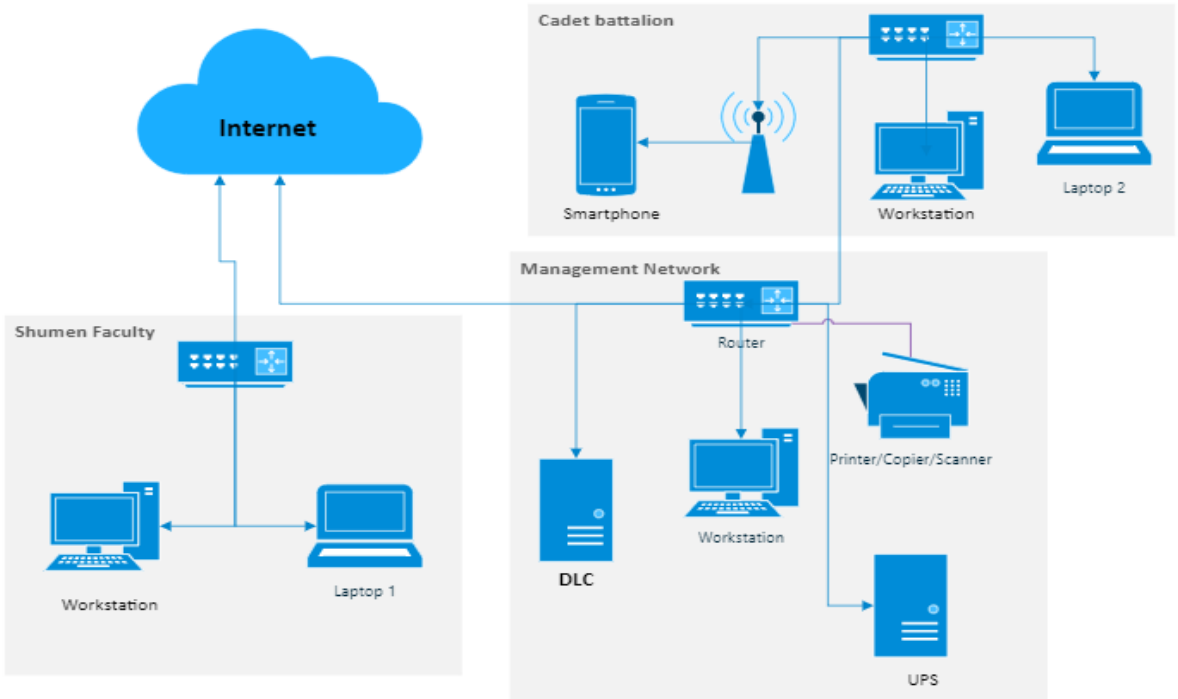


Figure 1: Distance learning environment

A proposed example of e-learning platform may be the famous "Moodle" [1] software. Anyway, it has vulnerabilities, presented in [2]. The distance, or online, learning environments are institutional-dependent and may vary in the number of subnets, hardware and software devices for security and services.

2. Penetraton testing methodology

The assessment methodology contains several phases including different kind of techniques and procedures which should be performed.

1. Information Gathering – collecting all the information we can about the targeted network and system. This includes reconnaissance, network discovering and vulnerability scanning with different tools.
    a. Netdiscover;
    b. Nmap/ZenMap;
    c. Dnesenum;
    d. DNSMap.
2. Vulnerability Scan – scan the network and hosts for any kind of vulnerabilities which can be used to compromise the system.
    a. OpenVAS Scan – in the proposed methodology OpenVAS is used as the main vulnerability scanning tool. It is an Open-Source vulnerability scanner with wide spectrum capabilities. Found vulnerabilities may be used as an injection points in the next phases;
    b. Nessus scanner – server-based scanner similar to OpenVAS project;
    c. Nmap Vuln Script;
    d. BED.
3. Network Security Assessment
    a. Cisco torch;
    b. Cisco Auditing Tool;
    c. Cisco Global Exploiter;
    d. Aircrack-ng;
    e. Fluxion;
    f. Ghost Phisher;
    g. Nmap
4. OS Security Assessment
    a. Metasploit
    b. Coreimpact
    c. Searchsploit
5. Web Security Assessment – include tests on the e-learning platform web interface)
    a. Burpsuite;
    b. Vega;
    c. Owaspzap;
    d. Nikto;
    e. Metasploit (using prebuild modules for web server platforms)
6. Database Security Assessment – testing the database management software for different kind of vulnerabilities.
    a. Sqlmap;
    b. Sqlninja;

   c. Oscanner
7. For better results, the assessment penetration tests may be performed on two stages:
   a. Network internal tests – assessments performed with the accessibility to the management network itself;
   b. Outside network tests – assessments performed from the public network.
8. It is recommended to divide the proposed assessment tests into two types:
   a. White Box Tests – supporting the penetration team with security information in order to help them in finding different vulnerabilities;
   b. Blind Tests – "Black box tests" provide the pentesting team with no security information about the targeted network/system. The idea is to search for vulnerabilities that could not be found otherwise.
9. Cybersecurity requirements definition – depending on the result analysis in the final report.

The Cheat sheet below presents the procedures which should be performed with their corresponding instruments and expected output.

Table 1: Cybersecurity e-learning platform methodology cheat sheet

№	Activity/Test phase	Instruments	Expected Output
1.	Information Gathering (Reconnaissance)	- Netdiscover; - Nmap/ZenMap; - Dnesenum; - DNSMap.	- IPs; - Network topologies; - Active services; - Used applications
2.	Vulnerability Scan (Scanning phase)	- OpenVas; - Nessus Scanner; - Nmap; - BED	- Network Vulnerabilities; - OS Vulnerabilities - Web Vulnerabilties; - DB Vulnerabilities
3.	Network Security Assessment: (Testing the network services and components)	- Cisco torch; - Cisco Auditing Tool; - Cisco Global Exploiter; - Aircrack-ng; - Fluxion; - Ghost Phisher; - Nmap	- users, passwords; - firmware vulns. exploits - misconfigurations; - Authentication Control; - Traffic encryption
4.	OS Security Assessment	- OpenVas Scanner; - Nessus Scanner; - Metasploit - Core Impact; - Searchsploit.	- users, passwords; - OS vulns. Exploits; - Configuration check; - Security Update Status
5.	Web Security Assessment (Web App check)	- Burpsuite; - Webscarab; - Owaspzap; - Nikto; - Metasploit	- XSS; - SQLi; - webApp (apache, nginx) vulnerabilities; - Update status; - Denail of Service; - URL manipulation
6.	DB Security Assessment	- Sqlmap; - Sqlninja; - Oscanner;	- users, passwords; - SQLi; - Privilege and role grants; - Data encryption;

№	Activity/Test phase	Instruments	Expected Output
			- Authorization Control; - Configuration Checking; - Update Status.
7.	Final Penetration testing report (detailed pentesting process overview)		- Assessment Overview; - Found Vulnerabilities; - Risk Factors; - Tools used; - Summary of Findings; - Evidence - Remediation and patching; - References
	Cybersecurity requirements definition	- Using Penetration testing report as a detailed cyberhealth estimation overview of the target network/system.	- Personalized cybersecurity policy; - Personalized cybersecurity recommendations

The penetration testing report should contain all the information collected in the assessment process and the methodology which was used. It should be written user-friendly and as understandable as possible. The pentesting results should be analyzed with proofs and evidences. The report should describe all the findings with discovered vulnabilities, and tools used by the pentesting team. One of the most important parts of the document is the remediation and patching section. This part of the document has to provide the clients with not only recommendations, patches and vulnerability fixes, but also a detailed information on how exactly to do that. An assessment methodology contains several phases including different kind of techniques and procedures which should be performed.

Conclusion

Data breaches in online platforms seem to be an everyday event and via the proposed methodology in this paper the aim is to perform adequate and correct cybersecurity tests, after which a Cybersecurity requirements policy to be creted. Most of the software described is an open source framework, but licensed functionality should be provided in order to perform deep analysis and harder security configurations and implementations.

Acknowledgments

This research paper is created in favour of Digital Competences for Improving Security and Defense Education (DIGICODE) project, funded by EU under the "Erasmus+" program, key action 02.

References

1. E-learning management system „Moodle", URL: https://moodle.com/
2. Moodle vulnerabilities, URL: https://www.cvedetails.com/vulnerability-list/vendor_id-2105/product_id-3590/Moodle-Moodle.html
3. Zero day attack for clear text token, kept in Windows and Linux machines, URL: https://www.bleepingcomputer.com/news/security/microsoft-teams-stores-auth-tokens-as-cleartext-in-windows-linux-macs/

4. Naomi Adedokun, databreach in EU online meeting, URL: https://www.express.co.uk/news/world/1363061/eu-news-defence-ministers-call-gatecrash-video-rtl-news-Daniel-Verlaan-vn

5. Distance learning center of NMU "V. Levski", URL: https://doi.org/xx.xxx/yyyy

6. M. Bedzheva, Iliev M., P. Boyanov, B. Bedzhev, Ts. Tsankov, Requirements to the Personal Work Stations in the University's Computer Laboratories, 29th annual conference of the European association for education in electrical and information engineering (EAEEIE), Ruse, 2019

7. Borisova, A., „Contemporary languages for programming artifical intelligence", Proceedings of International Scientific Conference ―Defense Technologies, Shumen, 2019, ISSN 2367-7902, pp. 373

8. Slavyanov, K., „Fuzzy logic procedure for drawing up a psychological profile of learners for better perception in courses", Environment. Technology. Resources. Rezekne, LatviaProceedings of the 12th International Scientific and Practical Conference. Volume II, Print ISSN 1691-5402, p.140, http://dx.doi.org/10.17770/etr2019vol2.4073

RESEARCH OF DIFFERENT TYPES OF DECODE ALGORITHMS OF TURBO CODES AND THEIR COMPATIBILITY WITH ENCRYPTION DEVICE

Stanimir H. Parvanov, Dimitar S. Dimov, Ivan Y. Radev

Communication Networks and Systems Department, Artillery, Air Defense, Communication and Information Systems Faculty, National Military University „V. Levski", Shumen, Bulgaria, sspar-vanov@gmail.com, dimovds99@gmail.com, secterity@abv.bg

***Abstract**: The noise resistance of the received signal in the main frequency band are from particular importance in the operation of communication equipment, as it plays a key role in ensuring the quality and reliability of the transmitted information. The study of the probability of the occurrence of a digital error is carried out on the basis of controlled sequences of digital signals and taking into account the lost bits. A method for correcting such digital errors is noise-resistant codes, the most widely used of which are convolutional codes and Turbo-codes. However, their effectiveness is a matter of constant analysis and research by specialists in communication techniques and technologies.*

***Keywords**: turbo codes, error correction, encryption, decode algorithm*

Introduction

Turbo codes are used in 3G/4G Mobile communications (e.g. in UMTS and LTE), in satellite communications and others where engineers seek to perform reliable information transfer over communication connection with limited bandwidth or latency in available noise disrupting the. Turbo codes are an encoding technique that aids reliable data transmission. Due to the special structure of the encoder and iterative decoder, this communication algorithms can achieved to the Shannon limit signal-to-noise ratio. However, redundant bits in the encoding should reduce bandwidth efficiency. The method of performing part of the bits could optimize the bandwidth usage. In this report, we focus on the analysis of recent decoding methods and the possibility to encrypt the transmitted information. The noise resistant of the received signal in the main frequency band is of particular importance in the operation of the communication systems, as it has an exceptional role in ensuring the quality and reliability of the transmitted information. The study of the probability of the occurrence of a digital error is carried out on the basis of controlled sequences of digital signals and taking detecting th lost or wrong bits. A method for correcting such digital errors with noise-resistant codes, the most widespread application of which is found in convolutional codes and turbo-codes. Their effectiveness, however, is a matter of constant analysis and research by specialists in communication techniques and technologies. In this report, simulation models of a special class of Turbo-codes will be used and a comparison of the achieved noise resistnant will be performed, with research done in reports and considered in the literature.

1. Communication model implemented in "Matlab" simulation environment

Matlab simulation environment of Simulink software was used to simulate the study. Figure 1 shows the communication channel with an added Matrix Interleaver for shifting the information by columns and rows. The purpose of adding the "Matrix Interleaver" block installed after the message source is to encrypt the transmitted information.

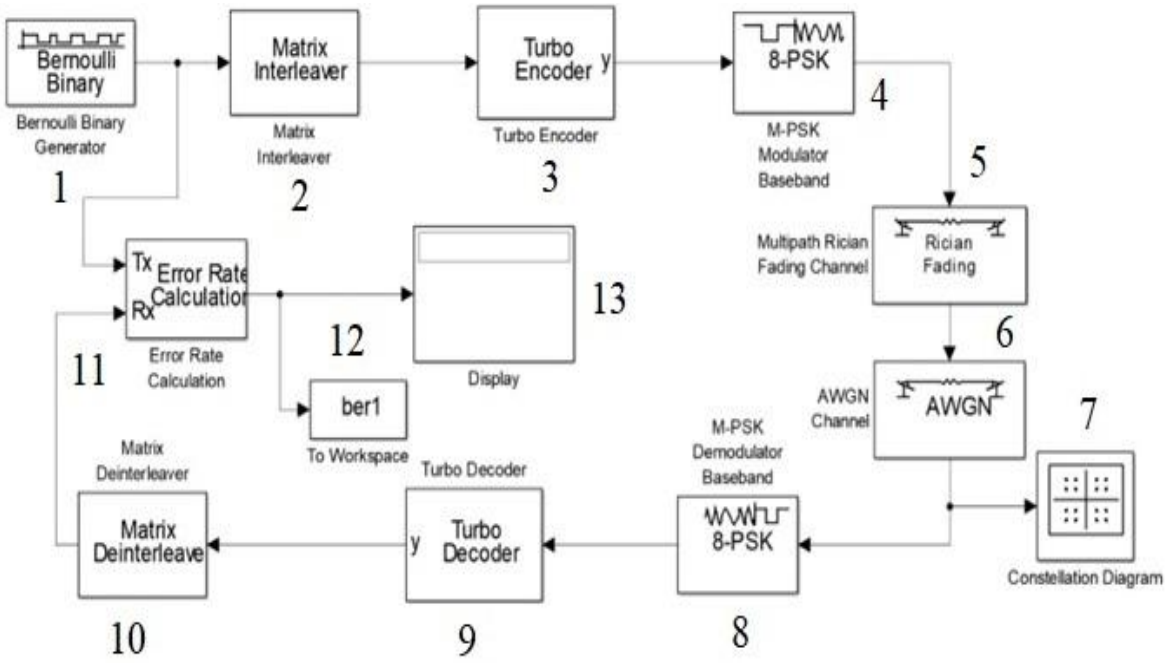


Figure 1: Block diagram of a communication system with Turbo coding and 8-PSK modulation

Composition of the block diagram of figure 1:

1. Message source
2. Scrolling block by columns and rows
3. Turbo encoder
4. Block for eight-fold phase manipulation
5. Rice channel
6. Block adding Additive white Gaussian noise
7. Constellation diagram
8. Eight-fold phase demodulator
9. Turbo decoder
10. Moving block by columns and rows
11. Error calculator
12. Block generating curves (results)
13. Display

Brief description of the operation of the communication channel.

The Bernoulli Binary Generator generates "0" and "1" with a set probability of 0.5 in order to simulate the reception of digital signals from a mobile network. The generated 0's and 1's go to the input of the Matrix Interleaver, which shuffles the bits by rows and columns, then the bit sequences go to the Turbo coder, which has a polynomial generator poly2trellis (7, [7 4], 170)'), poly2trellis (7, [15 11],170)') or poly2trellis (7, [31 26],170)').(table 1).

The condition are as follows that only the sender and receiver know the polynomials. The turbo coder adds an excess of bits in order to increase the noise resistant of the transmitted data, the useful information and this added excess goes to the 8-PSK modulator, where the signal is modulated from digital to analog and broadcast into the area, i.e. AWGN Channel and Multipath Rician Fading Channel. Rice channel imitates signal propagation on different paths with different attenuation and delay, and AWGN Channel adds noise to the transmitted useful signal with information redundancy, and the sum of useful signal, information redundancy and noise falls on the 8-PSK, Demodulator, where the signal is restore digitally.

Table 1: Forming polynomials in Turbo coder

N	K	Generator
7	4	$x^3 + x + 1$
15	11	$x^4 + x + 1$
31	26	$x^5 + x^2 + 1$

The received digital signals enter the Turbo Decoder with the decoding method SOVA, log-MAP or MAX-log-MAP and number of iterations: 1÷8, the signal is decoded to its original form and enter the input of the Error Rate Calculator, which calculates how are the bits sent, how many are received and determines the BER (Bit Error Rate) value. Adding noise to the channel is done by the relationship between E_S/N_0 and SNR, both expressed in dB, is as follows:

$$\frac{E_S}{N_o} = \frac{T_{sym}}{Tsamp} SNR, \quad (1)$$

$$\frac{E_S}{N_o} = \frac{Eb}{N_o} + 10log_{10}k\ [dB]. \quad (2)$$

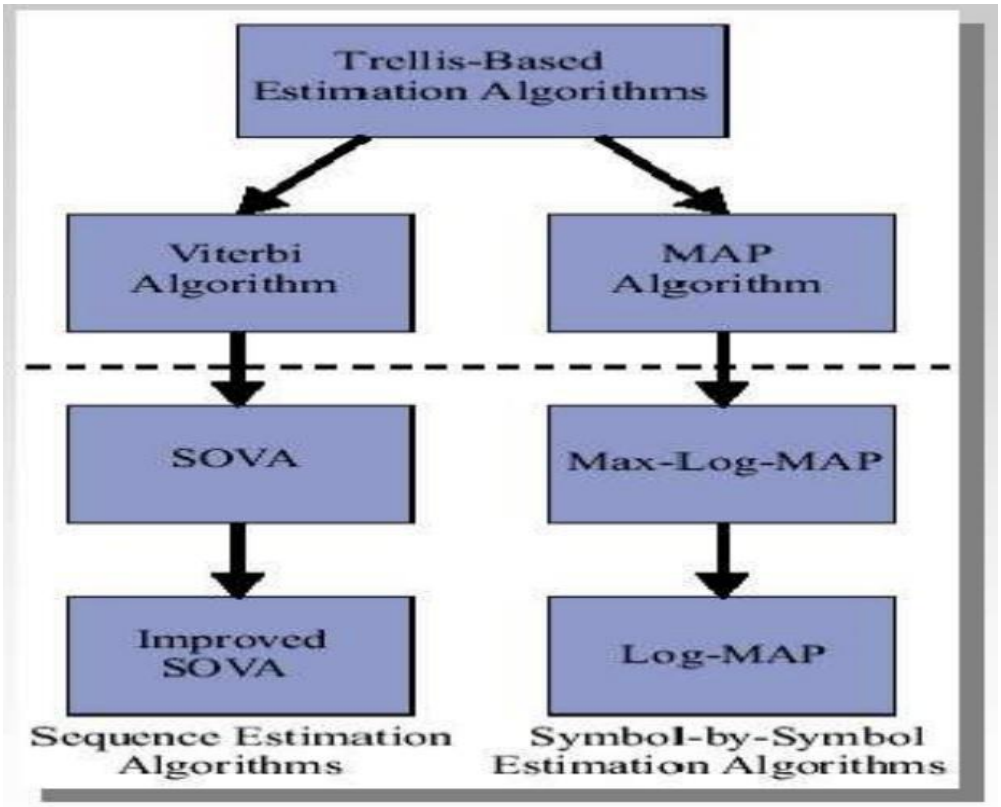


Figure 2: Turbo decoding algorithms

In (2) T_{sym} is the symbol period of the signal, a $Tsamp$ is the signal noise overlay period. For example, if a complex signal is represented by a factor of 4, then $\frac{E_S}{N_o}$ exceeds the ratio:

$$SNR = 10log_{10}4. \quad (3)$$

In [1], a report was reviewed that analyzed the performance of turbo decoders and the different types of decoding. Figure 2, below, shows the various decoding algorithms available for decoding turbo

codes. All algorithms are based on grid-based computing algorithms. Trellis diagrams are classified into two types. They are sequence evaluation algorithms and symbol-by-symbol evaluation algorithms. Viterbi algorithms, SOVA (soft output Viterbi algorithm) and improved SOVA are classified as sequence estimation algorithms. Like maximum likelihood (MAP) algorithms, MAX-log-MAP (maximum a posterio) and LOG-MAP algorithm are classified as symbol-by-symbol algorithms. In conclusion, we should note that symbol-by-symbol algorithms are more complex than sequence estimation algorithms, but their performance is much better. For a more detailed consideration of how the algorithms works, see [4, 5].

2. Study of the results of the implemented communication model in the "Matlab" simulation environment

In [1], the types of algorithms for decoding the turbo codes when spreading the signal in an AWGN channel are testing. Figure3 shows the results for 4 decoding algorithms and it is clear that the Soft-Output Viterbi Algorithm SOVA (Soft-Output Viterbi Algorithm) achieves the best results while maintaining a signal-to-noise ratio = 2dB, while not allowing a wrong bit ratio BER (bit error rate) = 10^{-6}.

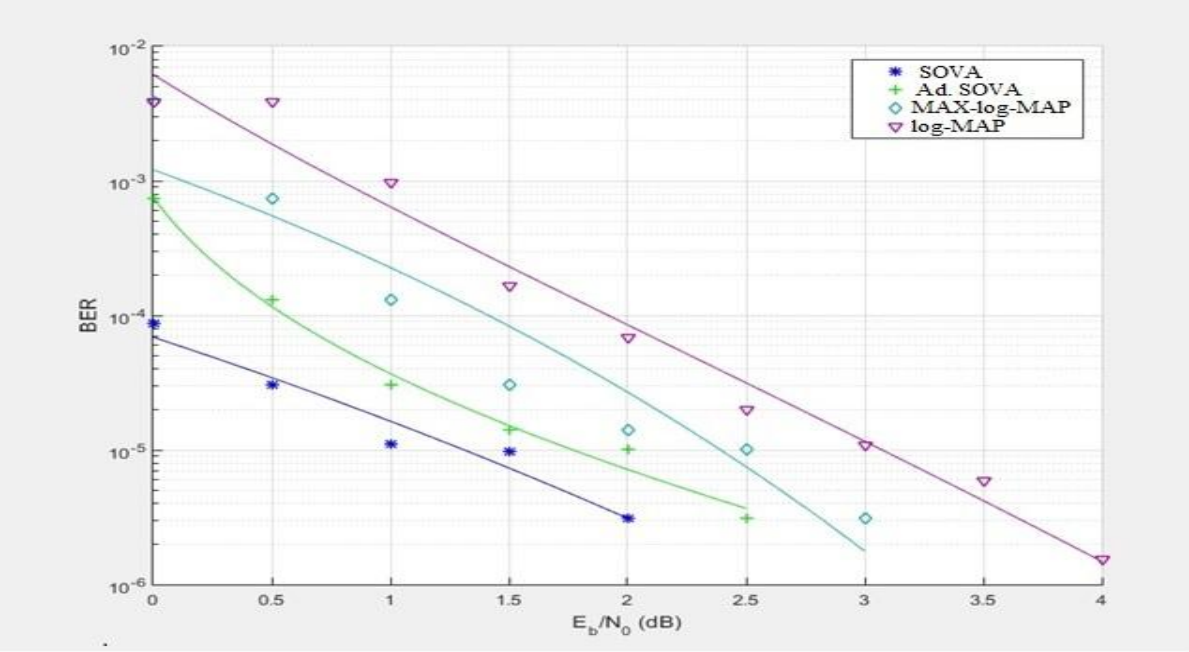


Figure 3: Results obtained with different turbo decoding algorithms when spreading signals in an AWGN channel

Figure 4 shows results [1] from research of types of turbo code decoding algorithms when propagating the signal in a Rice channel. Figure 4 shows the results for 3 decoding algorithms and you can see that the Soft-Output Viterbi Algorithm SOVA (Soft-Output Viterbi Algorithm), again achieves the best results compared to the other methods, although it requires signal amplification with half a decibel, namely signal-to-noise ratio = 2.5dB, with no bit error rate BER (bit error rate) = 10^{-6}.

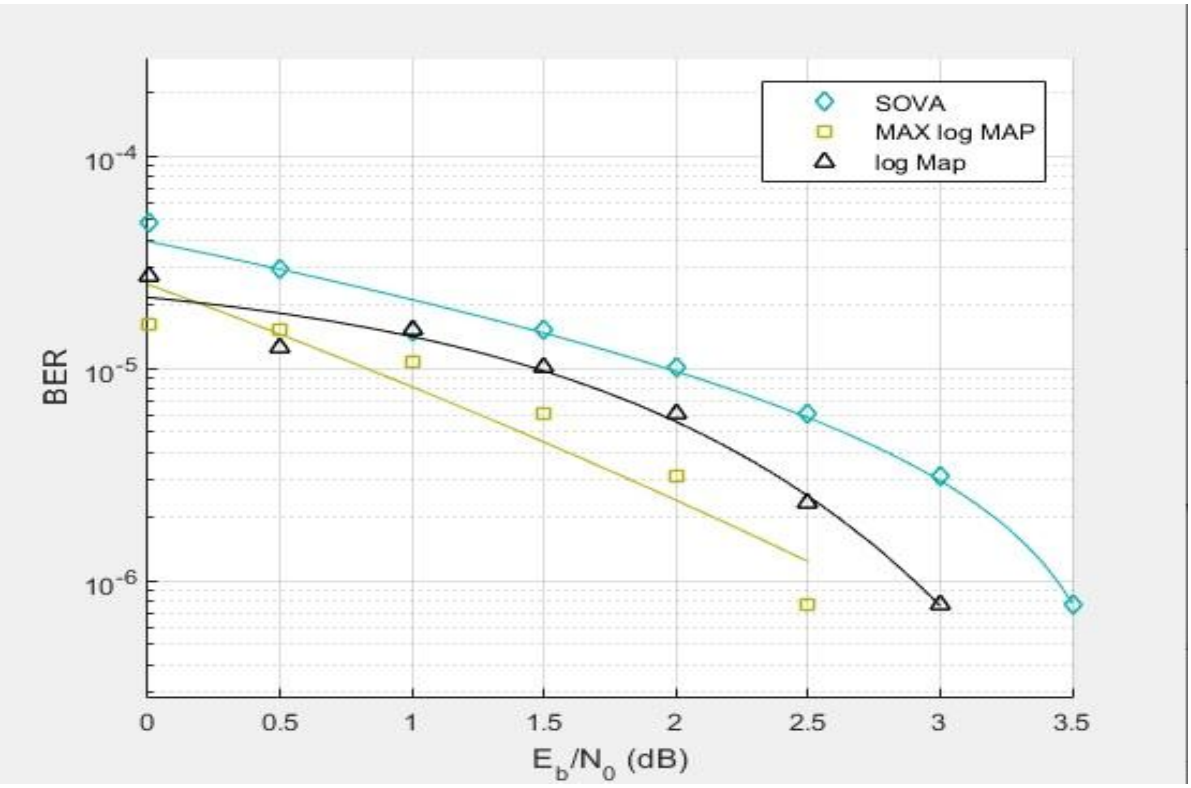


Figure 4: Results obtained with different turbo decoding algorithms when spreading signals in an AWGN channel

The noise resistant of the communication channel is evident from the results, but this report investigates whether the communication system will be significantly slowed down by adding an encryption device and also whether the signal-to-noise ratio (SNR) will be reduce ratio BER = 10^{-6}.

Results achieved in simulations from this report

Figure 5 shows the results obtained with the row and column shift block added. It can be seen from the graph that the results have reduced by half a decibel with the best signal-to-noise ratio being achieved with the SOVA decoding method. It should be noted that information transmission is slightly delayed as information transmission when setting the Bernoulli Binary Generator (the message source) to 1296384 samples as 1 sample = 3 bits, and the transmission time for simulation with added Matrix Interliever is equal to 13.91s, and the simulation without Matrix Interliever is 13.72s. This means that for a half-decibel amplification of the signal-to-noise ratio and a minimal delay in the transmission of information, encryption (unintelligibility, impossibility of reading) of the transmitted information can be achieved.

Figures 6 and 7 illustrate the Constellation diagrams of 8-PSK modulation, at SNR= 2dB and SNR= 4dB. It is clearly seen that with the SOVA decoding method at 2dB, the constellations are much more concentrated, than the result achieved at SNR=4dB with the Log-MAP decoding method, where the constellations are more scattered.

A summary of the results is shown in Table 2, from which result it is getting clear that for the same decoding algorithms with the addition of a scrambling block (encryption device),the SNR is reduced by 0,5dB and there is also minimally delays data transmission but the channel becoming unreadable for the opponent side.

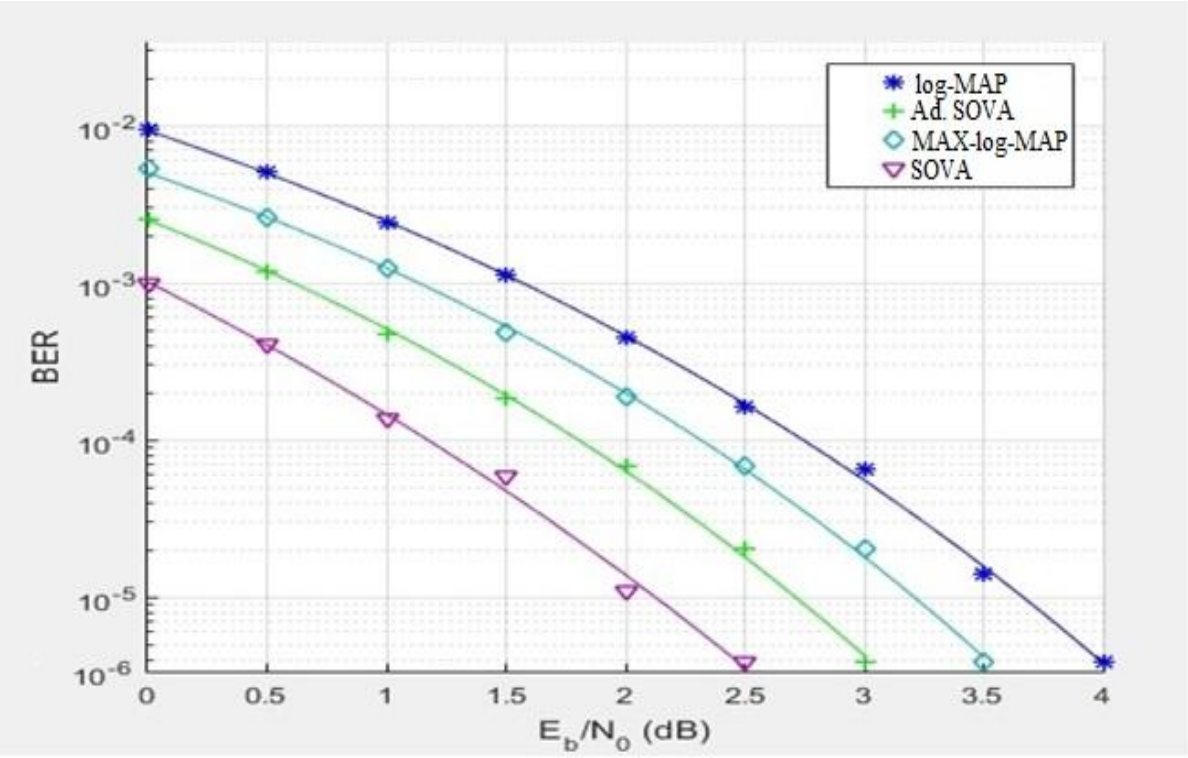


Figure 5: Results obtained with different turbo decoding algorithms when spreading signals in an AWGN channel

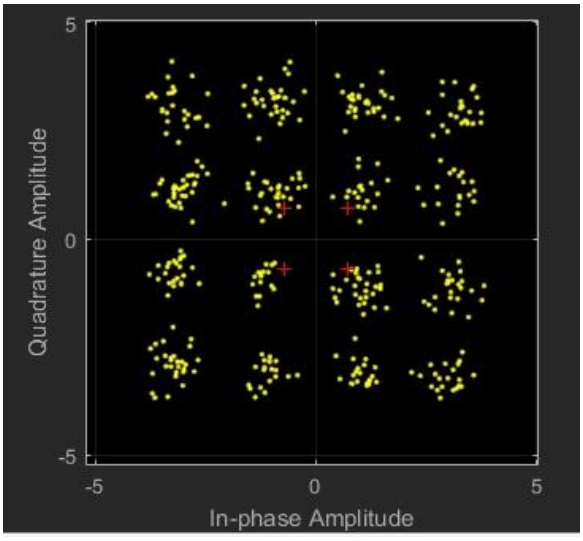


Figure 6: log-MAP algorithm при 4dB

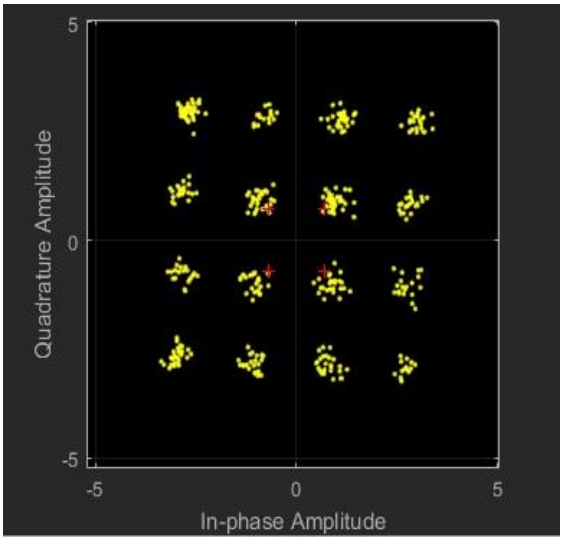


Figure 7: SOVA algorithm при 2dB

Table 2. Turbo coding with 8-PSK modulation and different decoder algorithms in AWGN and Rice Channel

Type of codding	**Spreading channel**	**Type of modulation**	**Decoding methode**	**SNR [dB]**
ТК	AWGN Channel	8-PSK	SOVA	2
ТК	AWGN Channel	8-PSK	MAX-log-MAP	3
ТК	AWGN Channel	8-PSK	log-MAP	4

Type of codding	**Spreading channel**	**Type of modulation**	**Decoding methode**	**SNR [dB]**
TK	Rician Channel	8-PSK	SOVA	2.5
TK	Rician Channel	8-PSK	MAX-log-MAP	3
TK	Rician Channel	8-PSK	log-MAP	3.5
TK	AWGN Channel Rician Channel	8-PSK	SOVA	2.5
TK	AWGN Channel Rician Channel	8-PSK	MAX-log-MAP	3.5
TK	AWGN Channel Rician Channel	8-PSK	log-MAP	4

Conclusion

In turbo coding, the selection of the forming polynomial, the type of modulation, the decoding method and the number of iterations are of particular importance, and it should be noted that the more iterations, the higher the sensitivity of the decoder and the lower the probability of an error. From the results in [1] showing the state-of-the-art performance of Turbo decoders under various decoding algorithms and the identical studies in the present report with the addition of a Matrix Interleaver block, it is understood that the system becomes more complicated by performing 0.5dB down, as a delay in the transmission of information due to the impossibility of understanding the transmitted content when someone listening to the channel.

References

1. Salim, M., Yadav, R. P., & Ravi, K. S., (2010), Performance Analysis of Log-map, SOVA and Modified SOVA Algorithm for TurboDecoder, *Dept. of Electronics & Communication Engineering, MNIT, Jaipur, Rajasthan (India)*
2. Chen, Y.-F., & Yang, Ch.-Y., (2006), Performance Analysis of Punctured Turbo Code under An AWGN Channel, *Graduate Institute of Networking and Communication Engineering Chaoayang University of Technology*
3. Pillay, N., Xu, H., & Takawira, F, (2010), Repeat–Punctured Superorthogonal Convolutional, Turbo Codes On AWGN Channels, *Electronic and Computer Engineering, University of Kwa*
4. Mugaibel, A. H., & Kousa, M. A., (1999), Understanding Turbo Codes, *King Fahd University of Petroleum and Minerals*
5. Sadjadpour, H. R., (2000), Maximum A Posteriori Decoding Algorithms For Turbo Codes, *Proceedings of SPIE Vol. 4045 (2000)*
6. Kumar, S., (2011), Performance Evaluation of Asymmetric Turbo Codes Using Log-MAP Decoding Technique, *2011 International Conference on Devices and Communications*
7. Oletu, G., (2011), The performance of turbo codes for wireless communication systems, *2011 3rd International Conference on Computer Research and Development*
8. Jasim, Y., A proposed Improvement Model for Turbo Codes Performance by Using Additional Interleaver

TRENDS IN DEVELOPMENT OF THE SMART GRINDS

Dobry S. Stoynov, Dimitar I. Raev, Dimitar St. Dimov

Communication Networks and Systems Department, Artillery, Air Defense Communication and Information Systems Faculty, National Military University „V. Levski", Shumen, Bulgaria, dobri_stoyanov@mail.bg, djlumpox00@gmail.com, dimovds99@gmail.com

***Abstract**: Today the electric power industries of the most developed countries are rapidly transformed in so-called smart grids. Smart grids can trade electricity with the consumers and that has become possible with the advent of advanced metering and sensing technologies, e.g., Industrial IoT, new distributed energy resources and ultra-ultra-reliable low latent communications. The abilities of smart grids make them extremely important for the forth industrial revolution advancement and give a way for a deep positive chage of the life-stile of all people in the world. Due to these reasons the paper aims to outline the technologies and the approaches, which should provide the transformation of today electric power system of Bulgaria in a smart grid.*

***Keywords**: electric power industry, smart grids*

Introduction

In the last decade, the direction of scientific and technological innovative transformation of the electric power industry, based on a new concept called *smart grid*, has been intensively developing all over the world. Subsequently, the smart grid concept was recognized and developed in almost all major industrialized and dynamically developing countries, where a wide range of activities in this direction is deployed. In 2004 in the countries of the European Union (EU) the program, called European Energy System of the Future (EEST), was created in order to coordinate work and develop an unified strategy for the development of the electric power industry and the smart grid technological platform. The ultimate goal of EEST is to elaborate and implement approaches for the development of the European energy system until 2020 and beyond.

The smart grid concept is an integral and comprehensively agreed system of views on the innovative transformation of the electric power industry, based on a holistic forecast of its role and place in modern and future society, defining the requirements for it, approaches to ensuring these requirements, principles and methods of implementation and the necessary technological basis for implementation.

The above facts show that the smart grids are extremely important for the forth industrial revolution advancement and they will positively chage the life-stile of all EU sitizen. Due to these reasons the paper aims to outline the technologies and the approaches, which should provide the transformation of today electric power system of Bulgaria in a smart grid.

The paper is structured as follows. Firstly, the reasons for emergence and development of electrical smart grids are described and systematyzed. Secondly, the basic principles of the smart grid concept are presented. Within this framework the key requirements (values) of the new electric power industry are outlined. Thirdly, the key technologies for smart grid development and progress are analysed and systematyzed. At the end, the basic directions of transformation of today electric power system of Bulgaria in a smart grid are summarized.

1. Reasons for the smart grid concept emergence and development

The reasons for the emergence of the smart grid concept are connected, first of all, with the fact that in recent decades, the predicted development throughout the world is characterized by the emergence of a number of factors that determine the need for fundamental changes in the electric power industry:

- the constant increase in the cost of electricity around the world;
- the need to improve the energy and environmental efficiency of the electric power industry;
- growing consumer demands for reliability and quality of power supply, the emergence of progressive technologies as a result of scientific and technical progress, which have not found proper application in the modern electric power industry;
- decrease in reliability of power supply;
- changing the conditions for functioning of electricity and energy markets.

Accounting the above circumstances, in the developed countries a deep analysis of possible ways for the development of the electric power industry was carried out [1], [2], [3], [4], [5], [6]. Its results showed the presence of serious limitations on the development of the industry within the framework of the previous extensive concept, based mainly on the improvement of certain types of equipment and technologies. The following factors were considered as the most significant:

- limited possibility of further increase both volumes and the efficiency of generating capacities due to the exhaustibility in the long term of non-renewable fuels and the rapidly increasing technogenic and infrastructural development risks as well as the emergence of significant environmental restrictions, curbing the development of network infrastructure, primarily in areas with a high population density;
- low potential for enhancement the efficiency of resource use: the existing technological base of the power industry has practically exhausted the possibilities for increasing the productivity of equipment;
- limited investment resources for the construction of new energy facilities and the development of network infrastructure.

The results of studies in developed countries have shown that taking into account all factors in the future development of the electric power industry requires a change in the principles and mechanisms of its functioning that can ensure social development, a breakthrough increase in consumer properties and energy efficiency. This decision required the development of a new concept for the innovative development of the electric power industry, which, on the one hand, would correspond to modern views, goals and values of social development, emerging and expected needs of people and society as a whole, and, on the other hand, would take into account maximally the main trends and directions of scientific and technological progress in all sectors, spheres of life and activity of society. The smart grid became such a concept. It should be noted that the developed approaches and variants of the concept that are publicly presented today are not perceived as something complete and normatively fixed - their development, concretization and approbation is set as one of the main tasks in the developed countries.

2. Basic principles of the smart grid concept

The analysis of the data, presented in a number of studies [1], [2], [3], [4], [5], [6], allows the following assumptions, adopted in the development and elabortion of the smart grid concept in the technologically leading countries, to be formulated:

1. The smart grid concept involves a systemic transformation of the electric power industry (power system) and affects all its main elements: generation, transmission and distribution (including utilities), sales and dispatching;

2. The energy system is considered in the future as an Internet-like infrastructure designed to support energy, information, economic and financial relationships between all subjects of the energy market and other interested parties;

3. The development of the electric power industry should be aimed at elaborating the existing and creating new functional properties of the power system and its elements, ensuring to the greatest extent the achievement of the key values of the new electric power industry, made as a result of a joint vision of the goals by all interested parties and ways of its progress;

4. The electrical network (all its elements) is considered as the main object of the formation of a new technological basis, which makes it possible to significantly improve the achievements and create new functional properties of the power system;

5 The development of the concept comprehensively covers all the main areas of development: from research to practical application and replication, and should be carried out at the scientific, legal, technological, technical, organizational, managerial and information levels;

6. The implementation of the concept is innovative in nature and gives impetus to the transition to a new technological order in the electric power industry and in the economy as a whole.

Accounting all the above asumptions, the general model of the smart grids could be presented as shown on fig. 1 [6].

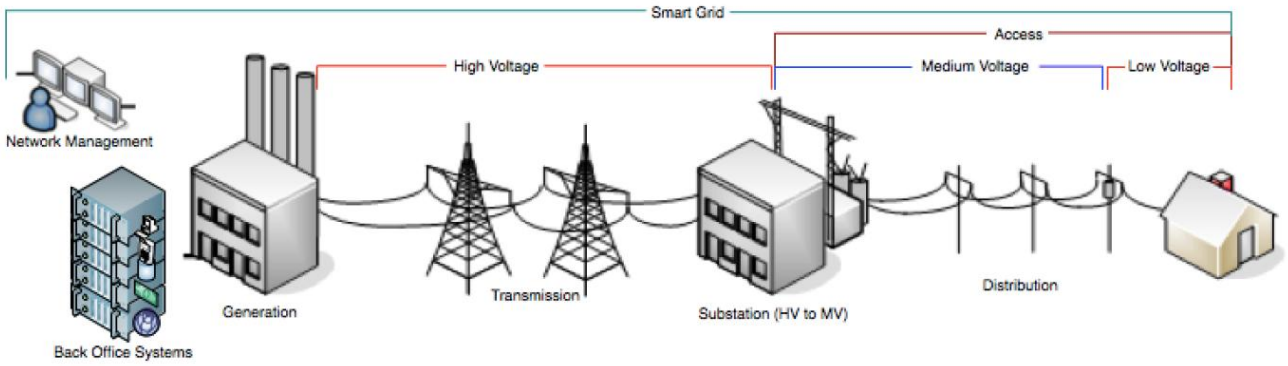


Figure 1: General model of Smart Grid

Within the framework of the developed smart grid concept, the variety of requirements of all interested parties (the state, consumers, regulators, energy companies, sales and utility organizations, owners, equipment manufacturers, etc.) can be reduced to a group of so-called key requirements (values) of the new electric power industry, formulated as [1], [2], [3], [4], [5], [6]:

- availability - providing consumers with energy without restrictions, depending on when and where they need it, as well as on the paid quality;
- reliability - the ability to withstand physical and informational negative impacts without total shutdowns or high costs for restoration work, the fastest recovery (self-healing);
- cost-effectivenes - optimization of tariffs for electricity for consumers and reduction of system-wide costs;
- efficiency - maximizing the positive effects of using all types of resources and technologies in the production, transmission, distribution and consumption of electricity;
- organic interaction with the environment - the maximum possible reduction of negative environmental impacts safety - preventing situations in the electric power industry that are dangerous for people and the environment.

Here it should be outlined that all the key requirements (values) listed above are supposed to be considered as equal, and the degree of their priority, level and correlation are not general, normatively fixed for everyone. More over, they can be determined and implemented for each considered subject of energy relations (energy company, region, city, household, etc.) in a fully individual way. Consequently, the task of developing the energy sector from a predominantly balance one is transformed into the task of creating, developing and providing the consumer and society as a whole with a kind of "menu" of energy opportunities.

Within the framework of the smart grid concept for achieving the key requirements (values), the development of the following functional characteristics is expected [1], [2], [3], [4], [5], [6]:

1. Self-healing in case of emergency disturbances: the power system and its elements must constantly maintain their technical condition at the required level by identifying, analyzing and switching the control so that the accidental damages to be avoided;

2. Motivation of the active behavior of the end consumer - providing the possibility for consumers to independently change the volume and consumer characteristics (level of reliability, quality, etc.) of the received energy, balancing their needs and the capabilities of the energy system on the base of information about the characteristics of prices, volumes, reliability, quality and etc.;

3. Resistance to negative influences - the presence of special methods to ensure stability and survivability, reducing the physical and informational vulnerability of all components of the energy system and contributing to both prevention and its rapid recovery after accidents in accordance with energy security requirements;

4. Ensuring the reliability and quality of electricity by moving from a system-oriented approach (System-based approach) for providing these properties to a customer-oriented (Customer-based), and maintaining different levels of reliability and quality of energy in different price segments;

5. Variety of types of power plants and energy storage systems (distributed generation) - optimal integration of power plants and energy storage systems of various types and capacities by connecting them to the power system according to standardized technical connection procedures and the transition to the creation of "micropower systems" (microgrids) on the side of end users;

6. Expansion of power and energy markets to the end consumer - open access to the active consumer and to markets for distribution of electricity, contributing to an increase in the productivity and efficiency of the retail market;

7. Optimization of asset management - transition to remote monitoring of production assets in real time, integrated into corporate management systems, as well as improvement the efficiency of operating modes and the exploitation, repair and replacement of equipment, according to its condition, and, as a result, ensuring a reduction in system-wide costs.

3. Key technologies for smart grid progress

The realization of the key requirements (values) and the implementation of the functional properties (fundamental characteristics) of the smart grid concept depend significantly on several key (basic) technological areas and technologies (technological basis) that require appropriate innovative development [1], [2], [3], [4], [5], [6]. Here, the technological basis is understood as a set of technologies which provide a consistent structure of intermediate and final products and services at a certain stage in the development of the industry. In developed countries the smart grids' technological basis is considered as a necessary condition for ensuring technological continuity of the transition from the existing technological base of the energy sector to a new one at the lowest possible costs. In the USA and the European Union, these problems are supposed to be solved by creating a certain regulatory field (space), which should be a wide system of standards and requirements for functions, elements, devices, interactions, and etc. For example, more than 100 types of standards are planned to be developed in the USA, within which developers and manufacturers would obtain the right and opportunity to create an offer, and users (energy companies and consumers) would obtain the opportunity to form their "own" smart grid, using puzzle principle (effect).

In order to create a new, innovative technological basis for the energy sector, five groups of key technological areas, providing a breakthrough character, have to be formed and elaborated [1], [2], [3], [4], [5], [6]:

G 1) Measuring instruments and devices, including, first of all, smart meters and smart sensors;

G 2) Advanced control methods - distributed intelligent control systems and analytical tools to support communications at the level of power system facilities, operating in real time and allowing the

implementation of new algorithms and methods of power system control, including control of its active elements;

G 3) Advanced technologies and components of the electrical network – flexible alternative curent (AC) and direct current (DC) transmissions, , superconducting cables, semiconductor power electronics, storage devices, etc.;

G 4) Integrated interfaces and methods for decision support, demand management, distributed monitoring and control system (DMCS), distributed generation management system (DGMS), automatic process measurement system (AMOS), etc., as well as new scheduling methods and design of both development and operation of the power system and its elements;

G 5) Integrated communications, which allow the elements of the first four groups to provide interconnection and interaction with each other, which is the essence of the smart grid, viewed as a technological system.

The above analysis demonstrates that integrated communications should provide high stabily and resistance of the power grid management and control in normal and extraordinary conditions, caused by natural and man-made disasters, as well as by cyberattacks, performed by criminal or/and terroristic groups. These abilities can be formed by the following approaches.

A 1) Building the smart grid communications as a a complex of optical, radio (wireless) and wired (including Power Line Communications – PLCs) communication systems, which compensate for each other's weaknesses [7].

A 2) Centralized and synchronous usage of cryptographic tools, communication protocols, spread spectrum signals and advanced signal processing algorithms [8], [9], [10], [11], [12].

Conclusion

In the paper the basic principles of the smart grid concept are analyzed. On this base the key technologies for smart grid development and progress are systematyzed.

The results of the study, presented in the paper, could be useful in the processes of implementation and development of smart electric grids in the Republic of Bulgaria.

References

1. Erol-Kantarci, M., (2021), Smart Grid? Yes, AI Says: Bring It on!, *IEEE CTN Issue: April 2021*
2. Wikipedia, (2016), Smart grid, Retrieved from https://en.wikipedia.org/wiki/Smart_grid
3. Ul Haquea, A., Mandalb, P., Menga, J., & Pineda, R., (2012), Performance evaluation of different optimization algorithms for power demand forecasting applications in a smart grid environment, *Procedia Computer Science 12 (2012)*, pp. 320 - 325
4. Almassalkhi, M., Frolik, J., & Hines, P., (2022), Packetizing the power grid, *IEEE Spectrum, February 2022*, pp. 43 – 47
5. Armstrong, T., (2022), Green buildings get a boost: wireless sensor nodes as a key application for energy harvesting, *EE Times Europe, May 2022*, pp. 15 – 20
6. ITU-T, (2010), Applications of ITU-T G.9960, ITU-T G.9961 transceivers for Smart Grid applications: Advanced metering infrastructure, energy management in the home and electric vehicles, *ITU-T Technical Paper 06/2010*
7. Stoyanov, D., Bochev, L., & Radev, I., (2021), Approaches for cybersecurity enhancement of the energy infrastructure management, *Proceedings of International Scientific Conference "Defense Technologies" DefTech 2021, Shumen, Bulgaria*, (in Bulgarian)

8. Iliev, M., Bedzhev, B., Bedzheva, M., & Kanchev, K., (2019), A Survey of Periodic Binary Nearly Perfect Signals with Lengths N≡1mod4, *Proceedings of 16th Conference on Electrical Machines, Drives and Power Systems, ELMA 2019, June 6 – 8, 2019, Varna, Bulgaria*
9. Iliev, M., Bedzheva, M., Kanchev, K., & Bedzhev, B., (2019), A Survey of Periodic Binary Nearly Perfect Signals with Lengths N≡3mod4, *Proceedings of 29th Annual Conference of the European Association for Education in Electrical and Information Engineering – EAEEIE 2019, 4th - 6th September 2019, University of Ruse, Ruse, Bulgaria*
10. Iliev, M., Bedzhev, B., Bedzheva, M., & Yanakiev, P., (2020), A Method for Synthesis of Nearly Ideal Phase Manipulated Signals, *Proceedings of the 2020 IEEE International Conference on Information Technologies - InfoTech-2020, 17-18 September 2020, St. St. Constantine and Elena, Bulgaria*
11. Yosifov, Y., Peshev, T., & Kulev, N., (2015), Synthesizing an adaptive algorithm to estimate parameters of a moving target, *Proceedings of International Scientific Conference "Defense, security and military technology", DefTech 2015, Shumen, Bulgaria*, Retrieved from https://aadcf.nvu.bg/scientific_events/papers/NS_2015.pdf
12. Bogdanov, R., Kulev, N., & Nedelchev, M., (2019), Estimation of directions of arrival, applied to fifth generation networks, *Proceedings of International Scientific Conference "Defense Technologies", DefTech 2019, Shumen, Bulgaria*, (in Bulgarian)

APPROACHES FOR PROVIDING CYBERSECURITY OF PRESENT POWER LINE COMMUNICATIONS

Dobry S. Stoynov, Dimitar I. Raev, Ivan Y. Radev

Communication Networks and Systems Department, Artillery, Air Defense Communication and Information Systems Faculty, National Military University „V. Levski", Shumen, Bulgaria, dobri_stoyanov@mail.bg, djlumpox00@gmail.com, secterity@abv.bg

***Abstract**: Today with the Internet technology progress the Power Line Communications (PLCs) became an attractive option for high speed data transfer for communication especially in rural regions. As a result, the providing of high resistance of PCLs to different cyberattacks is a very important engineer problem. It could be solved by appropriate application of cryptographic methods and complex signals with spread spectrum. Accounting this situation, in the paper the peculiarities of present PLCs are analyzed. On this base the approaches for improvement the cyberresistence of PLCs by the means of cryptographic and signal processing technologies are systematized.*

***Keywords**: power line communication, cybersecurity*

Introduction

Power Line Communications (PLCs) are mainly related to the use of existing electrical cables to transport data. In fact, even at the dawn of the development of electric power grids, the ability of transferring dispatching information from one power center to another has been successfully exploited. For example, at the beginning of the 20th century, direct current (DC) networks in the United States used the transmission of telegraph signals directly through the wires of electric power lines. This approach had diminished significantly the cost for building telephone and telegraph systems. Later, with the development of radio communications, a similar technique became applicable to alternative current (AC) networks. Today PLCs open new opportunities and new forms of interactions among people and things in many application areas (e.g., smart metering services and energy consumption reporting, traversing the power line wires to reach data concentrators), making the PLC medium an enabler for sensing, automation, and control in large systems spread over relatively wide areas (e.g., smart city and smart grid scenarios) [1]. On top of PLC, one can adopt also enabling technologies that can improve smart automation processes, such as Internet of Things (IoT). For instance, the adoption of the PLC technology in industrial scenarios (e.g., remote control in automation and manufacturing companies) paves the way to the concepts of Industrial IoT and Industry 4.0 [1].

Today with the Internet technology progress the PLC systems became an attractive option for high speed data transfer for communication especially in rural regions [2]. Broadband over power line can provide Internet access for many users, living in isolated country or mountain places. A laptop or any other device can theoretically be plugged into any power outlet (by use of PLC modem) in building to get access to high-speed Internet. The main advantage of using the existing infrastructure of power line grid would result in economising the infrastructure cost and providing Internet to customers in areas with limited access to internet infrastructural service - e.g. in rural areas and for the customers who do not have access to cable modems. Conversely, power line cables are not designed for transfer of data; therefore there are limiting factors such as electromagnetic interference, degrading the system such as from noise loads and other devices connected to the power line grid, as well as the cybersecurity of

PLCs. Due to this reasons the paper aims to systematize the technologies and the approaches, which can be exploited for providing the cybersecurity of PLCs.

The paper is structured as follows. Firstly, the classification of PLC technologies is presented. Secondly, the requirements of standards on PLCs are analyzed. Thirdly, the basic technologies and approaches, which can be exploited for data protection in present PLCs, are systematyzed. At the end, the main directions for development of technologies for providing the cybersecurity of PLCs are summarized.

1. Classification of Power Line Communications Technologies

PLC technologies can be divided into two basic groups [3]:

G 1) *Narrowband PLC*.

This technology operates in the 3-500 kHz frequency band, which includes the European CENELEC band 3-148.5 kHz, the US FCC band 9-500 kHz, the Chinese band 3-500 kHz and the Japanese ARIB band 10-450 kHz. According to the data bit rate, this technology can be further divided into:

G 1.1) *Low Data Rate* (LDR): These are technologies with a single carrier and a data rate of several kbps. Typical examples of LDR NB-PLC are LonWorks standards, IEC 61334, X10, HomePlug C&C and SITRED.

G 1.2) *High Data Rate* (HDR): These are multi-carrier technologies with data rates from tens of kbps to 500 kbps. Typical examples are technologies based on ITU-T standards by G.hn, IEEE P1901.2, PRIME and G3-PLC.

G 2) *Broadband PLC* (BPL).

Broadband technology operates in the 1,8-500 MHz frequency band and features data rates at the physical layer from a few Mbps to Gbps. It is some- times also referred to as Broadband over Power Lines (BPL). Broadband technology standards are covered by several organizations such as Universal Powerline Association (UPA), Open PLC European Research Alliance (OPERA), Consumer Electronics Power line Communication Alliance (CEPCA), Institute of Electrical and Electronics Engineers (IEEE), International Telecommunication Union (ITUT-T) and HomePlug Powerline Alliance.

The biggest difference between the standards of individual organizations is mainly in the methods of access to the shared medium, methods of encryption and robustness of transmission. The used frequency bands, modulations and the injection of the useful signal into the electrical network are almost identical across the standards.

2. Standards on Power Line Communications

Over the past several years, there have been intense research activities on modelling power line channels. Due to a significant interest in adopting the low- frequency bands for communication in PLC scenarios (from 20 kHz to 500 kHz), various standardization institutes have defined several PLC bands to regulate the frequency utilization, as illustrated in Fig. 1 [1].

Following the band allocations, shown on Fig. 1, different physical layer protocols have been recently defined [1], to support data transmission in the low frequency bands, and further adopted by different PLC modems vendors (e.g., Texas Instruments (TI), Maxim Integrated, STMicroelectronics). The main protocols to date are summarized as follows [1]:

- PoweRline Intelligent Metering Evolution (PRIME) specification: intended for PLC-based modems operating in the frequency range between 42 kHz and 88 kHz using Orthogonal Frequency-Division Multiplexing (OFDM);
- HomePlug specification: operating at frequencies up to 400 kHz;
- G3-PLC specification: intended for PLC-based modems operating in a subfrequency range of the "CENELEC A" band, from 35 kHz to 91 kHz;

- G.hnem specification: drafted by the International Telecommunication Unit (ITU) and selecting G3-PLC and PRIME specification as two annexes to its main body;
- IEEE P1901.2 specification: defined by the Institute of Electrical and Electronics Engineers (IEEE) and adopting G3-PLC and PRIME specifications as two profiles for PLC communication;
- PLCLite protocol: proprietary protocol available on TI-based PLC modems and operating in the frequency range between 42 kHz and 88 kHz using OFDM;
- FlexOFDM protocol: TI proprietary protocol intended for PLC-based modems using OFDM scheme and combining the strengths of PRIME and G3- PLC with variable bandwidth capabilities, adaptive tone mask capabilities, advanced modulation schemes, and the ability to work with an application specific stack to provide high performance.

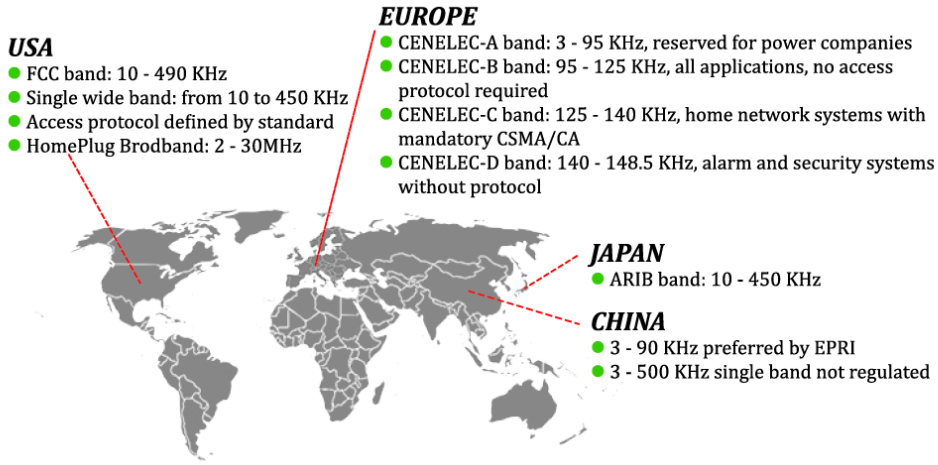


Figure 1: PLC bands

The technologies, exploited in present PLCs, and their data transmission rates are presented in Table 1.

Table 1: Technical characteristics of technologies, exploited in present PLCs

Protocol	Technology	Band occupied	Data rate
PRIME	OFDM	42 – 88 kHz	5,4 kbit/s by DBPSK – 128,6 kbit/s by D8PSK
HomePlug	OFDM	2 – 30 MHz	from 13,0 Mbit/s to 200 Mbit/s
G3-PLC	OFDM	35 – 91 kHz	from 44 kbps - up to 280 kbps in FCC
G.hnem	OFDM	2 – 25 MHz	up to 2 Mbps
IEEE P1901.2	OFDM	> 2 MHz	up to 500 kbit/s by FFT OFDM
PLCLite	OFDM	42 – 88 kHz	up to 21kbps

Here it showld be pointed out, that broadband PLC technology operates in the 1,8-500MHz frequency band, exploits OFDM and features data rates at the physical layer from a few Mbps to Gbps.

3. Review of technologies for providing cybersecurity of present Power Line Communications

The analysis, conducted in the previous chapter of the paper, demonstrates that the most exploited technology in present PLCs is the Orthogonal Frequency Division and Multiplexing (OFDM). Due to this reason the exploration of cryptographic and signal processing technologies, which can be used to prevent the cyberattack on PLCs, exploiting OFDM, has a signicant practical importance. Accounting this conclusion at the beginning of this chapter of the paper, the peculiarities of OFDM communication technology will be recalled.

As known, OFDM signal is formed by N harmonic subcarriers, which are spaced by equal frequency interval Δf. More specifically, the total frequency band ΔF, occupied by an OFDM signal, is divided into N subchannels with the width $\Delta f = 1/T_s$, where T_s is the duration of the symbol interval. Consequently, $\Delta F = N\Delta f = N/T_s$. This technical approach provides the main advantage of OFDM communication system - the ability to withstand difficult channel conditions. More specifically, channel equalization is simplified due to the fact that the OFDM signal really is a plurality of slowly modulated narrowband signals. The low symbol rate makes it possible to use a guard interval between symbols, which can eliminate inter-symbol interferences (ISIs). As a result, the OFDM technology allows the negative effects, caused by the specific factors, disturbing the communication over power line radio channels, to be effectively diminished. Indeed, when transmitting signals over power supply lines, there may be large attenuation in the transmitting function at certain frequencies, which can lead to data loss. PLCs, exploiting OFDM technology, provide a special method for solving this problem - dynamically turning off and on data-carrying signals. This method uses a special device, which constantly monitors the power line channel in order to identify the spectrum bands, where the attenuation exceed the admissible threshold. If this fact is detected, the use of frequencies, affected by the noises, is temporarily stopped until the normal attenuation value is restored, and data is transmitted on other frequencies. This approach also allows the problems, caused by impulse noise (up to 1 microsecond) of halogen lamps, as well as of turning on and off powerful (factory, household) appliances, equipped with electric motors, to be mitigated.

In the rest part of this chapter of the paper, the analysis of technologies for providing cybersecurity of present PLCs, will be performed by the means of fig. 2 and fig. 3, where the block-schemes of OFDM transmitter and receiver are presented respectively.

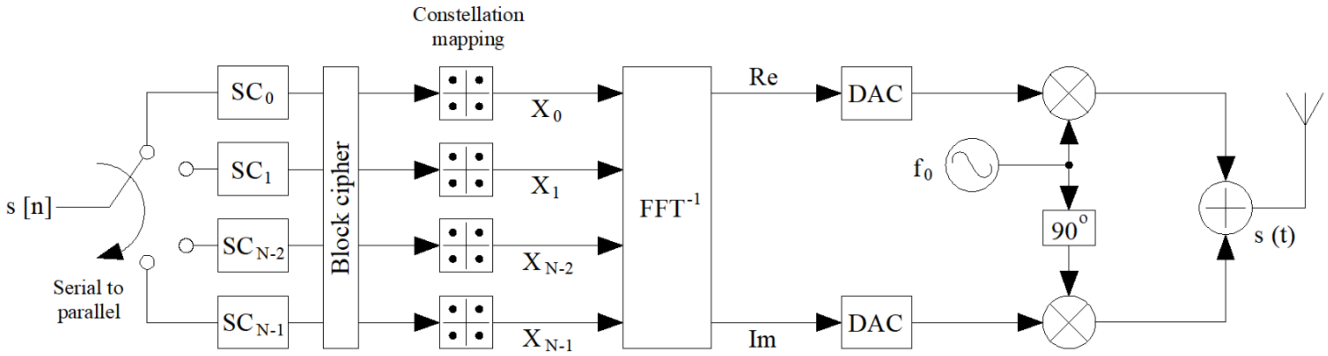


Figure 2: Modified OFDM transmitter, which can be used in PLCs

Namely, on fig. 2 $s[n]$ is the serial stream of binary digits, which should be send to the receiver over the power line radio channel. Firstly (before the inverse fast Fourier transform (FFT^{-1})), this stream is converted into N parallel substreams, after which each of them is mapped to a symbol stream using a phase (BPSK, QPSK, 8-PSK) or amplitude-phase quadrature modulation (QAM) procedure. When using BPSK modulation, a stream of binary numbers (1 and −1) is obtained, with QPSK, 8-PSK, QAM the result is a stream of complex numbers. Since the streams are independent, the modulation method and therefore the number of bits per symbol in each stream can be different. Therefore, different streams may have different bit rates. Here it should be outlined, that the inverse FFT is calculated for N simultaneously arriving symbols, producing a set of complex frequency-domain samples with the same size N. Next, digital-to-analog converters (DACs) convert the real and imaginary components separately to analog form, after which they modulate cosine and sine of the carrier frequency f_0 (which is in the band of radio frequencies (RF)) respectively. These signals are further summed, which forms the signal $s(t)$, radiated by the antenna.

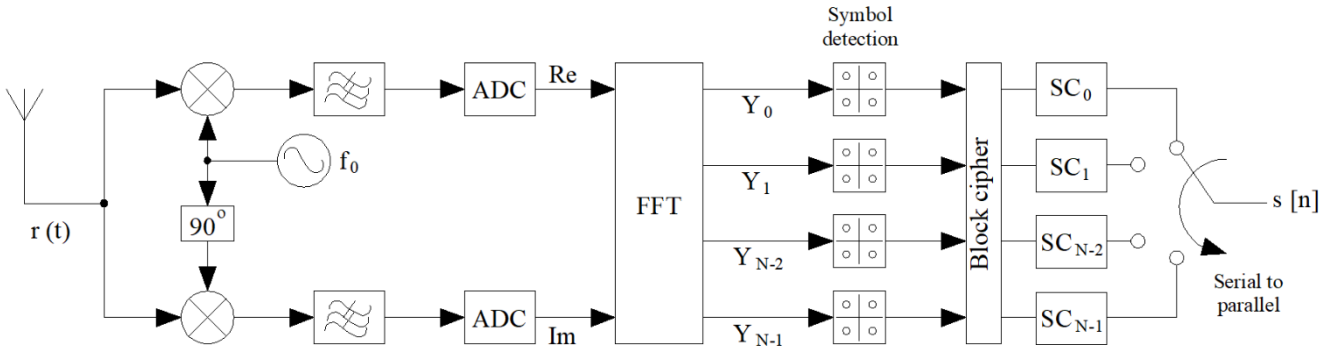


Figure 3: Modified OFDM receiver, which can be used in PLCs

In general, the OFDM reciver (fig. 3) performs "mirror inversely" the operations, executed by the transmitter. More specifically, the antenna detects a signal $r(t)$, which is sum of the sent signal $s(t)$ and noises, caused by all the factors, disturbing the communication over the power line radio channel. After that, the OFDM receiver extracts the quadrature components of $r(t)$ by multiplying $r(t)$ by cosine (cos) and sine (sin) of carrier frequency f_0 and rejecting by low-pass filters the multiplication products (charmonic components), which are out from the base frequency band. The resulting signals are then digitized using analog-to-digital converters (ADC) and processed by direct fast Fourier transform (FFT). This produces N parallel symbol streams, each of which is converted to a binary sequence using an appropriate phase demodulation or amplitude-phase quadrature demodulation (when BPSK, QPSK, 8-PSK or QAM are used in the transmitter) algorithm respectively. Ideally, a bit stream is obtained, which is equal to the bit stream, sent by the transmitter.

The peculiarities of the OFDM signal processing allow the following technologies for providing cybersecurity to be applied in present PLCs.

T 1) Application of diffrenet (indidually specified) stream cypher (noted as $SC_0, SC_1, \dots, SC_{N-2}, SC_{N-1}$ on fig. 2, fig. 3) in each substream $X_0, X_1, \dots, X_{N-2}, X_{N-1}$, $Y_0, Y_1, \dots, Y_{N-2}, Y_{N-1}$ respectively.

This approach can enhance significantly the cybersecurity of PLCs as the probability for success of a cyberattack P_{ca} is

$$P_{ca} = \prod_{k=0}^{N-1} p_{SC_k}, \tag{1}$$

where $p_{SC_k}, k = 0, 1, \dots, N-1$ is the probability for breaking the kth stream cypher.

As seen, when the number of subchannels N increases the probability for success of a cyberattack P_{ca} tends rapidly to 0, eventhough in cases of cheap, but not very reliable, stream cyphers.

T 2) Usage of a block cypher over the stream of blocks, consisting of all symbols $X_0, X_1, \dots, X_{N-2}, X_{N-1}, Y_0, Y_1, \dots, Y_{N-2}, Y_{N-1}$ in every clock (symbol) interval T_s.

The effectiveness of this approach ensues from the high cryptoresistance of present block cyphers in principle.

T 3) Exploitation of orders (permutations with repetitions) of algorithms for phase modulation/demodulation or amplitude-phase quadrature modulation/demodulation, which are known only for the authorized parties.

The usefulness of this approach is provided by the huge amount of consequently orderings (forming permutations with repetitions) of the different algorithms for modulation/demodulation, which can be exploited in subchannels $k = 0, 1, \dots, N-1$. Here it should be stressed that the list of algorithms for modulation/demodulation is very large as many advanced techniques for spreading the spectrum of signals can be applied [4], [5], [6], [7], [8].

T 4) Usage of appropriate protocols for communication over power line channels. For example, the authentication can enhace significantly the cybersecurity of PLCs as this approach authorise the user to access to the network only after its identifying.

Conclusion

In the paper the basic approaches, which can be exploited for data protection in present PLCs, are analyzed and systematyzed. As these approaches can be exploited separately or in different combinations, the following main directions for development of technologies for providing the cybersecurity of PLCs could be outlined:

- elaboration of all the approaches, explored in the last chapter of the paper;
- substantiating of cost and time effective schemes, combining the positive features of groups of different approaches.

The results of the study, presented in the paper, could be useful in the processes of implementation and development of smart electric grids in the Republic of Bulgaria.

References

1. Davoli, L., Veltri, L., Ferrari, G., & Amadei, U., (2019), Chapter 13: Internet of Things on Power Line Communications: an Experimental Performance Analysis, Retrieved from http://www.tlc.unipr.it/ferrari/Publications/Book_chapters/BC_DaVeFeAm_Springer18.pdf
2. Hosseinpour, A., Hosseinian-Far, A., & Jahankhani, H., (2015), Security and Feasibility of Power Line Communications System, Retrieved from https://www.researchgate.net/publication/280489153
3. Mlýnek, P., Rusz, M.; Benešl, L., Slácˇik, J., Musil, P., (2021), Possibilities of Broadband Power Line Communications for Smart Home and Smart Building Applications, *Sensors 2021, 21, 240*, Retrieved from https://doi.org/10.3390/s21010240
4. Iliev, M., Bedzhev, B., Bedzheva, M., & Kanchev, K., (2019), A Survey of Periodic Binary Nearly Perfect Signals with Lengths N≡1mod4, *Proceedings of 16th Conference on Electrical Machines, Drives and Power Systems, ELMA 2019, June 6 – 8, 2019, Varna, Bulgaria*
5. Iliev, M., Bedzheva, M., Kanchev, K., & Bedzhev, B., (2019), A Survey of Periodic Binary Nearly Perfect Signals with Lengths N≡3mod4, *Proceedings of 29th Annual Conference of the European Association for Education in Electrical and Information Engineering – EAEEIE 2019, 4th - 6th September 2019, University of Ruse, Ruse, Bulgaria*
6. Iliev, M., Bedzhev, B., Bedzheva, M., & Yanakiev, P., (2020), A Method for Synthesis of Nearly Ideal Phase Manipulated Signals, *Proceedings of the 2020 IEEE International Conference on Information Technologies - InfoTech-2020, 17-18 September 2020, St. St. Constantine and Elena, Bulgaria*
7. Yosifov, Y., Peshev, T., & Kulev, N., (2015), Synthesizing an adaptive algorithm to estimate parameters of a moving target, *Proceedings of International Scientific Conference "Defense, security and military technology (DefTech 2015)," Shumen, Bulgaria*, Retrieved from https://aadcf.nvu.bg/scientific_events/papers/NS_2015.pdf
8. Bogdanov, R., Kulev, N., & Nedelchev, M., (2019), Estimation of directions of arrival, applied to fifth generation networks, *Proceedings of International Scientific Conference "Defense Technologies (DefTech 2019)," Shumen, Bulgaria*, (in Bulgarian)

ANALYSES OF 0-DAY THREATS WITH FIREEYE EDR

Veselka Stoyanova, Martin Rakov

*National Military University **VASIL LEVSKI**, Shumen, Bulgaria, veselka_tr@abv.bg*

***Abstract**: In the current report is written about the functions for analysing and investigating 0-day threats using the Endpoint Detection and Response technology of Fireeye - HX Endpoint Security. The console is deployed and installed in Amazon AWS cloud and the agents has been deployed to over 20 Windows workstations. A few tests were executed on a few machines to analyse the reaction of Fireeye when unknown malicious code gets executed on the workstation.*

***Keywords**: 0day, threats, fireeye, edr, endpoint*

Introduction

FireEye is a cybersecurity company that offers hardware, software, and cloud services to counter cyber attacks. It can be seen that revenue from the category product and related subscription services was highest in 2018, generating approximately 500 million U.S. dollars. Since then, revenue generated from this category is declining. This trend reflects a migration from traditional IT product model to to cloud-based solutions[11].

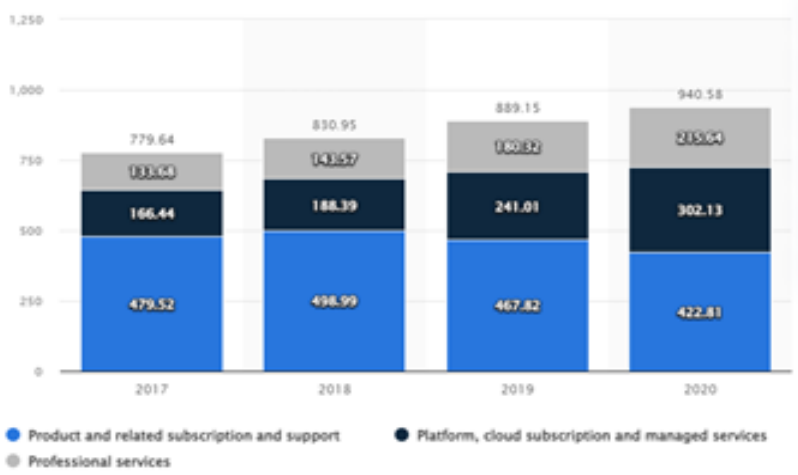


Figure 1: Endpoint security – Statistics[11]

The most recent researches in this area are stating that being successful in defending the parameter and the endpoint is not only into detection and protection, but as well in as early as possible investigation and response. In most of the cases in huge organizations around a month or even more to detect a threat successfully and fully and if there is a breach – to respond and remediate it. Such cases can drastically disturb the daily operations, expose the sensitive date or even impact the revenue in a negative matter. Also, can impact the customer retention as the organization may go under different legal and regulatory actions. Most of the times the risks are in [1], [2], [4] and [10]:

• Non-effective strategies for incident response – often organizations are approach of incident response is connected of wiping the whole compromised system and starting from scratch.

• Attackers having access to sensitive data for longer period of time – the key here is the validation of an alert;

• Reputation damage for the organization - bad incident response practices, ineffectiveness etc are of the main reasons that raise questions about the management of the organization;

• Exposure to legal liability and compliance – security incidents has to have effective incident management, otherwise this can get the organization to legal action and getting out-of-compliance with industry regulations and standards;

• Revelation and risk management – due to possibility of getting breached, organizations must prepair such a program, because the miss of it can get the organization to impacts as fines, intangible damage of the reputation etc.

The Endpoint detection and Response solution of Fireeye gives real-time answer to be able to confirm alerts and contains information of the size and the vector of the attack. All of this information assists organizations to rapidly response and successfully minimize the losses that the organization can suffer from if the attack is fully successful.

The solution is backed up by their leading threat intelligence service that connects millions of networks and endpoints that are all acting as sensors, many Incident Response engagements and billions of security events analyzed on a daily bases. All this helps customers of Fireeye to stay informed and even protected from the newest 0-day attacks.

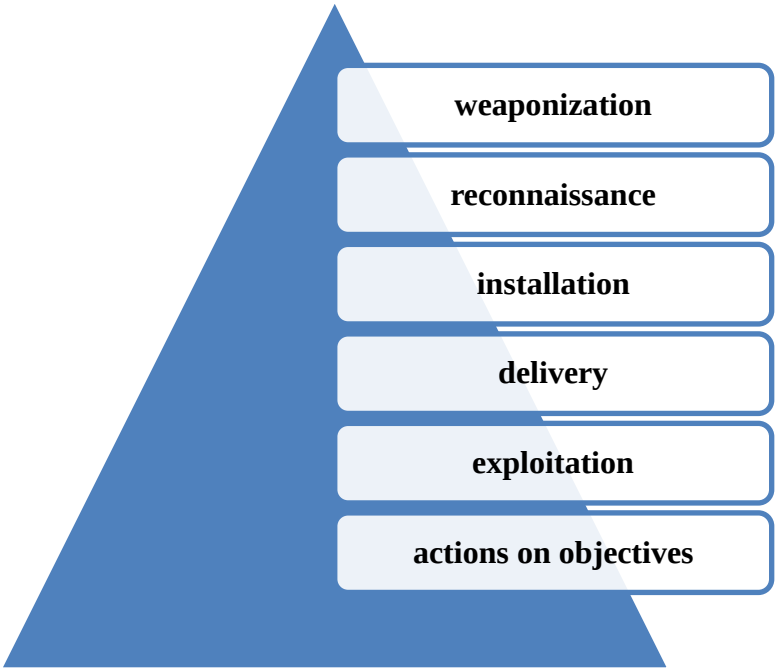


Figure 2: Attack Kill Chain

The so-called Attack Kill Chain is a methodology that helps the organizations and technologies that they are using to identify the insider threats, advanced persistent threats and even social engineering. It contains seven steps that objects to offer transparency of the attack itself while supporting the cybersecurity engineer to get better view of the attackers tactics, schemas, plans of actions and used techniques. The seven steps are[3]:

• Reconnaissance: That's the initial step where attacker is choosing his target and analyzing it deeply to be able to identify vulnerabilities that can be exploited. Many different techniques are used in this stage – most of them social engineering and manual research but also nmap, vulscan, etc

• Weaponization – that's the step where the attacker is developing malicious code like virus, worm or similar in order to exploit the vulnerabilities, found in the previous step. Depending on the aim of the attacker, this malicious code can exploit unknown vulnerabilities and then it's a 0-day attack or it can be exploiting already known but unpatched vulnerabilities. Sometimes the attacks are even mixed – with well-known vulnerabilities and in the same time with exploiting 0-day vulnerabilities.

• Delivery – this is the step where the target gets infected aka the attacker is pushing the malware to the targeted machine. Here can be used different methods like USB drives, e-mail attachments and phishing websites.

• Exploitation – that's the first step where malware code has been executed on the targeted machine. The code has been triggered to exploit the targeted vulnerabilities.

• Installation – in this step the malware starts the action that has been made for, so exploit is successful and installation of additional software (if needed) has been initiated. Also the attacker opens backdoor to the systems to easily start their malicious plan.

• Command and Control – all the communication with the Command and Control center has been successfully initiated and now is the time for the attacker to access the exploited systems and networks.

• Actions on Objective – after gaining persistent access, the attackers can start stealing data, encrypt data for ransom or even destroy the data. After this step, the attacker is getting out of the system and "wiping" all as many evidences as possible about his entrance and access.

The purpose of this paper was to provide the reader with an understanding of 0-day threats with Fireeye such that he/she may use it himself. 0-Day threats with Fireeye is a powerful tool that like we said time and time again, in the wrong hands can be used for great harm. It provides an abundance of resources for legitimate network security professionals, security administrators, product vendors, and developers to use in a variety of ways.

We start with deploying the Fireeye agent on the "victims" machines and that is how they are going to get protected. The installation of the agent is easy – its .msi file, generated from the HX appliance that is coming preconfigured to communicate with the management. After that we execute the script that in our case is bash script that executes malicious code and initiates communication between the endpoint and command and control server (the Kali Linux and based on Metasploit [6], [7] as shown in figure 3. In the beginning, nothing happens, but after 2 minutes the machines are automatically rebooted with a message warning for this action.

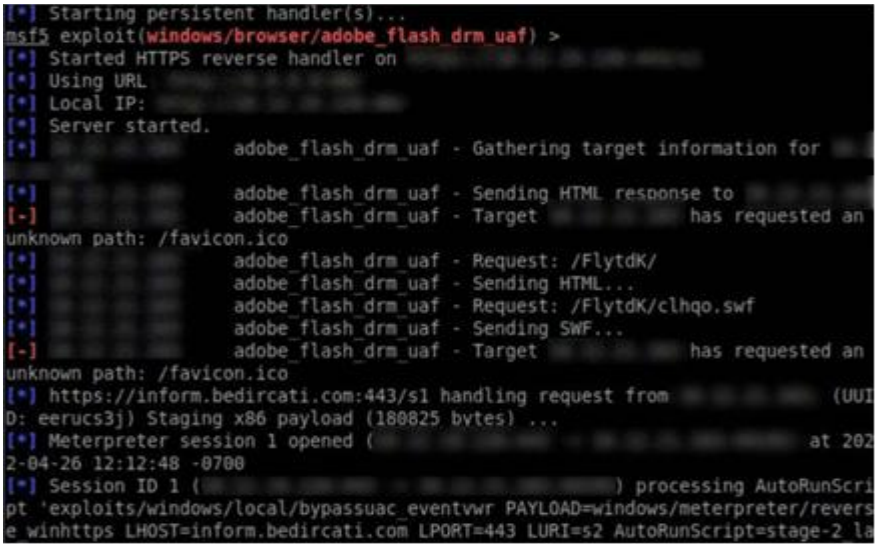


Figure 3 – Metasploit execution of malicious code and payload on endpoints

As seen – WmiPrvSE execution with exploitation for Internet explorer (iexplorer.exe) and powershell execution for memory injection. In the console is possible to see also the hashes of the processes and files, the timestamp, the recurring number and much more. For example, if we click on the exploit alert we will see additional information of what exactly happened as shown on Figure 4:

Figure 4 – ExploitGuard additional information after behaviour analyses

If we click on the powershell execution alert that is detected by IoC we will see what are the indicators objects that has been detected and what exactly has been executed (Fig. 5).

Figure 5 – IOC conditions detected on the infected machine

After the attack has been identified, it is possible to search all machines that has the Fireeye agent installed. This feature is called – Enterprise search [9] and is like "google search" for the endpoints. It is possible to search for hashes, strings, IoC etc but also to put watchdog to monitor of a specific search string will return some results.

The protection engines and layers of security provided by Fireeye EDR are shown on Figure 6:

Figure 6 – Fireeye Protection Engines [2]

In the inner circle are the out-of-the-box protection engines Malware Guard, Malware Protection, Exploit Guard and IoC Detector that are the core of Fireeye EDR.

• Malware protection – this is EOM partnership between Fireeye and Bitdefender – well-known cybersecurity vendor for endpoint security that is providing the signature-based protection for Fireeye EDR

• Malware guard – this engine is based on Machine-Learning algorithms. This layer is responsible for detection and prediction of prior execution of Windows executable malware. That's how the system is protected before the execution of the malicious code. The engine is not-based on signatures. (5)

• Exploit Guard – this is their behavior-based analyses. The engine is for detection and prevention for applications exploits at any of the threat stages. Also prevent exploit and payload codes from up-load/download or execute malicious code.

• IOC Detector – back in the days Fireeye invented the indicators of compromise. The meaning behind the term is an artefact that has been found in the operating system of the endpoint that indicates high possibility of compromise. IoCs can be more complex and be expressed like group of artefacts. So in the backend of the system, Fireeye scans the system for IOCs and triggers alert or an action of such is found.

The rest of the engines shown in Figure 6 are free add-ons that can be deployed additionally to Fireeye EDR if the customers need them. They add mostly additional investigation and forensics features that can be helpful when particular endpoints need extra care.

Acknowledgments

The purpose of this paper was to provide the reader with an understanding of 0-day threats with Fireeye such that he/she may use it himself. 0-Day threats with Fireeye is a powerful tool that like we said time and time again, in the wrong hands can be used for great harm. It provides an abundance of resources for legitimate network security professionals, security administrators, product vendors, and developers to use in a variety of ways..

References

1. Cichonski, P., T. Millar, Tim Grance, K. Scarfone, Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology, 2012, http://dx.doi.org/10.6028/NIST.SP.800-61r2 2.

2. Olaniyan,Ol., Applying the Diamond Model of Intrusion Analysis: FireEye Breach,

3. 7 Steps of Cyber Kill Chain - Comprehensive Guide Logsign

4. Gundur, R. V., Levi, M., Topalli, V., Ouellet, M., Stolyarova, M., Chang, L. Y.-C., & Mejía, . D. (2021). Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context. CrimRxiv. https://doi.org/10.21428/cb6ab371.5f335e6f

5. MalwareGuard: FireEye's Machine Learning Model to Detect and Prevent Malware | FireEye Inc

6. Yeo, J., Using penetration testing to enhance your company's security, Computer Fraud & Security Volume 2013, Issue 4, April 2013, Pages 17-20, https://doi.org/10.1016/S1361-3723(13)70039-3

7. Kennedy, D., J. O'Gorman, D. Kearns, M. Aharoni, Metasploit: The Penetration Tester's, 2011, San Francisko, ISBN-10:1-59327-288-X

8. Penetration Testing Is What We Do, Cyber Threat Defense Solutions- Threat Intelligence Services, https://mandiant.com

9. Lee,T, M. El-Banna, D. Dumond HX 3.X Enterprise Search – Finding the Achilles Heel | FireEye Inc, 24 May 2016.

10. FireEye (2020). Unauthorized Access of FireEye Red Team Tools. Retrievedfrom https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html

11. Sava, Al.,J., FireEye global revenue 2017-2020, by segment, https://www.statista.com/statistics/1197078/fireeye-revenue-category-worldwide-global/

12. Десев Х., „Технология за оценка на риска на кибербезопасността на енергийната критична инфраструктура", International scientific conference, collection of papers "Diferense and security", Artillery, Aircraft Defense and CIS faculty 2019г., стр.70-73, НВУ Шумен, ISSN 2367-7902

WLAN IEEE 802.11BE OPPORTUNITIES AND PERSPECTIVE IN FUTURE

Dimitar S. Dimov

Communication Networks and Systems Department, Artillery, Air Defense, Communication and Information Systems Faculty, National Military University „V. Levski", Shumen, Bulgaria, dimovds99@gmail.com

***Abstract**: We start by overviewing the latest Wi-Fi-related news, with emphasis on the recently launched Wi-Fi 6E certification program. We then provide an updated digest of 802.11be essential features, vouching for multi-AP coordination as a must-have for critical and latency-sensitive applications. Wi-Fi technology is continuously innovating to cater to the growing customer demands, driven by the digitalization of everything, in the home as well as in enterprise and hotspot spaces.*

***Keywords**: WLAN,PHY,MAC, MU-MIMO,OFDMA,MULTI-LINK*

Introduction

Wi-Fi technology is continuously innovating to cater to the growing customer demands, driven by the digitalization of everything, in the home as well as in enterprise and hotspot spaces. In this article, we introduce to the wireless community the next generation Wi-Fi, based on IEEE 802.11be. As the popularity and capabilities of Wi-Fi grow, so will the demand for wireless services. More and more households will accommodate smart-home appliances besides 8K displays and virtual reality gadgets, turning into dense environments with many concurrently connecting devices. Enterprises will be sharply increasing the amount of data collected across their premises, targeting enhanced manufacturing processes and augmented productivity. Importantly, such cross-factoryfloor communications will afford very low latency to enable machinery synchronisation and real-time control . Live video will take up a large share of the global IP traffic, with high-quality conferencing enabling more remote-friendly work, education, and healthcare in a post-pandemic world.[1] Our call for gigabits per second—delivered reliably to every nook and cranny of our apartments and enterprise spaces— is motivating the development of a new Wi-Fi 7 generation based on IEEE 802.11be Extremely High Throughput (EHT). Since the introduction of 802.11be to our research community,[2] much has been cooking in the regulation, certification, and standardisation bodies. The United States Federal Communications Commission (FCC) has made new spectrum available in the 6 GHz frequencies for unlicensed use, and the Wi-Fi Alliance—a worldwide network of companies driving the adoption and evolution of Wi-Fi through a certified seal— is soon expected to provide worldwide interoperability certification for Wi-Fi 6 devices to function in such a new band. Meanwhile, key experts are gathering at virtual IEEE meetings to define the building blocks of the 802.11be standard.[1]

1. IEEE 802.11be GOALS AND FEATURE SUMMARY

Wireless LAN (Wi-Fi) has been a key component of wireless data services in a wide array of environments. The recent surge of people working from home highlights how important Wi-Fi is for connectivity. Not only does it provide data and connections to office networks, it is increasingly used for video conferencing to connect remote workers and facilitate online meetings that are used as substitutes for face-to-face meetings and large conferences. The use of video traffic will continue to increase in the

coming years as applications such as VR/AR become more widely used. In addition, WLAN users will expect reliable and near real-time gaming and cloud computing experience.EEE802.11be aims to specify MAC and PHY features that will meet the high through put and low latency requirements for these applications. The IEEE802.11be PHY is very similar to the PHY defined in the highly successful IEEE802.11ax standard. For example, IEEE802.11be will support MU-MIMO, OFDMA and longer symbol duration (smaller subcarrier spacing). Some key IEEE802.11be PHY improvements and changes include the ability to assign multiple resource units to a single user in OFDMA transmissions as well as 320 MHz bandwidth and 4096QAM modulation support as listed in Figure 1.[3]

	IEEE 802.11n (HT)	IEEE 802.11ac (VHT)	IEEE 802.11ax (HE)	IEEE 802.11be (EHT)
Supported bands	2.4 GHz, 5 GHz	5 GHz	2.4 GHz, 5 GHz, 6 GHz	2.4 GHz, 5 GHz, 6 GHz
Channel bandwidth (in MHz)	20, 40	20, 40, 80, 80+80, 160	20, 40, 80, 80+80, 160	20, 40, 80, 160, 320
Subcarrier spacing (in kHz)	312.5	312.5	78.125	78.125
Symbol time (in µs)	3.2	3.2	12.8	12.8
Cyclic prefix (in µs)	0.8	0.8, 0.4	0.8, 1.6, 3.2	0.8, 1.6, 3.2
MU-MIMO	no	downlink	uplink and downlink	uplink and downlink
Modulation	OFDM	OFDM	OFDM, OFDMA	OFDM, OFDMA
Data subcarrier modulation	▸ BPSK ▸ QPSK ▸ 16QAM ▸ 64QAM	▸ BPSK ▸ QPSK ▸ 16QAM ▸ 64QAM ▸ 256QAM	▸ BPSK ▸ QPSK ▸ 16QAM ▸ 64QAM ▸ 256QAM ▸ 1024QAM	▸ BPSK ▸ QPSK ▸ 16QAM ▸ 64QAM ▸ 256QAM ▸ 1024QAM ▸ 4096QAM
Coding	▸ BCC (mandatory) ▸ LDPC (optional)	▸ BCC (mandatory) ▸ LDPC (optional)	▸ BCC (mandatory) ▸ LDPC (optional)	▸ BCC (mandatory) ▸ LDPC (mandatory [1])

Fig. 1: PHY parameter values for IEEE 802.11n, IEEE 802.11ac, IEEE 802.11ax and IEEE 802.11b.

Despite its name, 802.11be Extremely High Throughput will be much more than high peak data rates. Sure enough, Wi-Fi 7 is projected to support at least 30 Gbps per AP, about four times as fast as Wi-Fi 6, while ensuring backward compatibility and coexistence with legacy devices in the 2.4,5, and 6 GHz unlicensed bands. However, the 802.11be Task Group (TG) also recognised the need for—and is aiming at— lower latencies and higher reliabilities to enable time-sensitive networking (TSN) use cases [8]. The former is seen as an enabler for real-time applications including augmented and virtual reality, gaming, and cloud computing, demanding delay times reduced to below 5 ms. The latter is critical for nextgeneration factories and enterprises, where Wi-Fi may need to guarantee three or more 'nines' of reliability to aim at replacing some wired communications. To speed up the development and commercialisation of WiFi 7, whose timeline is illustrated in Fig. 2, the 802.11be TG deviated from the conventional single-phase development cycle, and agreed on two phases. The first one will place the spotlight on a set of features deemed of high-priority according to their gain/complexity ratio, time for standardization and implementation, as well as associated interest and market needs. [1]

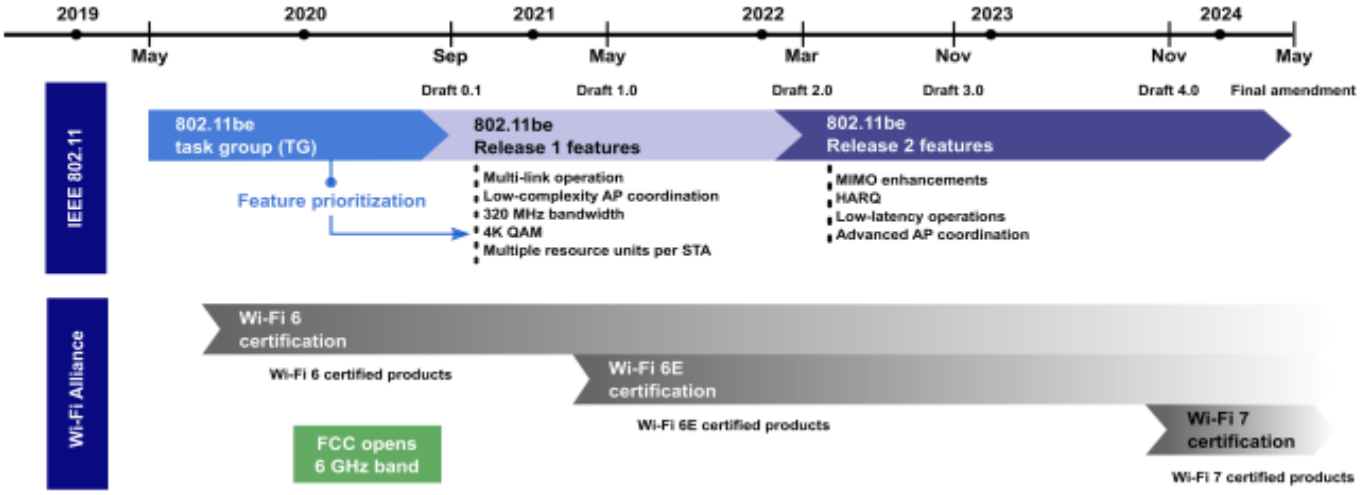


Fig. 2: Illustration of the current Wi-Fi 7 standardisation, certification, and commercialisation timelines.

2. IEEE 802.11be

2.1 PHY Layer

The ongoing release of the 6 GHz band throughout the world will be of great benefit to WiFi dense scenarios, not only due to the additional 1.2 GHz of available spectrum, but also to the resulting interference reduction among networks/BSSs. The incorporation of the 6 GHz band into IEEE 802.11be will also encompass channels as wide as 320 MHz, thus enabling higher transmission rates.

As for the maximum number of spatial streams, it is expected to double its number from 8 in IEEE 802.11ac/ax to 16 in IEEE 802.11be, thus further benefiting from fundamental advantages of predominantly indoor WiFi operation: rich scattering, higher angular spreads, lower correlation, and diversity of channels with good propagation conditions.

The maximum supported modulation size in IEEE 802.11be is likewise expected to be boosted with the adoption of the 4096-QAM modulation, whose practical use, however, will only be feasible in combination with beamforming.

All in all, new IEEE 802.11be PHY features favor low-latency operation, as wider available bandwidth results in faster transmissions and more spatial streams turn into higher rates in the single-user (SU) mode and into more parallel transmissions (with less waiting time in the buffer) in the multi-user (MU) mode.

2.2 MAC Layer

Many significant MAC features from IEEE 802.11ax such as Multi-User Multiple-Input Multiple-Output (MU-MIMO), Orthogonal frequency-division multiple access (OFDMA), and spatial reuse will be extended in IEEE 802.11be. The support of more spatial streams will also enable more flexible MU-MIMO arrangements. However, current explicit channel state information acquisition procedure may not cope well with such high number of antennas and, for that reason, TGbe is currently evaluating several alternatives to enhance explicit sounding, even considering the introduction of an implicit procedure.

As for OFDMA, enhanced resource unit Resource unit (RU) allocation schemes will allow allocating multiple contiguous. Consequently, these novel schemes could significantly increase spectral efficiency and overall network throughput and, even better, satisfy timely data delivery [6]. In fact, whether based on MU-MIMO or OFDMA, MU transmissions are key to reduce the channel access latency, as packets from/to different users can be de-queued simultaneously.

Multi-link operation will likely become the most representative feature of IEEE 802.11be, being able to yield an order-of-magnitude reduction in the worst-case latency experienced by WiFi devices and meet the stringent requirements of real-time applications even under dense traffic conditions [8].

In general, multi-link operation aims to improve throughput by aggregating links [4], enhance reliability by transmitting multiple copies of the same frame in separated links, decrease channel access delay by selecting the first available link in terms of latency [2], and enable isolation of time-sensitive traffic from other network traffic [5]. In short, having two active links operating at different bands/channels between an AP and an STA may increase channel access efficiency by enabling opportunistic link selection, link aggregation, and multi-channel full duplex [7]. Figure 1 shows several of the previously mentioned cases: opportunistic link selection, link aggregation, and multi-channel full duplex. Figure 3 shows several of the previously mentioned cases: opportunistic link selection, link aggregation, and multi-channel full duplex.

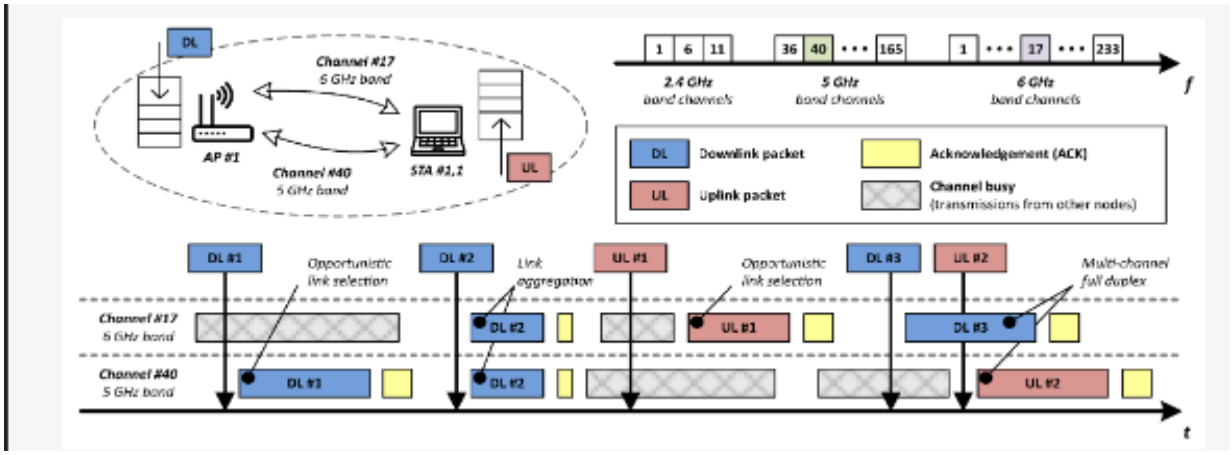


Fig. 2: Multi-link operation techniques at ISM frequency bands.

Conclusion

WiFi will never be able to guarantee fully deterministic communications because of its operation in license-exempt bands, there is still room to reduce the impact of all manageable causes, both internal and external, that may increase latency. Next-generation Wi-Fi will unlock access to gigabit, reliable and low-latency communications, reinventing manufacturing and social interaction through digital augmentation. The 802.11be amendment is the next significant milestone in the Wi-Fi long-term success story. Its core features are related to providing extremely high throughput and supporting real-time applications. Although the standard development process is at the very initial stage, we already can sketch the future technology and point out its advantages and limitations together with open issues, which require additional efforts from the community.

References

1. Adrian G.R., David L.P., Lorenzo G.G, and Giovanni G. (2021)."IEEE 802.11be: Wi-Fi 7 Strikes Back". *IEEE Communications Magazine*.
2. David. L.P., (2019). "IEEE 802.11be Extremely High Throughput: The next generation of Wi-Fi technology beyond 802.11ax,".*IEEE Communications MagazineSep.*
3. Rohde & Schwarz GmbH&Co ,(2022)."IEEE 802.11be TECHNOLOGY -INTRODUCTION". *White paper IEEE802.11be technology introduction.*

4. Song, T., Kim, T.,(2021). "Performance Analysis of Synchronous Multi-Radio Multi-Link MAC Protocols in IEEE 802.11be Extremely High Throughput WLANs", *Appl. Sci., 11, 317.*
5. Cavalcanti, D.; Bush, S.; Illouz, M.; Kronauer, G.; Regev, A.; Venkatesan, G. (2020). "Wireless TSN-Definitions Use Cases & Standards Roadmap". *AvnuAlliance: Beaverton, OR, USA.*
6. Avdotin, E.; Bankov, D.; Khorov, E.; Lyakhov, A. (2019). "Enabling Massive Real-Time Applications in IEEE 802.11 be Networks. In Proceedings of the 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)". *Istanbul, Turkey.*
7. Yang, M.; Li, B.; Yan, Z.; Yan, Y. (2019). "AP Coordination and Full-duplex enabled Multi-band Operation for the Next Generation WLAN: IEEE 802.11 be (EHT)". *International Conference on Wireless Communications and Signal Processing (WCSP), Xi'an, China*.
8. Naik, G.; Ogbe, D.; Park, J.M.J. (2021). "Can Wi-Fi 7 Support Real-Time Applications? On the Impact of Multi Link Aggregation on Latency". *IEEE International Conference on Communications (ICC), Xiamen, China*.

AUTONOMOUS DRIVING – STEP IN THE FUTURE

Ivan Y. Radev, Petya N. Stefanova

Communication Networks and Systems Department, Artillery, Air Defense Communication and Information Systems Faculty, National Military University „V. Levski", Shumen, Bulgaria, secterity@abv.bg, petyastefanova0202@abv.bg

***Abstract**: This paper gives overview about autonomous vehicles and advanced driver-assistance system which are driving the need for higher bandwidth and lower latency. Also what is Automotive Ethernet and how become the new backbone for faster automotive networks. Comprehensive testing of the transmitter, receiver, link segment, and higher-layer protocol functions ensures successful implementation.*

***Keywords**: autonomous driving, Ethernet, vehicles, speed*

Introduction

Major innovation drivers in the automotive industry span three categories: enhanced safety, a cleaner environment, and improved convenience with connectivity. To achieve these goals, automakers, automotive suppliers, governments, academia, and even nontraditional automotive players such as wireless chipset makers, mobile device makers, and wireless service providers are developing advanced driver-assistance systems (ADAS), connected car technologies, and, ultimately, autonomous vehicles. The wiring harness is now the third heaviest component in a vehicle and the third most costly system.

Wiring harness installation represents 50% of labor costs during automobile assembly. Automotive Ethernet is the emerging solution to these challenges in the same way that Wi-Fi is the foundation for dedicated short-range communications. Ethernet is a well-known, trusted, and ubiquitous solution in traditional local area networking (LAN).

The advantages of Ethernet — multipoint connections, higher bandwidth, and low latency — are attractive to automobile manufacturers. However, traditional Ethernet is too noisy and interference-sensitive for use in automobiles.

1. What is automotive Ethernet?

Automotive Ethernet is a wired network that connects electronic components in a car. It is intended to meet the bandwidth, latency, synchronization, interference (for example, electromagnetic interference [EMI]), security, and network management requirements of the automotive industry. Broadcom introduced the concept of automotive Ethernet, and the OPEN (One-Pair Ethernet) Alliance adopted and regulated it. The OPEN Alliance sponsored Broadcom's 100 Mbps BroadR-Reach as a multivendor licensed solution. The 100 Mbps PHY implementation uses technologies from 1 Gbps Ethernet to enable 100 Mbps transmission over a single pair in both directions. This works with echo cancellation using more advanced encoding to reduce the base frequency to 66 MHz (from 125 MHz), allowing automotive Ethernet to meet automotive EMI specifications.

2. Why automotive Ethernet?

Automotive Ethernet is the obvious choice over traditional automotive serial buses for in-vehicle electronic systems connections and communications, autonomous driving, and ADAS. Car electronics

architectures are becoming more complex, with more sensors, controllers, and interfaces; higher bandwidth requirements; more computers; and more communication links. The wiring harness that connects these systems is the third costliest and third heaviest component in a car. Today, automakers use multiple proprietary standards for communication; most components use a dedicated wire or cable. Automotive Ethernet serves as the unifying standard for all communications. It is carried on a single cable pair from each electronic component to a central networking switch.

3. An overview of automotive serial buses

We can better understand why autonomous vehicles and ADAS require automotive Ethernet by reviewing the main traditional automotive serial buses, including Controller Area Network (CAN), low-voltage differential signaling (LVDS), Local Interconnect Network (LIN), Media Oriented Systems Transport (MOST), FlexRay, and Controller Area Network Flexible Data-Rate (CAN FD).

CAN - 1983

CAN, developed by Bosch, is a shared serial bus that runs at up to 1 Mbps. The International Organization for Standardization (ISO) published the CAN standard in 1993. Its advantages are cost-effectiveness and reliability. Its disadvantages are shared access and low bandwidth. Power train, chassis, and body electronics use CAN.

LVDS - 1994

LVDS is a point-to-point link, not a shared bus. It has a much lower cost than MOST, and many automakers use it for camera and video data. However, each LVDS link can interface with only one camera or video output at a time.

LIN - 1998

A consortium of automakers and technology partners developed LIN. It runs at 19,200 bits per second and requires only one shared wire, compared with two for CAN. LIN uses a master-slave architecture, while CAN treats all nodes as equal. LIN costs less than CAN, and its speed and cost are suitable for body electronics such as mirrors, power seats, and accessories.

MOST - 1998

MOST has a ring architecture running at up to 150 Mbps (MOST150) using fiber or copper interconnects. Each ring can contain up to 64 MOST devices. MOST has the advantage of relatively high bandwidth for the automotive market, but it is costly. It was initially intended only for camera or video connections.

FlexRay - 2000

FlexRay is a shared serial bus running at up to 10 Mbps. The FlexRay Consortium, a group of semiconductor manufacturers, automakers, and infrastructure providers, developed FlexRay. Unlike CAN, FlexRay has no built-in error recovery; the application layer takes care of error handling. It has higher bandwidth than CAN, but has a higher cost and shared media. High-performance power train and safety systems, such as drive by wire, active suspension, and adaptive cruise control, use FlexRay.

CAN FD - 2012

CAN FD, released by BOSCH in 2012, is an extension to the original CAN bus protocol, intended to accommodate increases in bandwidth requirements in automotive networks. CAN FD enables more accurate and near-real-time data by minimizing protocol delays and delivering higher bandwidth. CAN FD is compatible with existing CAN networks.

4. A Better Way Forward

Autonomous driving and ADAS will bring benefits to society but will present engineers with new test challenges. With increasing demands for high data rates, bandwidth, data security, and future-readiness, automotive Ethernet offers advanced capabilities and overcomes limitations of traditional automotive serial buses for in-vehicle electronic systems connections and communications.

References

1. Apre, M., (2021), Why Automotive Ethernet is a strong choice, Retrieved from https://www.aptiv.com/en/insights/article/why-automotive-ethernet-is-a-strong-choice#:~:text=A%20key%20benefit%20of%20Ethernet,compute%20components%20in%20a%20vehicle.
2. Lim, M., (2021), Automotive Ethernet: The Future of In-Vehicle Networking, Retrieved from https://blogs.keysight.com/blogs/tech/sim-des.entry.html/2021/06/10/automotive_ethernet-E6FB.html
3. Saxena, A., (2020), Automotive Ethernet: driving in-vehicle communication for new-age vehicular functions, Retrieved from https://www.einfochips.com/blog/automotive-ethernet-driving-in-vehicle-communication-for-new-age-vehicular-functions/

M3R RADAR – ADVANCED COGNITION, AGILITY AND AUTONOMY CAPABILITIES

Ivan Y. Radev, Nikolay H. Kopanov, Petya N. Stefanova

Communication Networks and Systems Department, Artillery, Air Defense Communication and Information Systems Faculty, National Military University „V. Levski", Shumen, Bulgaria, secterity@abv.bg, nikolai.kopanov@abv.bg, petyastefanova0202@abv.bg

***Abstract**: The capabilities of modern multifunction/mission Radar can be only fully realized by using new sensor control strategies and the most obvious sensor management imperative is the development of optimal realtime waveform scheduling algorithms. This paper describes the functional architecture of radar resources management used for adaptive time budget optimization and key enablers for advanced cognition, agility and autonomy capabilities.*

***Keywords**: radar, cognition, scheduling, waveform*

Introduction

The capabilities of modern multifunction/mission radar can only be fully realized by using new sensor control strategies, due to the advance in array technology and development of waveform agility. The most obvious sensor management imperative is the development of real-time waveform scheduling algorithms that exhibit graceful degradation under overloads. The main objective of waveforms and dwells spacetime management is to optimize the sensor time budget to share and allocate resources of the array for different functions/missions/roles. The challenge is to take into account simultaneously time constraints (waveform duration/update rate, release-time/deadline of dwell requests,…) and priority constraints (priority allocation that assigns importance for each task) to find the optimal time sequence (especially in case of overload and for non-pre-emptive and non idling scheduling).

1. Extended air defence radar rationale

Applicative Radar is part of the Long Range Air Defense System that is a mobile detection system for Extended Air Defense. Extended Air Defence radar simulated in this study is a multi-mission radar used for both Air and Ballistic Missile Defenses, providing volume search in Air Defense modes and fence detection in Anti Tactical Ballistic Missile modes. It provides target designation to third party systems in charge of threat evaluation and engagement. This kind of radar has operational modes dedicated to Air Defense, providing detection of Air Breathing Targets including cruise missiles, and other modes dedicated to Tactical Ballistic Missile detection.

The Extended Air Defence radar is a multi-function radar with search and track capabilities used in rotating antenna state for Air Defense Surveillance as well as staring antenna state for longer range Anti Tactical Ballistic Missile Terminal Defense with Tactical Ballistic Missile fence detection. Acquisition on external cueing is another function of this Extended Air Defence that can be used in rotating or staring mode. Surveillance function performs Tactical Ballistic Missile detection and tracking in a 1000 km range domain. The tracking elevation coverage is up to 85°.

2. Functional architecture

Functional Architecture of Intelligent Radar resources management is defined by 2 main functions:

1) **RTM** ("Radar Task Manager"): takes into account information and generates Radar Tasks with appropriate dynamic priority and update rates according to Radar Load and Threat Levels. Operators can select different kind of "MENU" (related to different Search Time Budgets). Time Budget is managed at "soft" time scale (few seconds), with load regulator taking intosmoothed information from RDM.

2) **RDM** ("Radar Dwell Manager"): translates Tasks Table from RTM in elementary Dwell Requests. For each Dwell request, different candidate waveforms are allocated, and "instantaneous" priority are assigned (mixed of heritage from RTM Dynamic priority & scheduling policy constraints). Radar Load is handled and regulated at a "hard" time scale (few milliseconds). Dwells are scheduled and transmitted to the RBM ("Radar burst Manager") to be played by Antenna.

3. Intelligent radar resources management functions

We can divide the Intelligent Radar Resources Management functions in two mains categories :

Adaptive Resources Management:

• Dynamic Search Resources Allocation : "MENU" Selection with different time budgets (variant of nominal Search with changes of waveform durations & update rates), Dynamic Priority Allocation related to Threat information (de-masking area, Threatening area);

• Dynamic Track Resources Allocation: Dynamic Priority Allocation to Tracks related to Threat data (from C2, NCTR, kinematics,…), Load management by Active Track or "Track While Scan" strategies according to radar load, track priority and quality, Optimized Dwell Requests generation for Tack.

Initiation according to Threat Level (Track Init in One scan in threatening area), Robust Tracking strategies in case of maneuvering or stealth target (adaptive update rate against maneuver, re-enforced waveforms against S/N fluctuation, re-acquisition dwell/strategies,…), Active Track Request management over volume search limit (Track Init based on Confirmation for targets that get closer, Active Track dwell over search volume limit for targets that go away).

• Dynamic Resources Allocation according to Radar Environment Assessment : Robust Waveform including Doppler/range ambiguity solving and low false alarm rate, Active Dwell Regulation (e.g. Confirmation Dwell) in High Density False Alarm Area, Anti-Jamming Strategies, NCTR Dwell requests management to optimize active track resources allocation on higher threats.

Radar Time Budget Management:

• Local and global Radar Load Handling;
• Adaptive waveforms Computation according to clutter and target parameters (range, velocity, S/N);
• Advanced & adaptive scheduling algorithms.

Conclusion

M3R development program is a powerful engine to develop new concepts and architecture. Extended Air Defence Radar Time Resources Management is key-enabler to improve capabilities and performances of final radar product : higher autonomy (local resources optimization), agility (waveform adaptation) and cognitive ability (environment & threat assessment).

References

1. Adrian, O., (2008), M3R AESA Technology for Extended Air Defence, *IEEE International Radar Conference, Rome, May 2008*
2. Duron, C., (2002), Ordonnancement en temps-réel des activités des radars, *PhD thesis, Metz University, 20 December 2002*
3. Barbaresco, F., Intelligent Radar Resources Management, Tutorial, *International IEEE Radar Conference, RadarCon'08, May 2008, Rome*

QUANTUM IDEAS FOR PROVISION THE BEHAVIOR OF MICROSCOPIC OBJECTS

Yordanka M. Lambova, Veliko M. Lambov

Communication Networks and Systems Department, Artillery, Air Defense Communication and Information Systems Faculty, National Military University „V. Levski", Shumen, Bulgaria, y.lambowa@gmail.com, v.lambow@gmail.com

***Abstract**: We look at some of the quantum ideas that will allow us to predict the behavior of microscopic objects in the future. We will present some of the most popular quantum theories that will soon be at the core of future innovations.*

***Keywords**: quantum tunneling, quantum darwinism, Schrödinger's cat, quantum theories*

Introduction

Quantum mechanics studies an object not found in classical physics and is called quantum. In classical physics, it manifests itself either as a particle or as a wave, depending on the circumstances, but losing some of the properties of a quantum object. Classical images, concepts, time-space relationships, etc. therefore have (albeit approximately) their usual meaning. The quantum model also requires other images, concepts, etc., which do not have classical analogues, but allow to explain the observed patterns without a visual representation of what is happening.

Quantum physics deals with microscopic phenomena that a person is unable to detect only with the help of his senses. Quantum laws that summarize experimental facts about microscopic phenomena are not visual. This is the main difficulty in understanding them. Therefore, the best thing to do when you start studying the mechanics of microcosm (quantum mechanics) is to abandon the desire to build visual images of the objects and processes that are studied from the beginning.

Then comes an annoying question: how do fuzzy quantum probabilities suddenly focus on the clear certainty, or as physicists say - determinism - of the classical world? Physicists sometimes talk about this change as a "quantum-classical transition." But in fact, there is no reason to think that large and small are subject to fundamentally different rules, or that there is a sudden switch between them. Over the past few decades, researchers have become increasingly insight into the problem of how quantum mechanics inevitably becomes classical mechanics by interacting between particles or another microscopic system and the environment.

1. Quantum Darwinism

Quantum Darwinism explains why we experience the world the way we see it, rather than in the strange way that manifests itself in the scale of atoms and fundamental particles. Quantum physics isn't like that. It is not at all obvious that formal mathematical procedures speak of a "state of play" in relation to a quantum object. They are a kind of description that shows what we can come across after the measurement. For example, the same particle may have several possible states at the same time– this state of things is called "superposition". This does not mean that the particle is in several states at the same time – this means that when we make a measurement, we will see one of these results. And before the measurement, different states interfere with each other like waves, producing results with a greater or less likely.

Atomic-scale objects behave differently from larger ones. Your keys should be in one place or another, but an electron can be in two places at once, in the so-called "superposition" state. The position and momentum of your keys also exist. This is not the case for the electron: if you know its position, then its impulse should be indefinite and vice versa. Measuring the "collapsing" quantum state of the electron or wave function, how this happens remains unclear. Similarly, physicists have suggested that the keys may not be here and there because something has collapsed its superposition one way or another -- perhaps contact with the surrounding area. Quantum Darwinism is justified by quantum superposition? Why don't all these probabilities of different particle states survive, increasing to human scale?

The super position is a fragile thing, easily broken when the quantum system encounters a noisy environment. But it's not. Two quantum objects, interacting, "entangle" each other, entering a common quantum state in which the probabilities of their properties begin to depend on each other. The right kind of entangle is key to the theory. The keys must interact with the environment in a way that depends on position, not inertia. Most interactions between a large object and its environment depend on its location. If we put an atom in a superposition of two possible states of its quantum property called "rotation": states "up" and "down". We release an atom into the air, where it collides with an air molecule and entangles with it. Now they are in a common superposition. If the rotation of the atom is directed upwards, then the air molecule can be repelled in one direction, and if down, then in the other-and these two possibilities exist together. As the number of collisions with other air molecules increases, entangling spreads, and the super position once connected only to this atom becomes even more scattered. The states of the atom no longer interfere coherently with each other, since they are now entangled with other states of the environment . It looks as if the super position of the atom has disappeared and has been replaced by possible classical states that no longer interfere with each other. This process, in which "quantumity" disappears into the environment, is called decochereence. This is a critical part of the quantum-classical transition and explains why it is difficult to see quantum behavior in large systems with many interacting particles. This process is extremely fast. If a simple speck in the air is given a quantum superposition at two different physical locations located at a distance as far as the width of this speck from each other, then collisions with air molecules will lead to decocherence . Even in a vacuum, photons of light will quickly cause decocherence: you can not look at a speck without destroying its superposition.

2. Quantum tunneling

Quantum tunneling is the quantum mechanical effect of transition through a classically forbidden energy state. Quantum mechanics makes it possible to identify and study the potential barrier not only in the classic "hull" transition above it, but also through tunnel "wave" penetration through the barrier "tunnel effect" or "tunneling". Transmission through the barrier can be extreme and depends exponentially on the height and width of the barrier. The wave function can disappear on one side and reappear on the other side. The wave function and its first derivative are continuous. At steady state, the probability forward flow is spatially even. Not a single particle or wave is lost. As much as we wish, we can't go through walls, but that's what microparticles in the quantum world can do through one of a series of "wonders" of quantum mechanics: the tunnel effect. And just as large waves crashing into the breakwater can cross it, quantum particles can end up on the other side of an insurmountable energy barrier, according to classical physics, because as you can think of, they are both particles and waves. Quantum-mechanical tunneling occurs when the same system spontaneously passes from one state to another with lower energy, in the presence of an energy barrier, accompanied by the radiation of excess energy. The quantum mechanical tunneling process requires two important properties:

2.1. The physical system must have more than one energy state in order to allow for a transition between these conditions.

2.2. This system must have an energy barrier to complicate such transitions from one state to another. Since all physical systems tend to look for the lowest energy state, which is called the main condition: water, for example, always flows from the mountain down to the sea, not vice versa. In the absence of such an energy barrier, the physical system quickly transitions to a state with the lowest energy, where it remains forever.

When the physical system is closed in a state of higher energy, at some point in the future a transition to a state of minimum energy may be made, even if the energy of the system is less than the minimum energy required to overcome this barrier. This physical system can be an atom, a nucleus, or the vacuum configuration of the universe itself. According to classical mechanics, the particle can only be at such points in space, where its potential energy is less than its full energy. This follows from the fact that the kinetic energy of the particle cannot be negative at least in classical physics, since in this case, the pulse will be an iggy magnitude. Thus, according to newton mechanics laws, if two areas in space are separated by a potential barrier, so, passing particles through it is impossible.

In quantum mechanics, things are quite different. Because of the wave character that reality acquires over small distances, nature is never fully defined. Physical systems are constantly experiencing fluctuations due to the principle of uncertainty. And these quantum fluctuations are allowed, at first glance, forbidden events. If the ball scheme is replaced, with an electron, and the hill-with some electrical barrier, we will get a similar system, in which, however, quantum-mechanical effects are manifested. The tunnel effect can be imagined as a wide wave approaching and overlapping a barrier. Although the main part of the wave can never pass through the barrier, a small part of the wave, due to uncertainty, suddenly generates a wave on the other side of the barrier. In quantum mechanics, a particle is described by a wave function that gives only a probability of the location of the particle in a given place and at a given time. If the particle collides with a potential barrier, Schrödinger's equation allows us to calculate the probability of the particle penetrating behind it, with the wave function simply energy absorbing the barrier and quickly, exponentially extinguishing after it. The potential barrier in the quantum world, unlike the world of Newton physics, is fuzzy, and while it still interferes with passage, it is not such a rigid and impenetrable frontier as in classical mechanics.

The probability that the electron will turn out to be "on the wrong" side of the potential barrier is usually relatively small, but not zero. Because of the uncertainty, in practice, with sufficient time, the electron is always made a transition from the left pad into the state of lower energy, which provides the right pad, where it usually remains. When an electron makes a transition from one pad to another, it actually "permeates" , passes under the energy barrier. In this sense, it tunnels through the barrier, and this process is called quantum mechanical tunneling or tunneling effect.

3. Quantum superposition

Quantum superposition is a fundamental principle of quantum mechanics. It states that, like waves of classical physics, any two (or more) quantum states can be added together and the result will be another valid quantum state, and vice versa, that each quantum state can be represented as the sum of two or more other different states. The principle of quantum superposition states that with two open slits, the particle is in a state of superposition of the first and second states, and accordingly its wave function is the sum of two wave functions. This amount leads to the appearance of an interfering pattern. In this sense, it is said that the particle passes through the two slits at the same time. Surprisingly, despite the role that the double-slit experiment plays in quantum physics, many scientists misunderstand it. Moreover, this incorrect explanation is present in most textbooks on quantum mechanics. The fact is that the phenomenon of superposition in this experiment is usually explained as follows: the wave function of the state in which the electron passes through two slots is the sum of the wave functions of the states in which it would be if one of the slots were closed. However, this explanation does not take into account that by opening the second slit, we can change the way the electron passes through the first. Renowned physicist Robert Boyd conducted an experiment in 2014. (he is known, for example, for the fact that the

first performed an experiment with "slow" light) and his colleagues suggested increasing the "severity" of non-classical trajectories near a plate with slits through the use of so-called plasmons. Plasmons are a kind of "photons on a leash", which can move only on the metal surface from one slit to another. To do this, a plate with slits is made of gold. Gold is an excellent conductor, so it creates particularly strong plasmons.

In the experiment, the light source irradiated only one of the three slits. Moreover, if the other two were closed, then a typical picture of a slightly blurred tape against the open slit was observed. But when the other two slits were opened, the picture was radically different: a typical interfering pattern with much narrower stripes appeared.

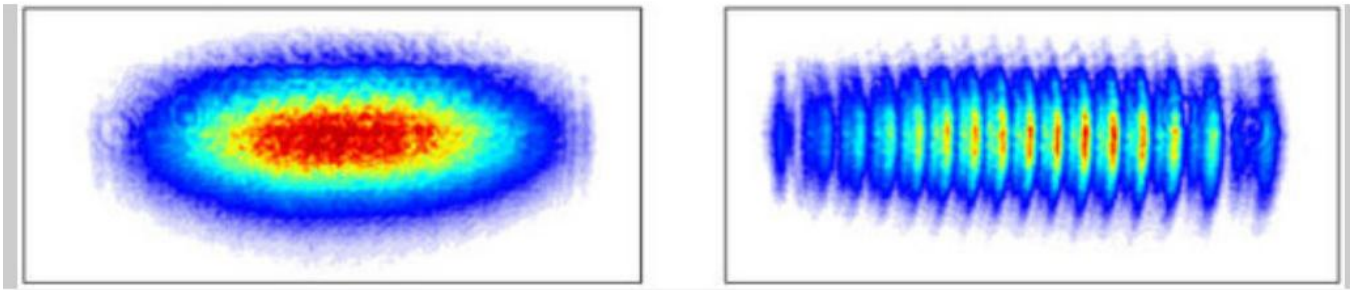


Figure 1: Quantum superposition

Compare images on the screen (fig. 1) when two of the three slits are closed (left) and when all three slits are open (right) Can these studies have any practical value? The phenomenon of quantum superposition is widely used for so-called quantum communication. On its basis, for example, quantum cryptography works. This is the phenomenon of supercontest that gives quantum computers undeniable advantages over computers based on traditional electronics. Therefore, in these directions, an accurate understanding of how quantum superposition works is extremely important. And that's why we hope that research into three-slot interference will help invent new, more effective protocols for quantum devices to work.

4. Schrödinger's cat

Erwin Schrödinger's original article was published in 1935. The box contains a mechanism containing a radioactive atomic nucleus and a container of poison gas. The experimental parameters are selected so that the probability of nuclear decay in 1 hour is 50%. If the core breaks down, the gas container opens and the cat dies. If the core does not disintegrate, the cat remains alive and well. We close the cat in a box, wait an hour and ask ourselves: is the cat alive or dead? Quantum mechanics, so to speak, tells us that the atomic nucleus (and therefore the cat) is in all possible states at the same time (see quantum superposition). Before we open the box, the "cat core" system is able to "the nucleus has disintegrated, the cat is dead" with a probability of 50% and in a state "the nucleus has not disintegrated, the cat is alive" with a probability of 50%. It turns out that the cat sitting in the box is alive and dead at the same time. According to the modern Copenhagen interpretation, the cat is still alive/dead without any intermediate conditions. And the choice of the state of decay of the nucleus becomes not at the moment of opening the box, but even when the nucleus enters the detector. Because the reduction of the wave function of the cat-detector-core system is not related to the human observer of the box, but is related to the detector-observer of the nucleus. According to quantum mechanics, if the nucleus of the atom is not observed, then its condition is described by a mixture of two states - a decaying nucleus and an undistinguished nucleus, therefore a cat sitting in a box and embodying the nucleus of the atom is alive and dead at the same time. If the box opens, then the experimenter can see only one specific condition - "the core has disintegrated, the cat is dead" or "the core has not disintegrated, the cat is alive". The essence of human language: Schrödinger's experiment showed that from the point of view of quantum mechanics,

the cat is both alive and dead, which it can't be. Therefore, quantum mechanics has significant drawbacks. The question is this: when does a system cease to exist as a mixture of two states and choose one specifically?

The aim of the experiment is to show that quantum mechanics are incomplete without some rules specifying under what conditions the wave function crashes and the cat either becomes dead or stays alive, but ceases to be a mix of both. Since it is clear that the cat must necessarily be either alive or dead (there is no intermediate state between life and death), this will be the same for the atomic nucleus. It must necessarily be either decomposed or undeveloped.

Conclusion

Quantum computing systems are one of the most promising technologies at the moment. It is assumed that they will become the first in the world with full-fledged artificial intelligence, will be able to compare computer and military systems, simulate new materials and light. It is also possible that in the future, quantum systems will be able to collect game data in a virtual universe that mimics all the physical laws of fictional worlds.

In other words, a quantum computer is a computing device that uses the phenomena of quantum mechanics to transmit and process data.

References

1. De Raedt, H., & Hess, K., (2012), Multi-beam interference analysis in three-slit experiments
2. Sawant, R., Samuel, J., Sinha, A., Sinha, S. & Sinha, U., (2014), Nonclassical pathways in experiments with quantum interference
3. Herzenberg, C. L., (2007), Why our human-sized world behaves classically, not quantum-mechanically A popular non-technical exposition of a new idea, Retrieved from https://arxiv.org/ftp/physics/papers/0701/0701155.pdf(04.09.22)

INTRODUCTION OF TECHNOLOGIES IN MEDICINE BASED ON ARTIFICIAL INTELLIGENCE

Aleksandra K. Atanasova

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

Abstract: *Artificial intelligence is pervasive and surrounded all around us. AI is an imitating machine that mimics human behavior. Its application is immeasurable and as the years go by, its practice is expanding more and more. Our society has a huge potential thanks to the various fields of artificial intelligence such as healthcare, technological sciences, transportation and others. Through optimal solutions can be found there, as AI can process large volumes of data and recognize patterns for work.*

Keywords: *Artificial intelligence, medicine, technology, electroencephalography, digital assistant*

Introduction

Historically, artificial intelligence (AI) is not new. The technology was developed back in the early 1950s with Alan Turing's project, to which the famous Turing test belongs. Much later, the DEEP BLUE chess supercomputer - the first machine to beat world chess champion Garry Kasparov in 1997.

With each passing day, humanity moves one step closer to a future in which machines and humans will live in closer symbiosis. Behind the very definition of artificial intelligence hides experience and realization, with which human activity can be copied.This is done with the help of computer programs or mechanisms, that react as a person would react in a given situation.

Artificial Intelligence (AI) is getting very close to computer science, which creates not only intelligent machines, but which can also react and function like humans.

By defining commands in a linear fashion, it uses written instructions from algorithms. Every computer system is based on such algorithms and responds to certain commands and data.

These days, AI software analyzes and generates data-driven decisions that are too complex to analyze to process.

AI works mainly to study how the human brain thinks and functions, how people make decisions and solve problems. All research results are created through the development of intelligent software and systems.

AI is still in such a field where it causes many questions and the most diverse reactions from people. It is all around us in almost every field. Medicine is one of those fields in which AI is actively involved. An example of this is the placement of accurate diagnosis. Namely, AI is developing in this direction. Yes, intelligently, quite realistically, it can replace the doctor's diagnosis and make a correct one on the basis of many such.

1. Artificial intelligence in Electroencephalography

Artificial intelligence is not a mind of its own. It is a set of systems that process massive data based on machine learning. In the future, it is expected that human intervention will not be a necessary factor as AI will free us from routine work in many spheres. Its inevitability of use quite often enters medicine.

Currently, there is still no fully built model that replicates the human brain.However, there are a number of developments based on artificial intelligence.

One of the examples of artificial intelligence is the so-called electroencephalography. It is a recording of signals that arise from the work of the brain, which measure the electrical potential that arises on the scalp. With the help of millivolts in medicine, the signals that are measured are used, that is, whether a person is asleep or in a coma.

Figure 1: Electroencephalography

Thanks to these devices, signals are captured and recognized seamlessly.

When a given group of people watch a certain media, it is possible to recognize second by second what most attracted and interested their attention from the given media content directly by their brain activity, without giving any opinion on the content in question.

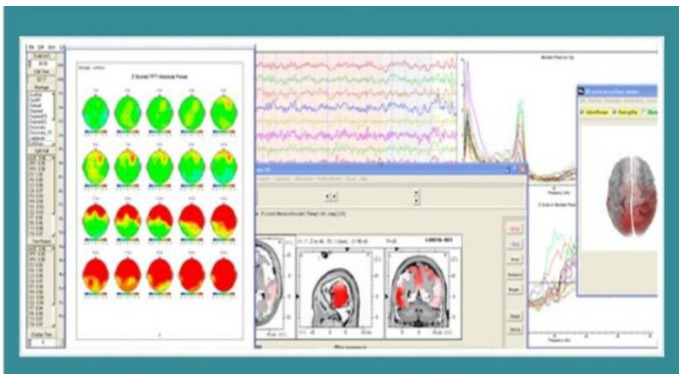


Figure 2: Computed tomography

The volume of data that passes through the wireless computer system records all electrical brain activity. The recording with the electroencephalograph takes place within 30 minutes. The recording is then subjected to computer processing and analysis.

The functional activity of the brain is studied, with a goal suitable for the examination of people with a disease of the central nervous system.

2. Artificial intelligence in health apps

It is quite difficult for patients to get an accurate diagnosis, because doctors, no matter how experienced, cannot always see the full picture of patients' illnesses. Cons such as fatigue and insufficient competence in a certain area prevent an accurate diagnosis.

From Google, they create a "digital assistant" Google (Deepmind Health) and IBM (Watson Health).

As doctors' first friends, these products help with diagnoses by analyzing patient information and symptoms and then providing a list of instructions to doctors.

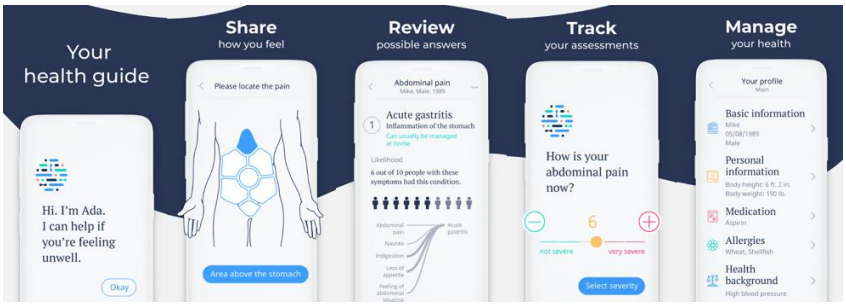


Figure 3: Ada application

Another innovative application that saves many doctors and clients time is the Ada application. It represents a chatbot that diagnoses the client's illness.

An example of this is when a person is not feeling well, his first job is to check his symptoms on Google. Then he has to decide for himself whether he should see a doctor or not.

But this is where artificial intelligence intervened.

Users of the Ada app enter their symptoms and based on that the chatbots ask a lot of questions based on the information they have received. After all the questions the chatbot directs treatment or book appointments with a doctor, as well as enter video chats with them.

Ada analyzes all past diagnoses, symptoms and risk factors. It is a kind of preliminary consultation before the user is directed to a real specialist.

Ada not only provides help to consumers, but also to doctors.

The main idea of the application is to relieve medical personnel. The artificial intelligence based on very similar applications such as Ada, processes all the information of patients with the same symptoms and thus suggests to doctors what treatment to turn to.

3. AI in neuroncology

Intensive clinical applications of artificial intelligence in neuro-oncology could fundamentally change things for people with brain problems, for example.

The promise of artificial intelligence is that it is taking its first steps by using its algorithms.

They enable the identification of patients with brain tumors through complex repetitive images in the nuclear magnetic resonance images. Their application is drastic, prognostic and therapeutic.

In fig. 4 a diagram of the types of elements of artificial intelligence - AI, machine learning, neural networks, deep learning - are depicted.

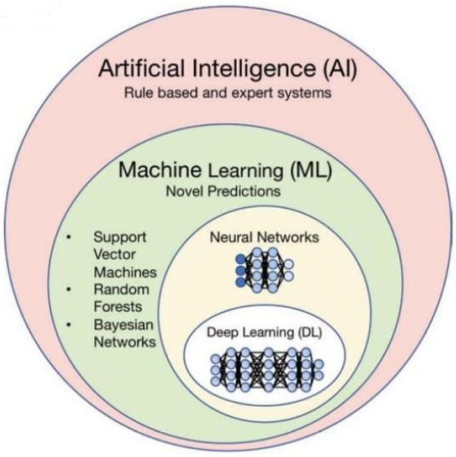


Figure 4: Diagram of the types of elements of artificial intelligence

Nowadays, we don't think about how many things we do routinely, and we don't realize that without the use of AI, many activities and tasks would be missing.

AI is already an indispensable part of our lives.

The most elementary example of such a system is Apple's online assistant Siri (digital assistant) that serves customers.

Siri records our voice in the form of sound waves and forms them as a code.

The code is converted as an algorithm and sends a certain number of combined sentences to form the meaning of the phrase.

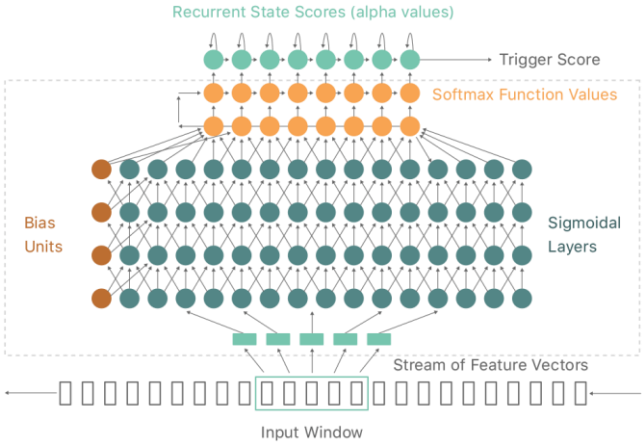


Figure 5: The deep neural network used to detect "hey siri"

The neural network method is based on teaching computers to process data similar to the human brain. The machine learning process uses inherently connected nodes (neurons) in a layered structure similar to the human brain.

The digital assistant uses a deep neural network.DNN is mainly matrix multiplication and logistic nonlinearities. Hidden and the layers are linked. The topmost layer performs temporal integration while the actual neural network is indicated by the dashed box.

Neural networks find application not only in digital assistants in the distribution of text and voice, but also, as already implied, in neuro-oncology.

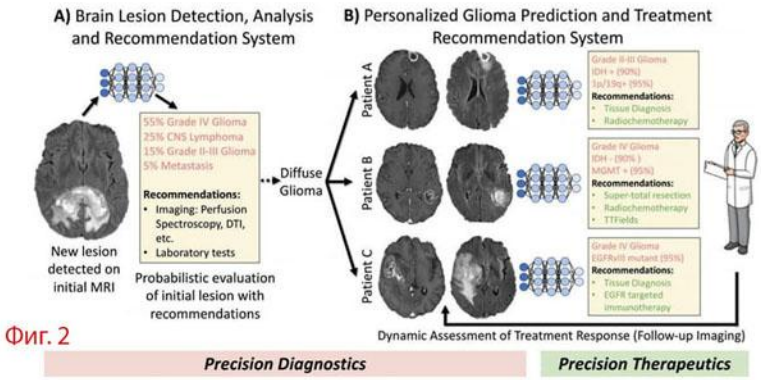


Figure 6: Schematic representation of future neurodiagnosis based on AI methods.

Figure 6 depicts the future innovative neurodiagnosis based on artificial intelligence.

Where under point A is the initial detection of a tumor in the brain, which allows to create a model of glioma and appoint recommendations for further research.

In point B, a model of expected glioma development and possible therapies is discussed.

This type of modality also aims to formulate the final personal treatment plan.

Conclusion

Artificial intelligence is becoming more and more influential with each passing year.

The potential of AI in healthcare has its pros and cons. Patient status will be managed from mobile devices. This technology allows people to check their health status just by entering their symptoms, as well as advise doctors about the critical condition of the sick. With the advent of chatbots, the emotional and living connection between doctor and patient is drastically lost, as the diagnosis and examination of the patient will become digital. Chatbots also support human decisions by providing a treatment plan. In the future, it is possible that the chatbot itself will replace the doctor of flesh and blood.

References

1. Siri, H., (2017), An On-device DNN-powered Voice Trigger for Apple's Personal Assistant, Machine Learning Research, Retrieved from https://machinelearning.apple.com/research/hey-siri

2. SmartDataCollective, (2008-2022), Artificial Intelligence Chatbots Could Make Your Doctors Obsolete, Retrieved from https://www.smartdatacollective.com/artificial-intelligence-chatbots-could-make-your-doctors-obsolete/

3. FUTURIST.BG, (13.06.2019), The future of medicine: how artificial intelligence is rushing into it, Retrieved from https://futurist.bg/ai-v-medicinata/

4. HEALTHIX, (2021), https://www.biofeedback.bg/elektroencefalografia/

5. Gerganov, V., (2020), Artificial intelligence and the era of "precision medicine" neuroncology, Retrieved from https://dr-gerganov.eu/bg/news/Izkustven-intelekt-i-erata-na-„pretziznata-meditzina"-Nevroonkologiya/

SOCIAL STUDIES

SYNCHRONISATION OF THE PROCESSES OF SOCIOLOGICAL STUDY ON THE QUALITY OF EDUCATION AND THE LEARNING LESSONS PROCESS AT THE RAKOVSKI NATIONAL DEFENCE COLLEGE

Zarko I. Zdravkov, Zhivo B. Petrov, Anelia A. Atipova, Sevdalin H. Stoykov

DARI, Rakovski National Defence College, Sofia, Bulgaria, z.zdravkov@rndc.bg

***Abstract**: In the paper are examined the processes of lessons learning and a sociological survey of the opinion of cadets and students on the quality of learning,. The possibility of achieving synergy by reconciling them is analysed. The aim is to increase the effectiveness of the decisions taken by the academy's leadership to address emerging problems and to reinforce and disseminate identified positive practices.*

***Keywords**: lessons learned, sociological study, quality of education, monitoring, analysis*

СИНХРОНИЗИРАНЕ НА ПРОЦЕСА НА СОЦИОЛОГИЧЕСКО ПРОУЧВАНЕ ЗА КАЧЕСТВОТО НА ОБУЧЕНИЕ И ПРОЦЕСА ПО ИЗВЛИЧАНЕ ПОУКИ ОТ ПРАКТИКАТА ВЪВ ВОЕННА АКАДЕМИЯ „Г. С. РАКОВСКИ“

полк. доц. д-р Зарко И. Здравков, полк. доц. д-р Живо Б. Петров, гл. ас. д-р Анелия А. Атипова, ас. д-р Севдалин Хр. Стойков

ИПИО, Военна академия „Г. С. Раковски“, София, България, z.zdravkov@rndc.bg

***Abstract**: В доклада са разгледани процесите на извличане на поуки от практиката и на социологическо проучване на мнението на слушателите и студентите за качеството на обучението и е анализирана възможността за постигане на синергия, чрез съвместяването им. Целта е повишаване на ефективността на вземаните решения от ръководството на академията за отстраняване на възникващите проблеми и затвърждаване и разпространение на идентифицираните положителни практики.*

***Keywords**: поуки от практиката, социологическо проучване, качество на обучението, наблюдение, анализ*

Увод

Планирането и провеждането на преподавателска и научноизследователска дейност във Военна академия подлежат на непрекъснат мониторинг и контрол, с цел подобряване качеството на обучението[2]. Този контрол се осъществява съгласно изискванията на нормативната уредба [7] и възприетите добри практики[10], както в сектора на образованието и науката, така и в МО и БА.

Водеща роля в разкриването на недостатъци и идентифицирането на добри практики има процесът по извличане на поуки от практиката[8]. Той е залегнал в основата на проучването на всички дейности по изграждането на способности за изпълнение на мисията и задачите на Военна академия „Г. С. Раковски" .

Паралелно с това, за оценка на качеството на обучение, чрез обратна връзка, в рамките на академията се извършва ежегодно социологическо проучване на мнението на слушателите и студентите от факултетите „Национална сигурност и отбрана" и „Командно-щабен". Основна задача на проучването е да се открият недостатъци в качеството на учебния процес.

Процесът по поуки от практиката обхваща цялата способност за учене от опита, докато посоченото социологическо проучване визира само качеството на обучението.

Въпреки, че целите и задачите, в частта „обучение" и „учебно-материална база", на двата процеса се припокриват в значителна степен, те се провеждат независимо един от друг, с различна честота и липсваща координация. В резултат, решенията от двата процеса се вземат независимо един от друг на базата на отделни анализи. Това се дължи основно на факта, че те са въведени за изпълнение по различно време и на различно основание.

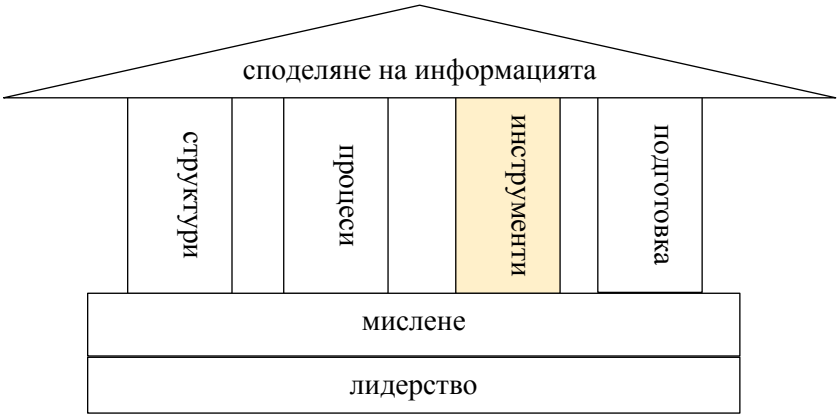
В доклада са разгледани двата процеса и е анализирана възможността за постигане на синергия, чрез съвместяването им. Целта е повишаване на ефективността на вземаните решения от ръководството на академията за отстраняване на възникващите проблеми и затвърждаване и разпространение на идентифицираните положителни практики.

1. Процес по извличане на поуки от практиката в дейността на Военна академия „Г.С. Раковски"

Процесът по извличане на поуки от практиката е целенасочена дейност на „учене от опита", като идеята е чрез научените уроци да се намали риска от повтарящи се грешки и да се увеличи оперативната ефективност на дадена организация[10].

Процесът широко се прилага в структурите на НАТО[10], като регламентирането му в рамките на Българската армия е определено с „Ръководство за поуки от практиката във Въоръжените сили"[7] от 2020 г. Във Военна академия „Г. С. Раковски", също е създадена организация по извличане на поуки от практиката[8]. Формирана е специална постоянно действаща работна група, включваща представители на ръководния, академичния и експертния състав, която има за цел да извършва наблюдения и анализи, като идентифицира поуки и добри практики, които да се валидират и утвърждават чрез коригиращи действия.

Ключовите елементи на процеса по извличане на поуки от практиката са определени в „Ръководство за поуки от практиката във Въоръжените сили" [7] и са показани на фигура 1.



Фигура 1: Ключови елементи на процеса по извличане на поуки от практиката

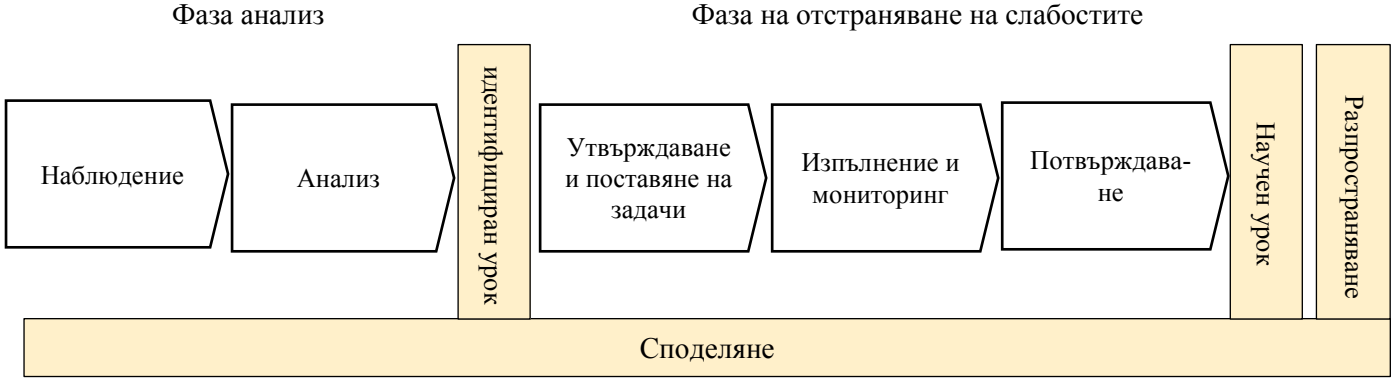
В основата на процеса са мотивацията и разбирането на необходимостта от оптимизиране на дейностите в организацията. Това неизменно е свързано с креативност, лидерство и воля за промяна.

Градивните стълбове на процеса са:

- структури – създадените организационни елементи;
- процеси – отделните дейности формиращи процеса;
- инструменти – средствата за изпълнение;
- подготовка – необходимите знания и умения.

Споделянето на информация покрива всички ключови елементи. Така, чрез сътрудничество и координация между членовете на организацията се постига единна цялост на процеса.

Разгледан във времевата проекция, процесът по извличане на поуки от практиката се разделя на фазите „анализ“ и „отстраняване на слабостите“, като отделните етапи са показани на фиг. 2.



Фигура 2: Етапи на процеса по извличане на поуки от практиката

Базов елемент на ученето от опита е формирането са наблюдения. Това е началния етап на процеса по извличане на поуки от практиката. Той е в резултат на събитие с неблагоприятни ефекти или при установяване на устойчив успех, което налага необходимостта от провеждане на наблюдение с цел изясняване на причините.

Добра практика е да се извършват наблюдения на организацията и от външна гледна точка, като се спазва принципът на „ограничена степен на анонимност“, т.е. личността на респондента

не е известна, но е известна принадлежността му към конкретно звено от организационната структура.

Начините за формиране на наблюдение са два – чрез активно или пасивно събиране на информация. При активния начин информацията се събира чрез целево командироване на групи за наблюдение в районите на събитията, а при пасивния начин се разчита на данни от съществуващи документи.

Наблюденията биват два вида – необработени и обосновани. Необработени наблюдения са тези при които се изисква допълнително изследване или анализ за пълно изясняване на първопричините, а обосновани са тези при, които са събрани достатъчно данни и има яснота за причините за възникване.

Трансформацията на наблюдението в установена поука се осъществява чрез анализ, като се разкрива корена на проблема и се определят подходящите коригиращи действия. Анализите дават отговори на въпросите „кой, какво, кога, къде и защо" като се очертава къде се корени проблема или постигнатия успех[9]. При анализите в важно да се отбележи, че всички възможни източници са проверени и че са отразени различни гледни точки с цел пълно разбиране на проблемните въпроси[3, 6]. Необходимо е да се разкрие не само какво се е случило, но и защо се е случило.

След определяне на необходимите коригиращи действия се разработва и изпълнява план за действие. Потвърждаването на изпълнението на коригиращото действие или, че поуката е възприета, се осъществява под контрола на постоянно действащата работна група във ВА. Процесът да не завършва, докато не се потвърди, че са настъпили промени, като резултат на проведените коригиращи действия.

Въпросниците са ефективен инструмент за събиране на допълнителни данни, в случаите, когато е необходимо да се събере една и съща информация от голям брой източници. Това е еднакво валидно за етапите „наблюдение" и „изпълнение и мониторинг". Правилното структуриране на въпросите, тяхното групиране, кодиране на търсената информация и оптималния им брой, предоставят висока степен на яснота относно позициите на респондента. Въпросите могат да бъдат затворени (с посочване на един или повече отговора), отворени (които дават възможност за свободна интерпретация по даден проблем от страна на респондента), по Ликертова скала (отчитащи степен) и обикновено събират данни за „нагласи, убеждения, поведение и атрибути". Обработката на данните се извършва с подходящ софтуер за статистически анализ, като в рамките на Военна академия се използва IBM SPSS 22.

Процесът на извличане на поуки от практиката във Военна академия „Г. С. Раковски" се основава на принципите на непрекъснатост и външната оценка.

По отношение на първия принцип, всяко наблюдение, докладвано по съответния ред, следва да бъде разгледано, дори в случаите, когато идентифицираният на тази база урок има характера на междинен продукт от процеса. Това е разписано в Указанията за провеждане на процеса по извличане на поуки от практиката, съгласно които, при постъпили извън редовните сесии доклади, „действащата работна група провежда извънредни заседания за [..тяхното] обсъждане и определяне на мерки за решаване на проблемните въпроси".

Що се отнася до външната оценка, допълнителни проучвания, които се основават на мнението на лица, различни от експертния и академичния състав, би могло да се окаже изключително полезно.

Социологическо проучване на мнението на обучаемите за качеството на обучението във Военна академия

Оценката на випускниците за качеството на обучението във Военна академия „Г. С. Раковски" е социологическо проучване, въведено със Заповед на Началника на Военна академия „Г. С. Раковски"0, което се извършва веднъж годишно, съгласно разпоредбите на Закона за висшето

образование, Закона за въоръжените сили на Република България и Правилника за учебната дейност на Военна академия „Г. С. Раковски"[5]. Извършва се по разработена методика [0,4], а за постигане на целта му, се решават следните дейности:

• Определяне обхвата на изследването – определени са 10 въпроса, оценяващи съдържателни аспекти от качеството на обучението и 7 въпроса, оценяващи нагласите на випускниците относно социално-битовите услуги и удобства в академията;

• Подбор на респонденти – извършва се със слушателите и студентите от факултет „Командно-щабен" и факултет „Национална сигурност и отбрана" на Военна академия;

• Създаване на въпросник за анкетна карта – използва се метода пряка анонимна анкета, като са конструирани диференцирани анкетни карти за всяка специалност или специализация, съобразно разработените учебни планове;

• Провеждане на проучване – провежда се в заключителния етап на обучението;

• Анализ и обобщение на резултатите – използва се набор от статистически методи за анализ и контент-анализ.

Съгласно методиката за провеждане на социологическо проучване за оценка мнението на слушателите и студентите от Военна академия отговорите на въпросите включват петстепенна скала, а резултата се получава, чрез изчисляване на средноаритметични величини.

Изследването обхваща следните предметни области:

• Обща удовлетвореност на обучаемите – оценява цялостното усещане на респондентите;

• Материално-техническа осигуреност на обучението – оценява пригодността на материалната база, чистота на помещенията, технически възможности и достъп до техника и места за самоподготовка;

• Административно осигуряване – оценява организацията на учебния процес и административното обслужване;

• Информационно осигуряване – оценява навременността и достоверността на предоставяната информация;

• Планиране на учебния процес – оценява планирането на учебните занятия и изпитната сесия;

• Ефективност на изучаваната специализация – оценява съответствието и яснотата на преподавания материал, спрямо тематиката на дисциплините;

• Система за оценка и контрол на знанията – оценява обективността и неутралността при оценяване;

• Удовлетвореност от определени аспекти от обучението – оценява придобитите компетентности, знания и умения; отношенията с преподавателите и възможностите за научноизследователска дейност;

• Проведено дистанционно обучение – оценява уменията за презентиране, предоставените материали и достъпността и качеството на връзката;

• Задължителни дисциплини – оценява адекватността от гледна точка на актуалност на преподавания материал и практическа насоченост на занятията.

Следващите количествено оценявани предметни области обхващат социално-битовите условия в академията и включват: условия за хранене в стола, условия за консумация на храни напитки в бара, условия за спорт, условия за паркиране, среда за отдих и достъпност на параклиса на Военна академия. Всички те се оценяват посредством опциите „Да", „Не", „Отчасти" и изключващата опция „Не ползвам тази услуга".

Последният въпрос в блока е формулиран като „Коментари и предложения за подобряване на социално-битовите услуги и удобствата". Той е отворен въпрос и отговорите по него се анализират чрез контент-анализ.

Така структурираната методика дава широк поглед върху мнението на обучаемите по практически всички аспекти на учебния процес и материално-техническата база, като същевременно

позволява допълнение на проблемни области, незастъпени в анкетната карта, които обучаемите считат за важни. По този начин, тя покрива съдържателно предимствата на метода интервю и метода анкетна карта, използвани за получаване на допълнителна информация в процеса по извличане на поуки от практиката.

Оценка на съвместимостта на процесите

За оценка на съвместимостта на процесите на социологическо проучване за оценка качеството на обучение и извличане на поуки от практиката във ВА се извършва анализ на характеристиките на двата паралелно протичащи процеса, който допуска наличието на съвместимост в следните области (таблица № 1):

1. Целева съвместимост – обхваща параметрите цел и задачи.

2. Съвместимост по ограничения – обхваща параметрите интегрираност, обхват и честота.

3. Методическа съвместимост – обхваща параметрите методически аспекти и субординация.

4. Информационна съвместимост – обхваща параметър инструментариум.

5. Годност на информацията за формулиране на наблюдения – обхваща параметър инструментариум.

Таблица № 1

Сравнителни параметри на процесите по оценка качеството на обучение и извличане на поуки от практиката от процеса по обучение във ВА „Г. С. Раковски"

Параметри за сравнителен анализ	**Социологическо проучване за оценка качеството на обучение във ВА**	**Извличане на поуки от практиката**	**Степен на съответствие**
Честота	Веднъж годишно	Непрекъснато	Висока
Цел	Подобряване на качеството на обучение във ВА, чрез оценка на мнението на слушатели и студенти.	Подобряване на качеството на обучение във ВА чрез учене от опита.	Висока
Задачи	Оценка на качеството на обучение във ВА, формирана на базата на мнението на слушатели и студенти	Оценка на: - схващанията за използването на войските и силите; - програмите за обучение на офицерите,; - методиката за преподаване; - повишаването на квалификацията на преподавателите; - оценяването на обучаемите, научно-преподавателския и научноизследователския състав; - качеството на обучение; - реализацията на обучаемите на различни нива и категории; - усъвършенстването на учебно-материалната база.	Частична
Обхват	Процес на обучение на слушателите и студентите от ВА	Целият обхват на мисията и задачите на ВА	Частична

Параметри за сравнителен анализ	**Социологическо проучване за оценка качеството на обучение във ВА**	**Извличане на поуки от практиката**	**Степен на съответствие**
Методически аспекти	Анкетиране на слушателите и студентите във ФНСО и ФКЩ	Събиране и анализ на наблюдения след събитие.	Частична
Инструментариум	Пряка анонимна анкета, с диференцирани анкетни карти, съгласно учебните планове, статистически анализ (Ликертови скали за оценка) – за първична инфромация	Обмен на мнение (за първична информация), интервю, анкетна карта (за допълнителна информация)	Висока
Субординация	Инструмент в етап от процеса по извличане на поуки от практиката	Използва социологическия анализ като инструментариум	Висока
Интегриране	Налични условия за интегриране на социологическото проучване в процеса на учение от опита	Налични условия за интегриране на социологическото проучване в процеса на учение от опита	Висока
ОБЩА СЪВМЕСТИМОСТ НА ДВАТА ПРОЦЕСА			**ВИСОКА**

Възможността от съвместяване на социологическото проучване в общия процес по извличане на поуки от практиката във ВА, произтича от регламентирането и изпълнението и на двата процеса, посредством заповеди на Началника на Военна академия. Ученето от опита включва по-широк периметър от дейности, в рамките на един и същ обхват – процесът на обучение. Социологическото проучване попада по естествената логика на субординация в рамките на извличането на поуки от практиката във фаза „Анализ", етапи „Формулиране на наблюдение" и „Анализ на данните от наблюдение", като допълващ информационно-обслужващ процес, с регулярен характер.

Най-съществената съвместимост между двата процеса е информационната. Информацията, получавана регулярно от социологическото изследване, може да е основна или допълваща по съдържание информацията, получена от други източници, в рамките на процеса по извличане на поуки от практиката. Информационната съвместимост е съвместимост по данни и по метаданни[1] и се реализира през целево разработени въпросници.

Налице е методическа съвместимост, която се наблюдава между стъпките на провеждане на двата процеса, а именно – събирането и обработването на информация, изготвянето на доклади, както и посредством ползването на сходен инструментариум.

Наблюдава се и съответствие в ограниченията при имплементиране на двата процеса, като за тях са валидни принципите на „ограничена степен на анонимност", „външна оценка" и „непрекъснатост на информационното постъпление". Първият принцип предполага познаване на принадлежността на респондента (източника на информация) към съответната организационна структура, без да е известна неговата самоличност. Вторият принцип въвежда „добрата практика" за външно оценяване, която се реализира чрез събиране на информация от външни за институцията лица (временно съпричастни). Третият е пряко свързан с характера на информацията, придобита от социологическото проучване, която в социологическото проучване е възприета като „първична", докато за процеса по извличане на поуки от практиката може да се третира като „първична" (индицираща) и „вторична" (допълваща), тъй като е част от по-обширен процес на информационно-аналитично обезпечаване.

[1] Метаданните са данни за пол, възраст, местоживеене и организационна принадлежност на респондентите за социологическото проучване и данни за час, място, лице, терен на формулиране на наблюдение

По отношение на методите за провеждане на социологическо изследване, от съществена важност е годността на въпросите от анкетната карта на социологическото проучване, за целите на формулиране на наблюдения. Тя се наблюдава по отношение на следните параметри:

• Адекватност – подходящо формулиране на въпросите;

• Пълнота - широта и изчерпателност при формулиране на въпросите;

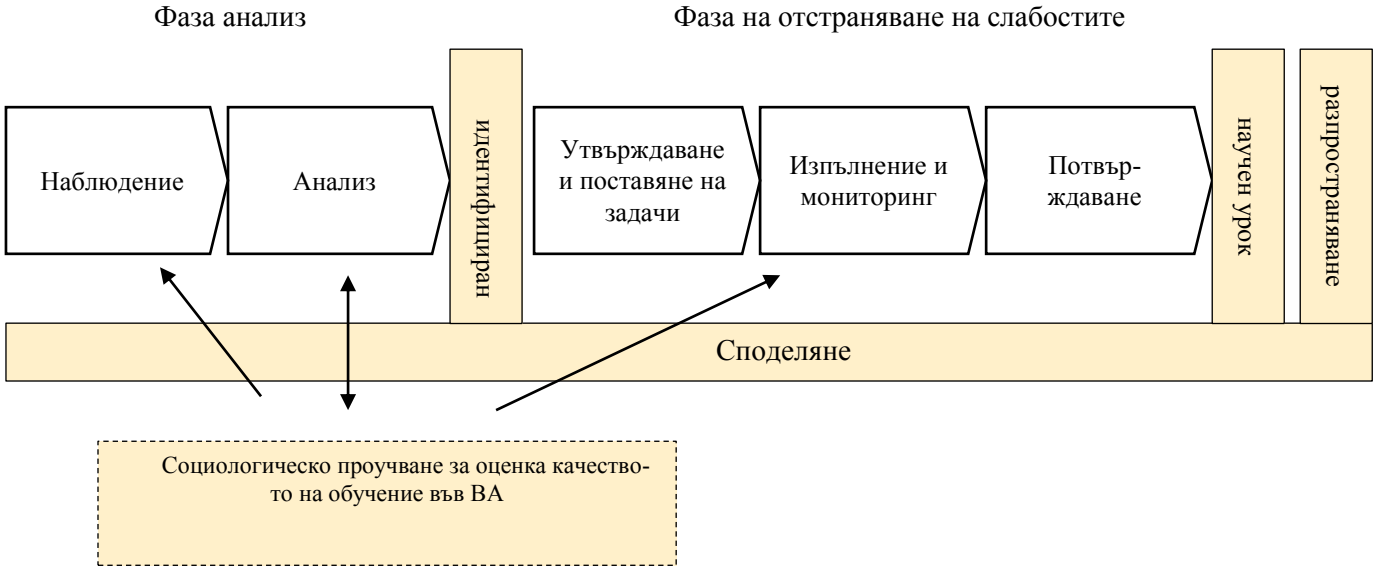
• Обективност – анкетната карта е анонимна и презентирана като инструмент за коригиране на процеса на обучение, което предполага висока степен на обективност;

• Системност – при формулиране на наблюдения на база на въпросниците в социологическото проучване и съхранението им в бази данни дава възможност за ревизиране на проблема от предходни години;

• Възможност за приоритизиране на проблема – при статистическо натрупване (многократно посочване на един и същи проблем от различни респонденти), той автоматично се очертава като приоритетен.

Съвместимостта на процесите покрива целия спектър от дейности и се реализира по отношение на целите, ограниченията, методите, вида обработвана информация и нейната годност за формулиране на наблюдения.

Възможността за постигане на синергия между процесите е свързано с използването на социологическо проучване за оценка качеството на обучение във ВА във фазите на процеса за поуки от практиката, показани на фигура 3.



Фигура 3: Свързаност на процесите

При подходящо формулирани въпроси на социологическо проучване за оценка качеството на обучение във ВА може да се идентифицират наблюдения за процеса на поуки от практиката.

Резултатите от социологическо проучване за оценка качеството на обучение могат да се използват като допълнителна информация за вече идентифицирано наблюдение и така да се добие по-пълна и непосредствена представа за възникналия въпрос.

Социологическо проучване може да даде обратна информация дали има резултат от взетите коригиращи мерки т.е. урока е научен.

Заключение

Въпреки наличната съвместимост между процесите на социологическо проучване за оценка качеството на обучение и извличане на поуки от практиката във ВА, към този момент, те се изпълняват самостоятелно и резултатите от тях се имплентират по отделно в управленския процес, при липсваща координация и взаимообвързаност. В резултат на това решенията свързани с единия процес са независими и необвързани с решенията от другия процес. Това се дължи на факта, че двете групи от решения са на базата на отделни анализи и изводи. Потенциално, дори е възможна ситуация при което едно управленско решение взето на база на анализ от първия процес да се окаже в противоречие с решение в резултат от втория процес, което е напълно недопустимо. Това е явен признак за липсата на синергия между двата процеса. Предложения в доклада подход съвместява различни процеси, което води до повишаване на ефективността в управлението на ВА.

Изводи

В резултат на проведеният аналитичен обзор на двата процеса, са направени следните изводи:

1. Към този момент процесите по извличане на поуки от практиката и провеждане на социологическо изследване във ВА, са два паралелно протичащи, независими един от друг и некоординирани помежду си процеса, насочени към подпомагане взимането на управленски решения.

2. Съвместяването на двата процеса ще доведе до синергия, която ще повиши ефективността на управленския процес, като повиши качеството на управленските решения в направленията пълнота и непротиворечивост.

3. Съвместяването на двата процеса следва естествената логика на субординация между тях и е възможна, посредством инструментализиране на социологическото проучване в рамките на процеса за учене от опита, за постигане на синергия и ефективност на управлението.

References

1. Грозданова, Т. & Георгиева, Т. (2021). Методическо ръководство за оценка качеството на обучение във Военна академия „Г. С. Раковски“. Печат Военна академия „Г. С. Раковски“. ISBN 978-619-7478-76-1.
2. Заповед на началника на ВА "Г.С. Раковски" № СИ29-РД02-336 /02.06.2021 г. за създаване на организация и провеждане проучване на мнението на слушателите и студентите от „Випуск 2021“ за качеството на обучението във ВА "Георги Стойков Раковски".
3. Лазаров А., Христов Н., Радулов И., Андреева П. (2008), “Операционен анализ. Ръководство за провеждане”, печатна база на Генералния щаб на Българската армия, гр. София
4. Марков, З. & Георгиева, Т. (2014). Методика за оценяване на обучението във Военна академия „Г. С. Раковски“. Печат Военна академия „Г. С. Раковски“. ISBN 978-954-9348-56-9.
5. Правилник за учебната дейност на Военна академия „Г. С. Раковски”, (2021)
6. Радулов И. (2019), "Прилагане на архитектурния подход в публичната организация", гр. София, издателство ДиоМира, ISBN 978-954-2977-57
7. Ръководство за поуки от практиката във Въоръжените сили, (2020)
8. Указания за организиране на процеса на извличане на поуки от практиката и прилагането им във Военна академия „Г. С. Раковски“, (2020)
9. Joint Analysis Handbook, (2016),

https://www.jallc.nato.int/application/files/9416/0261/6056/Joint_Analysis_Handbook_4th_edition.pdf

10. The NATO Lessons Learned Handbook, (2022), https://www.jallc.nato.int/download_file/view/1616/872

FEATURES OF LANGUAGE IN PROFESSIONAL MILITARY COMMUNICATION

Valya Simeonova

valiasimeonova_sweet@abv.bg

ОСОБЕНОСТИ НА ЕЗИКА ПРИ ПРОФЕСИОНАЛНАТА ВОЕННА КОМУНИКАЦИЯ

Валя М. Симеонова

***Abstract**: The report examines the importance and peculiarities of language and professional military communication. Language as a system of sound signs is a means of communication between people. Professional military communication is a phenomenon that is of great importance for the development of employees, as well as for the transmission and reception of specific service information between them.*

***Keywords**: language, professional military communication, officers, military organization.*

Езикът се възприема като система, чиято структура подлежи на моделиране в зависимост от възприетите принципи и норми на провежданата комуникация. Езикът обслужва възприетите решения на поставената проблематика пред комуникацията. [2]

Езикът придобива смисъл на въздействаща форма върху изработването на начина на мислене. Приема се следното определение за език: Езикът като система от членоразделни звукови знаци представлява средство за общуване между хората. Тази система, развиваща се в рамките на обществото, е социално средство за съхранение и предаване на информация, като се реализира и съществува в речта.

Тук може да се допълни, че езикът се развива и в рамките на военната организация като средство за съхранение и предаване на специфични военни термини и информация, като се реализира и съществува чрез професионалната военна комуникация.

Професионалната комуникация е раздел с изключително голямо значение за работния процес. Тя се изгражда и формира като гранична област между поведение, комуникация, етика. Професионалната комуникация е социален феномен с решаваща роля за развитието на човешката индивидуалност във военната организация.

Комуникацията във военната област е вид социално общуване. Тя е основен механизъм за организиране и осъществяване на дейности във военната организация. По своята същност тя може да се определи като преднамерена, съзнателно проектирана и осъществявана дейност, като активно взаимодействие и многостранен процес. Чрез комуникацията се реализира предаването на опит и знания, на определени норми на отношение и поведение на личността в съответствие със социокултурни модели. Тази комуникация е вторична спрямо всекидневната комуникация, има официален статус, отличава се със своята целенасоченост, преднамереност, системност и регламентираност.

Особеностите на езика при професионалната военна комуникация могат да бъдат разгледани в няколко аспекта:

- Избор на езикова норма, като основната цел е постигане на адекватност и яснота на изказа.

- Избор на изразни форми на тялото, като тук основната цел е езикът на жестовете да бъде в комуникационен синхрон с общия контекст на езика (ръкуване, отдаване на чест да са в синхрон с думите за поздрав, изричане на имена и военни звания).

- Използване на специфични военни термини, чиято основна цел е да предразполагат към правилно възприемане на лансираните идеи и тези.

- Формиране и моделиране на изказни форми, които да бъдат съобразени с възприетите цели, стратегии и политики във военната организация, с нагласите на военнослужещите.

Професионалната военна комуникация се реализира чрез разнообразни форми и на различни равнища - в процеса на работа между ръководители и подчинени, между равнопоставени. Тя има характеристика на професионална комуникация и като такава предполага професионално поведение от страна на военнослужещите и цивилните служители, участници в комуникационния процес. В социалната му детерминираност намират отражение специфичните задължения и задачи на комуникиращите субекти. Тази обвързаност със специфичните задачи придава професионалния профил на поведение при комуникацията и изискването да се спазват етични и строго професионални стандарти при изграждане на взаимоотношения.

Като система от знаци езикът въздейства пряко върху предаваното и приеманото съобщение, разглеждано в контекста на комуникационния процес. Сами по себе си езиковите знаци не могат да привнесат смисъл. Необходимо е те да се разбират по един и същи начин както от изпращача на посланието, така и то получателя му. Необходимо е наличие на установени по споразумения правила за кодиране и декодиране на значението. Тези правила могат да бъдат установени по закон или традиция, или по силата на обстоятелствата за даден конкретен случай. След като знакът се подчини на установените правила на значението, той реално става носител на смисъла на съобщението - инструкции, заповеди, доклади, стратегии, политики. Налице е вече състояние на комуникация.

Характеристиките на самото споразумение за установяването на правила за кодиране и декодиране се формират на базата на спецификата на конкретно използваните комуникационни начини и форми на професионалната военна комуникация. Това означава, че езиковият код се подчинява на виждането за бъдещата материализация на самата комуникация. Липсата на адекватност между езиковия код и предпочетената съвместимост на комуникационните начини и форми би означавало, че липсва възможност за възпроизвеждане на комуникационен процес.

Като знакова система езикът може да се наблюдава в два аспекта по отношение на смисъла му като изразно средство. Първият аспект може да се определи като вербален език, а вторият аспект като невербален - език на жестовете и символите. И при двата аспекта основен и водещ е принципът за изграждане и интерпретация на бъдещи събития или на съществуващи в реалността факти. Като приема този принцип за верен, професионалната военна комуникация използва възможностите на посочените два аспекта на знаковата система на езика, за да изгради същинската комуникационна форма.

Важен момент при осъществяването на професионалната военна комуникация е символното интерпретиране на връзката език-мислене-нагласи. Тук става въпрос за възможностите на езика да изразява адекватно мисълта. Фактът на адекватното изразяване съответно води до формиране на нагласи във военната организация или на отделните служители - военнослужещи и цивилни служители. Реалното осъществяване на връзката език-мислене-нагласи винаги води до изменение на нагласите и конкретно формиране на поведенчески модели. Това изменение се корени преди всичко в стремежа да се защитят ценностите и интересите на отделните служители в организацията. Тук става въпрос за достъп на служителите до организирани езикови курсове, курсове за повишаване на квалификация и за военнослужещи и за цивилни служители, също така и за кариерното развитие на военнослужещите.

За професионалната военна комуникация езикът има особено важно значение по отношение на създаването на доверие. То няма друга среда, в която би могло да възникне, да се развие и да се утвърди, освен в условията и нормите на общуването. Езикът играе ролята на ключ, чрез който процесът на комуникация става реално възможен. Посочената връзка език-доверие се отнася най-

вече за установяване на необходимата степен на сътрудничество в рамките на военната организация. Според О Хара [1] важна функция на доверието е да подпомага сътрудничеството между хората. Тя свързва индивидуалното и колективното. В някои случаи поведението на отделните служители води до сътрудничество и положителни резултати за институцията като цяло. Участниците виждат, че в дългосрочен план ще извлекат полза от сътрудничеството, така че до известна степен теорията може да помири индивидуалното и колективното.

Във връзка със значението на езика по отношение на комуникационния процес е лингвистичния аспект, отнасящ се до скоростта и яснотата на думите. Факторите, които влияят върху скоростта на думите са следните:

- Намиране на баланс между думите и идеята;
- Необходимост от време за съставяне на комуникационно информационна конструкция, така че тя да е адекватна спрямо кодирането и декодирането;
- Време, необходимо да се материализират думите - чрез речта, чрез средствата за комуникация и медиите.

Яснотата на думите е в пряка връзка и зависимост с тяхната скорост. Елиминирането на повърхностните като мислене аналогии и се акцентира върху разликите като се оцени обективно разнообразието, означава яснота на думите, а от тук и яснота на мисълта.

Военното общуване е човешко общуване, което от една страна поражда бариери, които са резултат от влиянието на субективното отношение на общуващите. От друга страна, тези бариери могат да бъдат преодолени точно с различните възможности на индивида да интерпретира ситуацията и да постъпва по подходящ начин. От военнослужещите зависи да изберат най-подходящите за тяхното взаимодействие стратегии, да използват най-адекватните средства за общуване и да определят границите на военното, деловото и неформалното общуване помежду си, водени от общата си цел, взаимна удовлетвореност, двупосочно влияние и развитие.

Същността на професионалната военна комуникация се изразява в:

- обмен на знания и умения между взаимодействащите си субекти;
- взаимно възприемане, разбиране на участниците в комуникационния процес, в резултат на което се постига или не се постига сътрудничество помежду им;
- организация на управлението на специфичната работа;
- регулиране и координиране на междуличностните взаимоотношения между субектите в процеса.

Ефективното военно общуване предлага осмислен баланс между професионалното общуване като въплъщение на военните цели и съдържание и между общуването на личностно ниво - като проекция на индивидуалните връзки и отношения на близост, доверие.

Особеностите на професионалното военно общуване в голяма степен зависи от редица фактори: съвместна дейност, изградени знания и умения, обща стратегия на поведение при взаимодействието.

В заключение може да се посочи, че езиковите знаци сами по себе си не могат да привнесат смисъл, необходимо е те да се разбират по един и същи начин както от изпращача на посланието, така и от получателя му. Езикът се развива в рамките на военната организация като средство за съхранение и предаване на специфични военни термини и информация, като се реализира и съществува чрез професионалната военна комуникация.

References

1. **О Хара**, К. (2004). Доверието. Новата криза на обществото. София: Кръгозор.
2. **Палашев**, Н. (2007). Да създаваш реалности. София: За буквите - О писменехъ.

THE EFFECT OF STRESS ON MENTAL FUNCTIONING IN VOLUNTEERS AND NAVAL SPECIALISTS

Elena Anzova

Higher Naval School "N. Y. Vaptsarov" – Varna, MU – Plovdiv, Bulgaria, e-mail: elenaanzova@gmail.com

Abstract: Stress and its effects are very present in the work and daily life of maritime professionals and volunteers.

Stress can be seen as a process rather than an outcome.

It occurs under the influence of stimuli that cause a state of anxiety.

Coping represents the model of self-regulation, the effectiveness or ineffectiveness of which is related to the way of understanding and experiencing situations, experienced emotions and satisfaction. This makes it interesting to follow the links with mental well-being and its components.

Keywords: *Biofeedback, Audio-visual entrainment of brain waves (AVE), physical and mental health, stress, anxiety, level of resilience, marine volunteers*

In modern scientific literature, the term "**stress"** has at most three meanings.

First, conceptually, "stress" can be seen as any external stimuli or events that cause tension or excitement in a person. For this reason, the terms "stressor", "stressor" are often used.

Second, stress can refer to a subjective response, and in this sense it reflects an internal mental state of tension and arousal, meaning emotion, defensive reaction, and *coping processes*. Such processes can contribute to the development and improvement of functional systems, and also cause mental tension [2, 3].

Third, stress can be a physical reaction of the body to certain demands or harmful effects.

Looking at different variants of stress, N.H. Rizvi notes:

- Sometimes "stress" refers to a state of anxiety in the body that it seeks to remove or reduce. In this sense, the concept of stress is little different from such unpleasant conditions as anxiety, mild pain and dissonance.

- Stress is also seen as psychological and behavioral reactions that reflect a state of inner anxiety or its suppression. Such protective reactions are observed in various functional manifestations: emotional, cognitive and behavioral.

- Stress is defined as an event in a physical or social environment that leads to taking measures against a threat [2, 3].

In the scientific article, we will present some psychological test methods from clinical practice, which can be successfully applied and used in the study of psychological functioning, coping strategies in volunteer marine specialists.

This makes it possible to evaluate the impact of personal characteristics and subjective perception, the influence of the environment on the level of stress and the coping strategies developed.

DATA COLLECTION METHODS - TOOLKIT

QUESTIONNAIRE TO DETERMINE CURRENT PHYSICAL AND MENTAL CONDITION

Test and apparatus methods from clinical practice, which can be successfully applied to study the level of stress and improve the psychological functioning of these specialists:

1. Affective state rating scale
2. Von Zerssen self-esteem scale
3. Questionnaire for studying the adaptation of the individual to the environment
4. Questionnaire for assessment of long-term motivation and individual behavior
5. Questionnaire for assessing localization of control
6. Apparatus research with the Biofeedback system using the apparatus methodology "Mind reflection GSR"
7. Audio-visual entrainment of brain waves (AVU).

Biofeedback and Audio-Visual Entrainment of Brain Waves (ABU) apparatus methods are the most modern and newest apparatuses that provide extremely many opportunities in the field of research aimed at the development of self-knowledge, self-control and stress management.

An advantage is that with the apparatus methodology Mind reflection, it is possible to determine which stressors have the greatest impact on these specialists - noise, emotions, decisions under stress or cognitive load, stressors that these specialists face every day in their work [1].

Audio-visual entrainment of brain waves (ABU) is an effective method for reducing various mental and emotional states.

Its working principle is based on stimulation of the central nervous system with light and sound signals.

The accumulation of a database, through this type of methodology, will allow to establish both the leading stressors and their power of impact on the personality, as well as the level of self-awareness and their influence on the skills to quickly recover from the negative consequences of the experienced stress.

References

1. Beauchamp, M., Harvey. R, Beauchamp. P. (2012), An integrated Biofeedback and Psychological Skills Training Program for Canada Olympics short – track Speed skating Team. Journal; of Clinical Sport Psychology, 6, pp.68-84

2. Lazarus Richard, S. (1999), Stress and Emotion. Free Association Books, London

3. Selye, H. (1979), Stress without stress, Progress

4. Schultz, D. (2004), Growth Psychology - Models of the Healthy Personality. Sofia, Science and Art.

VIROLENCE AND MEMETIC POTENTIAL OF "CHEMICAL, ETHNIC AND BIOLOGICAL WEAPONS" IN INFORMATION WARFARE

Victor Dobrev

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

***Abstract**: This article discusses the memetic suggestive impact potential of narrative and visual forms of representation of "chemical, biological, and ethnic weapons" used in modern information warfare. Some of the results of modern research conducted in the field of biological weapons are indicated, as well as the possible perspective of creating such types of weapons as genetic and ethnic weapons and the reliability of the information related to them.*

***Key words** information warfare, genetic weapons, ethnic weapons, biological weapons.*

ВИРОЛЕНТНОСТ И МЕМЕТИЧЕСКИ ПОТЕНЦИАЛ НА „ХИМИЧНИ, ЕТНИЧЕСКИТЕ И БИОЛОГИЧНИ ОРЪЖИЯ“ В ИНФОРМАЦИОННАТА ВОЙНА

Виктор Добрев

Генетиката е една от най-старите науки и най-яркия и дебют е селекцията, чиито резултати се използват и до ден днешен. Съответно методите и не намират приложение само при растения и животни, а нескрито поглеждат и към човека. Кастовата система в Индия от дълбока древност е грандиозен генетичен експеримент. В древна Спарта слабите и недъгавите деца просто са били убивани.методи на основата на селекцията са прилагани и в древен Рим от чистият брутален геноцид с пълно изтребление на цели народи до толерирането и привличането на занаятчии в Рим и получаването на статус на римски граждани.

В по-ново време създаването на генетични и химически оръжия като начало са направени от съветския генетик А. Серебровский използвани срещу селскостопански вредители. Факт също така, че най-мощната военно химическа индустрия се появява в Съветския съюз след края на Първата световна война и до ден днешен не е загубила своите мащаби и потенциал.

На съвременния етап в областта на идентификацията на отличителни гени се водят изследвания на много места по света – идентифицирани са 50 човешки етноса с различни генетични маркери.

Какво в същност представлява генетичното оръжия?

Предназначението ми е избирателно да порази население по расов, полов или възрастов показател или други човешки характеристики. Действието му е насочено към избирателно поразяване от изкуствено създадени патогенни организми на строго определена част от населението

като във военен контекст могат да бъде мъжката популация на дадена нация. Патогенното въздействие е така моделирано, че от една страна да не дава поражение върху другите членове на етноса, а то друга всички лекарства известни до този момент да са неефективни. Такова въздействие се формира на анализ на ДНК съдържащо генетичен код и неравномерното разпределение на белтъците при различните националности определящи техния външен вид, поведение, продължителност на живота и редица други характеристики. На тези принципи работи и клонирането което изначално е отречено от обществото и църквата.

В една от информациите на „Файнешъл Таймс" се казва, че ЮАР доста продължително време е разработвал бактерии които да предизвикват безплоди при чернокожите, но науката е доста скептично настроена към постигането на подобен резултат.

Развитието на молекулярната генетика през периода 1960-70 година даде възможност да се осъществи разделянето и рекомбинирането на гени,а от там образуването на нови молекули и рекомбинирано ДНК носещо различна информация. На тази основа се осъществи пренос на гени с помощта на микроорганизми и да се създадат силно токсини въздействащи на човека, животните или растенията. През 1970 е създаден първият изкуствен ген и тогава започва реалната работа по създаването на генетично оръжие. Първоначално във военните лаборатории са се стремили да постигнат 100% поразяваща способност на изкуствените щамове на африканските вируси на Марбург, Лас и Ебола превръщащи вътрешните органи на поразения в жале. Американските бойни щамове на талуремия са притежавали способността да устояват на антибиотици и да преодоляват имунната защита.

Още през 1970 г. са създадени вируси които да сработват спрямо определена възраст или пол с ефективност до 90%. Такива разработки има в СССР, САЩ, Китай и редица Западно Европейски държави. През 1980 започва проектът „Човешки геном" в последствие преминал в „Генома на живота".

През 1989 в САЩ започва да се разпространява японското лекарство L-трептофанна основата на изкуствено създадени бактерии. В лекарството по неизвестен начин попадат патогени преодоляващи имунната система и поразяващи десет хиляди човека. През октомври 2000 година също в САЩ избухва нов скандал свързан с продуктите в магазините съдържащи трансгенетична царевица „Стар Линк"разрешена само за храна за добитък. В самата царевица е добавен ген отговарящ за синтеза на пестицидите унищожаващи европейският царевичен червей, но представляващ мощен алерген за човека (не се преработва в организма и не се разрушава при термична обработка довеждайки до алергична реакция достигаща до анафеличен шок. Опасността от такива генно модифицирани хранителни продукти идва не само от възможни грешки, а и от недостатъчното изследване на механизма на действие на използваните гени върху човека.

Редица специалисти говорят вече за „геноцидна война" ориентирана към унищожаването на въоръжените сили военната техника и излишното население на потенциален противник. Според разчетите американският медик Р. Хамершлаг генетичните оръжия могат да нанесат 20-30% поражение върху населението на дадена страна – такива поражения не са „приемливи" дори при ядрена война и са показател за поражение на засегнатата страна. Предполага се, че на един следващ етап генното инженерство ще достигне нива, които ще позволяват производството на токсични продукти възможни за използване като оръжие. Това ще създаде съвсем нова концепция за „генетичните войни" за които главна цел ще е не унищожаването на въоръжените сили, а унищожаването на голяма част от населението считано за излишно от интервента имайки предвид спадащата производителност на Земята и възможността да изхранва населението. В това е и смисълът на т. нар. геноцидната война.

Възниква въпросът: До колко е възможна такава война? Повечето сериозни генетици отговарят на този въпрос отрицателно приемайки темата като спекулативно търсене на журналистите на сензации. Според завеждащия лабораторията за изследване на генома в Института по обща генетика на РАН Николай Яковлев, да се разпознае по генетични признаци националността на човека е възможно, но да се използват те за въздействие водещо до това да ви е добре или зле е

невъзможно.

Появяват се обаче и други мнения като на заместник директора на Института по молекулярна генетика при РАН Вячеслав Тарантул който не е толкова категоричен в прогнозата и заключенията си: "…Аз не виждам до днешен ден механизмите, които да позволяват по цвета на кожата и цвета на косата или очите да се създаде оръжие. Освен това ние трябва да имаме разбирането, че някакви различия в гените съществуват и това не изключва появата на такова оръжие. От морална гледна точка ние трябва да сме готови за това. В крайна сметка разпространението на такъв род оръжия практически е непроследимо и процесите не подлежат на контрол".

Такова оръжие с избирателно действие върху определена таргет група с генетични маркери е изключително опасно променяйки изцяло правилата на традиционната война – вирусът може да бъде разпространен през някаква храна и не изисква дори транспортиране. Нещо повече въздействието от прилагането му може да се отложи за по късен етап когато проследяването му става невъзможно. Примерно ако си представим, че „испанския грип" е такова генетично оръжие то за краткия период от 1918 до 1920 от него са загинали 20 милиона човека – повече от жертвите дадени през Първата световна война.[4]

Общо известен факт е, че естествения биологичен подбор като обща генетична реакция върху цялата популация се движи от един общовалиден принцип: само организмите които преди да загинат са имали успешно потомство – за историята отделния организъм няма значение. За всеки един политик или военен това е съществено важен момент. Известни са обаче и редица опити на някой държави да въведат форми на ефгенетичен подбор.

Американският журналист Том Хартман в статията си „ Генетично модифицираната бомба" по проекта „Нов американски век" със заглавие „Престрояване на отбраната на Америка: стратегии, сили и ресурси през новото столетие". В този доклад се фиксира тенденцията Америка да се ориентира към победи в нетрадиционния тип войни – с един противник може да се бориш в киберпространството, с друг под вода или в космоса, с трети в рамките на собствените им тела.

„ Най-високите постижения на биологичните войни която може да бъде „целева" (насочена към някакъв човешки генотип, превръща царството на терора в полезен инструмент"

Според други източници редица авторитетни ядрени центрове в Окридж, Брукхевен, Ливермор и др. отдавна работят в областта на секретните генетични изследвания финансирани от министерството на енергетиката на САЩ. При създаването на атомна та бомба по Манхатънския проект щателно са изучавани генетичните материали от бомбардировките над Япония. Според американските учени от 90% от изследванията в молекулярната биология и генетика във всеки един момент могат да бъдат пренасочени към създаването на генетични оръжия. . и сега са известни примери на експерименти по създаването на насекоми които могат да увреждат пътни настилки, самолетни писти на територията на противника, да разрушават метални конструкции, защитни покрития и смазочни материали на военната техника и оборудване. Група учени патентоваха микроорганизъм който разгражда **полиоретана** в боята използвана в корабостроенето и авиацията. Друга биотехнологична лаборатория разработи „антиматериален биокатализатор" разрушаващ горивата и пластмасите.

В СМИ се появиха съобщения, че група учени от Израел разглеждат възможността за водене на етническа война срещу палестинците като базово тези изследвания са копирани от опитите на Южноафриканската република по времето на Апартейда. Източници от Министерството на отбраната на САЩ потвърждават, страна подлежаща на отчет пред Пентагона) работи по създаването на патогени с етническа спецификация което веднага се интерпретира и насочва към Израел. Потвърждение за такава информация се превежда публикувания в списание Jane's специализирано в анализа на проблеми на отбраната и безопасността. В него се споменава, че южноафрикански източник потвърждава, че израелски учени използват южноафрикански изследвания в опита си да създадът „етнически куршум" срещу арабите. Говори се също, че израелтяните са открили аспект на арабския генетичен комплекс експериментирайки с „евреи от арабски произход, особено от Ирак". Подобна компилация от информация буди съмнение поради факта, че и

израелтяните и арабите са от един генетичен клон – симитския дифиренциацията между тях е изключително трудна ако не и невъзможна.

Подобна кампания преди започването на инвазията в Украйна в всички медии на Русия се поде вълна от информация за генетични лаборатории на Англия и САЩ разработващи генетично оръжие за унищожаване на руската популация на основа сходния славянски геном на украинците служещи като експериментална среда. Телевизия „РЕН-4" специализирана в сензационни, паранаучни и пропагандни предавания широко тиражираше подобна информация. Входа на самите бойни действия се излъчваха кадри от лаборатории в АЕЦ, които по никакъв начин не показваха някаква специална апаратура или техника говореща за биологични експерименти (естествено изнесени преди разкриването им). Истерията достигна своя връх когато в руската преса се появи информация за инпланти превръщащи украинските войници в зомби на бойното поле превръщайки ги в непобедими и безстрашни зверове. Нищо обаче в действителност не потвърждава подобна информация.

Подобна беше и стратегията спрямо химическите и бактеорогичните оръжия на Ирак, чийто единствен аргимент беше използването на химични газове срещу политически опониращи на режима на Садам Хюсеин.

Подобна кампания имаше и срещу Сирия и Башар Асад използвайки химически оръжия срещу опозиционни райони.

И в трите случая неизменно атакуваната с такава информация държава бива мигновено стигматизирана и маргинализирана в международен план с последваща пряка военна интервенция.

Не малка е интригата и с върлуващия КОВИД-19, за който се появиха информация за умишлена модификация на болестотворен вирус във военните лаборатории, но в случая информационната битка се разпръсна върху три супер сили като автори на разработката – Китай, Америка и Русия. В случая латентно се държи спусъка на поредната информационна бомба за стигматизиране на съответната държава.[6] [7]

Друга форма на информационна война е използването на вносните храни като форма на генетично оръжие. Русия се позовава на Бюлетина на изследователския център на болница Вилю от юни 1993, който констатира, че 22 добавки на внесените в Русия продукти съдържат психотропни вещества предизвикващи физиологични и психични изменения. Става въпрос за една генетична особеност на руснаците при употребата на алкохол. Според френския доклад тези 22 добавки помагат за забавеното разграждане на алкохола в кръвта, предизвикват неправилно усвояване на редица минерали и в крайна сметка сърдечно-съдови заболявания. Естествено използването на подобни вещества е целенасочено спрямо Русия без да се взема под внимание, че тези вещества се прилагат и в продуктите на Запад. В случая става въпрос за икономически вектор на информационно въздействие. Според руското Главно статистическо управление засегнати са хората на средна възраст от мъжки пол и това естествено влия върху отрицателния демографски прираст на страната и боеспособното население в нея. Фиксират се в чисто етнически план населението на областите Курска, Резанска, Владимировска и Смоленска. Пика на смъртността е между 1988 и 1996 г. когато САЩ и Англия оказват мащабна хуманитарна продоволствена помощ. Като пример се дава шоколада западно производство където в състава на 450 молекули има психотропни елементи предизвикващи зависимост.

Друг пример се дава с тонизиращата напитка „Екстази която се предвижда да бъде внасяна в Русия. Напитката се произвежда от южноамериканска секта от вид лиана наричана „шагуб" предизвикваща мистични видения и зависимост към този „наркотик за бедни". Тъй като тази билка не се отглежда в Русия , Беларус и Украйна то в организмите на хората няма ферменти които да я разграждат.

Преди много години подобна кампания се беше надигнала и срещу Кока Кола за наличието на растението кока в съставките 'и

И в двата случая се говори за бомба с забавено действие при което в „денят Х" е достатъчно

да се добави определен катализатор и заложената програма да сработи предизвиквайки разрушаване вътрешни органи изкуствени мутации на гени и промени в съзнанието.

Тук отново има премълчаване на някой съществени факти - за да е успешно едно генетично оръжие то трябва да порази минимум 25-30% от населението на противника. В Русия няма такова количество чисти руснаци и подобна етническа хранителна бомба е неефективна за 85% от населението.

Руските СМИ отчитат това като провал на Англия и Америка, които са пренасочели своето оръжие в сегашно време към Китай и сега там се наблюдават огромен брой онкологични заболявания.

Трябва да се има предвид, че самата Русия има като наследство огромен „архипелаг на военната химическа промишленост“ който според редица автори дълги години поради централизирана структура на управления дълги години е прикривала пораженията които е нанесла на собственото си население и екология. Разработените генетични оръжия са разработени включително с доброволни и недоброволни участници.[9]

От всичко казано до тук можем да направим заключението, че посочените МЕМ формации на „етнически, генетични, химически и биологични оръжия“ притежават уникален сугестивен потенциал влияещ върху съзнанието на хората предизвикващи масови психози и стигматизация на цели култури и народности. Тъй като и трите вида оръжия са изключително нападателни и по никакъв начин не се вписват в концепцията за „справедливата война“, поради агресивния си инвазивен потенциал моментално пренасят маркираната страна като подлежаща на интервенция Концедпцията на Джордан Питерсон за четирите архетипни образ на *чужденеца, епидемията, войната и природното бедствие,* предизвикващи задължително негативен емоционален отговор. В съзнанието сработва безотказно и ефективно в информационното пространство, предизвиквайки търсения ефект. [8]

References

1. Броуди, Р. Психични вируси. Екслибрис
2. Шейнов, В. П., Манипулирование сознанием, Минск: Харвест, 2010 г.
3. Митрев, Д „Информационни и психологически операции”, УИ „Епископ Константин Преславски“, Шумен, 2006 г.
4. Лукин, Е. В., Психологические основы информационной войны, центр стратегических оценок и прогнозов, http://csef.ru/ru/oborona-i-bezopasnost/265/psihologicheskie-osnovy-informaczionnoj-vojny-3725
5. Бобылов, Ю. А. Нетрадиционные войны будущего. Генетическое оружие на службе террористов//Независимое военное обозрение. - №7, 2004.
6. https//www/ufa kp. ru. М. Берн. Эксперты объяснили почему версия про коронавирус как генетическое оружие – миф, 30.01.2020.
7. https//news. rambler.ru/ М. Рождественская. Коронавирус: биооружие или проделки природы, 5. 02. 2020.
8. Питерсон, Д. Карта смисла. Архитектура верование. Питер. 2019
9. Федорова, Л. А. Советское биологическое оружие: История, екология, политика. М. МСоЭС. 2006
10. Федорова, Л. А. Химическое вооружение - война с собственным народом (трагический русский опит). М., Лесная страна. 2009.

ETHNICITIES, RELIGIONS AND INTERESTS INREGIONS OF PAZARDZIK AND PLOVDIV

Daniela D. Dimitrova

Military academy "Georgi S. Rakovski", Faculty " Command-staben", Department "Land forces"
didadoneva@abv.bg

ЕТНОСИ, РЕЛИГИИ И ИНТЕРЕСИ В ОБЛАСТИТЕ ПАЗАРДЖИК И ПЛОВДИВ

Даниела Д. Димитрова

Военна Академия „Георги Стойков Раковски", докторант къмкатедра „Сухопътни Войски", Факултет „Командно-щабен" *didadoneva@abv.bg*

Abstract: *In the regions of Pazardzhik and Plovdiv, there is diversity in terms of ethnicity and religion, which interact with each other. Each of the ethnic and religious communities have their own interests, defended based on their specific influences.*

The line between the turks and the roma in these areas is thin, due to an emerging group called the "millet" that floats between these two ethnic communities.

Keywords: *ethnicity; religion; roma; millet; turks; interaction;radicalization; Plovdiv; Pazardzhik*

Въведение

Изключително интересни са областите Пазарджики Пловдив, защото има разнообразие в етническо отношение, различни вероизповедания, които на този етап имат взаимодействие и взаимотърпимост. В същото време трябва да се посочи, че всяка от етническите и религиозни общности имат свои интереси, които по различен начин защитават на база своите специфични влияния.

Според статистиката на НСИ към 2001г. в България общо населението е7 928 901 души, от които българите са 6 655 210 души, турците са746 664 души и ромите 370 908 души. Необходимо е да се посочи, че сред експертите има сериозен спор за броя на ромското население в България. Така например френският учен Жан Пиер Лижоапосочва, че в нашата страна живеят 800 000 роми и, че на всеки 20г. техния брой се удвоява[1]. Някои наши учени в България считат, че в нашата страна живеят около 1 000 000 роми. Тази неточност се дължи на факта, че една част от ромите се самоопределят като българи на база доброто владеене на български език и християнска религия.

[1] „Роми, Цигани, Чергари", София 1996г.

Втората част от ромите се самоопределят често за турци и миллет на база своя диалектен турски език и това, че са последователи на мюсюлманската религия.

В религиозно отношение населението на България има следната статистика:

- Източноправославни- 6 552 751 души;
- Католици - 43 811 души;
- Протестанти – 42 308 души;
- Мюсюлмани – 966 978 души, от които 913 957 са сунитите, и 53 021 са шиитите в България;

Пазарджик и Пловдив са интересни области, защото в тях има разнообразие в етническо отношение население, както и хора които са последователи на различни религии.

В област Пазарджик живеят общо 310 723 души, от които българите са 261 260 души, турците са 20 448 и ромите – 23 970 души.

При тази статистика за област Пазарджик трябва да се посочи, че е много тънка границата между турците и ромите, защото има една група наричана „миллет", която е плаваща между тези етнически общности. Това е особено характерно за кв." Изток" – Пазарджик, град Пещера и град Септември и за част от Велинград.

В област Пловдив общото население е 715 816 души, от които 621 338 са българите, турците са 52 499 души и ромите са 30 196. Подобен проблем има и в област Пловдив, както в област Пазарджик – тънката граница между миллетскатаи турската общност. В град Пловдив е инай- големият етнически квартал - това е кв." Столипиново" - 60 000 души, където 95% се самоопределят за турци и 5% за роми.

В област Пловдив милетскатаобщност живее в Асеновград, Садово, Първомай, Стамболийски, Карлово и др. Ромската общност живеят в град Раковски, Брезово, Калояново и др.

По религиозен признак в област Пазарджик от общо 310 723 души, източноправославните са 250 556 души, католиците са 260, протестантите са 2 913 души и мюсюлманите са 46 338 души.

В област Пловдив при общо население 715 816 от, които източноправославни са 608 226, католици са 23 122 души, протестантите са 3 913 души и мюсюлманите са 62 595 души.

В много аспекти тези области – Пазарджик и Пловдив формират и нагласите в Южна България в етническо и религиозно отношение.

Уязвимостта в населените места в тези две области е това, че миллетската общност от ромското население ускорено се радикализира на базата на исляма.

Интересно е мнението на бившия синдикалист К. Тренчев:

„Дори в етнически план те са твърде вероятни. Искрата може да пламне единствено по някакъв етнически признак, а не по идеен, което е още по-страшно. Защото етнически веднъж започна ли се, няма спиране. Подобни пожари се гасят десетилетия. Когато една нация е изнервена от мизерия, е чиста случайност кой ще взриви бомбата. Войни са почвали от една сватба. Много притеснен съм и си давам сметка, че каквото и да правя, не мога да спра нещата."[2]

Защо Пазарджик се превърна в „ Столица на радикалния ислям?

Много често в различните изследвания се посочва, че радикализирането на ромската общност е тръгнало от кв."Изток", но почти никой от изследователите на радикалния ислям в Пазарджик не посочва причините, а именно защо този град стана база за възникването на радикалния ислям сред ромите?

За да възникне радикалният ислям сред ромите в кв. "Изток"- Пазарджик има сериозни причини и част от тях са следните:

[2]в."24 часа" от 22.12.2014г.

- През 1992г. в кв. „ Изток" – Пазарджик МВР – проведе наказателна акция срещу ромите под ръководството на директора на РДВР – Пазарджик, където са арестувани и пребити много хора;
- Стимулиране на слуха „Пазарджик става столица на циганите";
- Случаят със сестри "Белнейски"– В град Пазарджик бяха изнасилени и убити двете сестри Белнейски. По този период се започна една целенасочена кампания от политици и медиите да докажат, че убийци са „ неграмотни жестоки цигани". След три години се доказа, че убийците не са роми от кв. "Изток"- Пазарджик. Върху съзнанието на българите сериозен натиск оказаха и политически партии, които искаха да влязат в кв." Изток" – Пазарджик и да накажат „виновните", които са нямали нищо общо с убийството на момичетата.

Счита се, че причините за възникването на радикалния ислям сред ромите в кв." Изток"- Пазарджик, не се дължи толкова на религиозни възгледи, а на социални причини и оказване на натиск върху тях.

Радикализация в кв." Столипиново „ – Пловдив

Важно е да се подчертае, че радикализацията на миллетската общност в гр. Пловдив се движи по различна линия – чрез джамията на Джумаята, търговията с Турция, както и дейността на 11 мечити в кв." Столипиново".

Необходимо е да се отбележи, че ако радикализацията в град Пазарджик се извършва чрез религиозна идеология на база страха от външния враг, то в град Пловдив, радикализацията се извършва на база целенасочените интереси.

Трябва да се посочи, че в кв. "Столипиново" – Пловдив тази радикализация става чрез търговия с Турция.В кв. "Хаджъ Хасан Махала"- Пловдив тази радикализация става чрез Саудитска Арабия.

Причини за радикализацията в България

Радикализацията на исляма е сериозен проблем не само за България, но и за Европа, защото основните моменти на исляма се подменят с други, които нямат никаква база в исляма. Ето и примери в този аспект сред ромското население:

След връщането си от война, в Хадисите, пророк Мохамед посочва, че са се върнали от малък джихад – войната за религията и предстои големия джихад – вътре в човека борбата между добро и зло[3]. Съвременните ислямисти обръщат нещата, така че да докажат, че големия джихад за мюсюлманите - е борбата за религията.

Основните моменти от исляма и ислямизма

Ислямът:	**Ислямизмът:**
-джихад на езика	-джихад на меча
-вяра в духа	-вяра в действия
-духовност	-действие
-молитви	-джихад
-писание	-меч
-джихад на доброто	-джихад за вярата

По този повод представителите на движението " Мюсюлманските братя" посочват следното:

[3]Хадисите за Мохамед, I, София, 2016г. с. 632

„Ислямът – това не е само дух, но и власт и изпълнение, това е учение и законодателство. Ислямът едновременно е и религия и средство за лекуване, духовност и действие, молитва и джихад, писание и меч. Тези елементи са неделими един от друг".

В заключение темата за „Етноси, религии и интереси в областите Пазарджик и Пловдив" е една много сложна тема, по която са необходими задълбочени изследвания и проучвания.

По повод на радикализацията в Южна България, Гюрсел Алиев, председател на турците в Пловдив посочва следното:

„Още преди години на всички органи е известно за навлизането на ислямския фундаментализъм и това, че традиционния ислям е заплашен. Арабските емисари идват у нас всеки месец, а милиони долари, с които арабските страни захранват България се разпределят от главното мюфтийство по мечитите за промиването на мозъци, на младите хора. Такива мечити в кв."Столипиново" има 7-8 и всички те са незабележими, тъй като не са регистрирани, според чл. 14 от Закона за вероизповеданието"[4]

References

1. Лижоа. Ж. П. „Роми, Цигани, Чергари" София 1996.
2. „Хадисите за Мохамед", том I, София, 2016.
3. Вестник „24 часа" от 22.12.2014.
4. Вестник „Марица" от 17.08.2000.

[4] в. Марицаот 17.08.2000 г.

GEODESY

ON THE CHOICE OF MAPPING PROJECTION IN GEOINFORMATION SYSTEMS

Petina A. Andreeva

Department Artillery and Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levsky" petiand@abv.bg

Abstract: *The choice of mapping projection is an important point in the process of geoinformation modeling. In modern conditions, specialized cartographic program packages are used in the application of geoinformation technologies. They contain multiple cartographic projections and the task of choosing a mapping projection is facilitated by reducing the selection of one of the lists. But this choice should not be random but should be based on criteria that provide quality of the mapping image, small deformations, accuracy, reliability, etc.*

Key words: *Digital maps, map projection, UTM.*

ВЪРХУ ИЗБОРА НА КАРТОГРАФСКА ПРОЕКЦИЯ В ГЕОИНФОРМАЦИОННИТЕ СИСТЕМИ

Петина А. Андреева

1. Въведение

Избора на картографска проекция е важен момент в процеса на геоинформационното моделиране. В съвременни условия при прилагането на геоинформационните технологии се използват специализирани картографски програмни пакети. Те съдържат стотици картографски проекции и задачата за избора на картографска проекция се улеснява като се свежда до избора на една от списъка [1],[9].

2. Фактори при избора на картографска проекция

Факторите, които определят избора на картографската проекция се делят на три групи:

- *обект на картографиране;*
- *характеристика на картографското изображение;*
- *характеристика на проекцията*.

Обект на картографиране включва:

- Категория на обекта на картографиране (планета, спътник и др.);
- Отделни обекти (регион, континент, държава, област и др);
- Особености на обекта (местоположение, размери, топология и др.)

Характеристика на картографското изображение включва:

- Съдържание на картографското изображение (общогеографско, тематично, специално и др.);
- Тематика и специализация (геофизическа, гравитационна, геодезическа и др.);
- Особености (област на приложение, ползватели, способи за използване, мащаб и др.).

Характеристика на проекцията включва:

- Деформации в проекцията (характер и големина на деформацията, разпределението на локалните и регионални деформации и др.) [2];
- Специфика на изобразяването на характерни обекти (полюси, екватор, осев меридиан и др.);
- Особености (вид на картографската мрежа, условията на нейната симетрия и ортогоналност и др.).

Избора на проекцията е на базата на отчитането на всичките фактори, но се допускат разумни компромиси.

Факторите от *първата група* са безусловни и не подлежат на изменение. Категорията на обекта преди всичко определя какви проекции трябва да се използват за изобразяване на реалната повърхност – сфера, ротационен елипсоид, триосен елипсоид и др. Определят се и параметрите на геодезическата основа. Местоположението на обекта е от съществено значение и дава информация дали е на полюса, екватора, средни широчини и др. Необходима е информация за размера на обекта и неговата форма – овална, разтегната по посока на полюса, по направление на меридиана или паралела, под определен азимут и др.

Втората група фактори е тясно свързана с решаването на поставените задачи и също не бива да се пренебрегват. Към общо географските карти се отнасят:

- едро мащабни топографски карти в мащаб от 1:2000 до 1:100000;
- обзорно - топографските – мащаб от 1:200000 до 1:1000000;
- обзорни – над 1:1000000.
- Специалните карти - за решаване на конкретни задачи и са за определени ползватели. Обикновено за тези карти картографските проекции са емпирично подбрани (кадастрални карти)[4, 6, 7].
- Тематичните карти е най разнообразната категория карти. Съдържанието и картографската проекция дефинира конкретна тематика и специализация, която е предназначена за определени ползватели [8].

Факторите от *третата група* в която може да се коригират, прибавят и разпределят тежестите за подбора на проекцията. Често подбора на проекцията е на база традиции, нормативни документи и предшестващи работи. Така например в България до 2005 г се използваше проекцията на Гаус-Крюгер, а след това UTM за изработване на топографски карти.

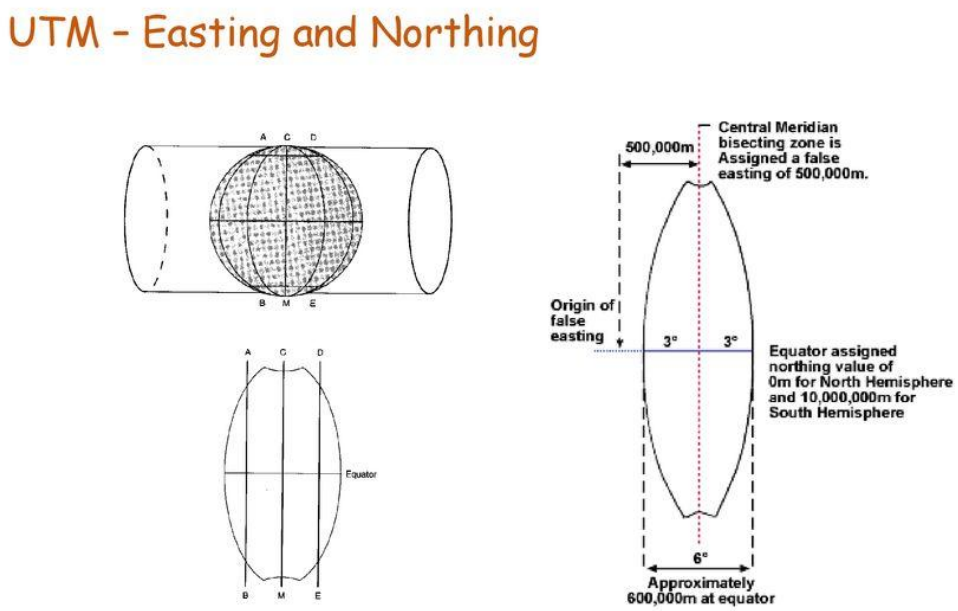
Равноъгълната напречно-цилиндрична проекция UTM (*Universal Transversal Mercator*) е проекция на елипсоида със секущ цилиндър. Проекцията е разработена през 1936 г от Международния съюз по геодезия и геофизика и е приета от много национални и международни картографски организации.

В тази проекция, както при Гаус-Крюгеровата проекция също се прилагат шест градусови зони, но зоните тук са ограничени на север до паралел с широчина 84^0, а на юг до 80^0. За картографиране на тези полярни области се използва равноъгълната азимутална (стериографска) проекция.

Частният линеен мащаб по осевия меридиан е m_0=0.9996. За това в проекцията се образуват две линии на нулеви деформации, успоредни на осевия меридиан на разстояние около 180 км от двете му страни. На границата на зоните частния линеен мащаб е 1.0003.

Земният елипсоид се дели на 60 шест градусни зони, които се номерират от 1 до 60, като се започва от меридиана със западна дължина 180^0. Територията на РБългария попада в 34N и 35N зони. Осевите меридиани са съответно 21^0 и 27^0.

В пределите на всяка шест градусна зона се прилитат две системи правоъгълни координати, в които положителните направления на осите *N(x)* и *E(y)* са насочени на север и на изток.



Фиг. 1. Универсална трансверзална Меркаторова проекция

За да се изключат отрицателните значения на *E'* във въведената за всяка зона правоъгълна координатна система, оста *N* се измества успоредно на запад на 500 км:

Координатите в UTM проекция се отнасят за елипсоид WGS84.

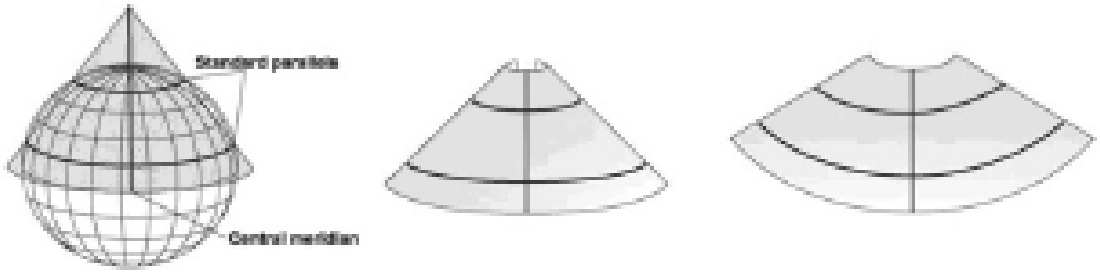
Съгласно ЗАКОН ЗА ГЕОДЕЗИЯТА И КАРТОГРАФИЯТА (Обн. ДВ. бр.29 от 7 Април 2006г., изм. ДВ. бр.57 от 13 Юли 2007г., изм. ДВ. бр.109 от 20 Декември 2007г., изм. ДВ. бр.36 от 4 Април 2008г.) [2] [5]:

Чл. 12. (1) Геодезическата система за територията на Република България, наричана по-нататък "Българска геодезическа система", се определя на основата на европейската геодезическа референтна система. Българската геодезическа система включва:

1. фундаментални геодезически параметри;
2. геодезическа координатна система;
3. височинна система;
4. система от равнинни координати, основана на приетите геодезическа координатна система и картографска проекция, която се използва за граждански приложения;
5. система за разграфка и номенклатура на картните листове.

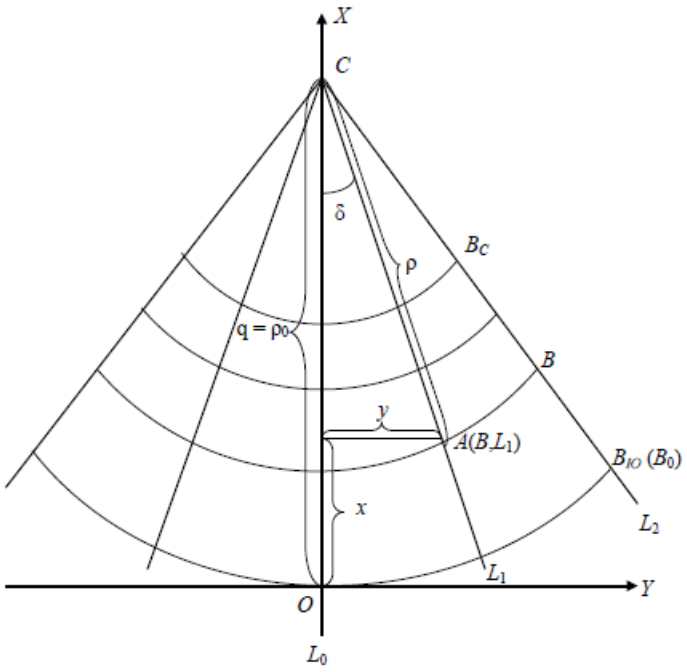
Основен недостатък на БГС2005 (UTM) е наличието на две зони и две координатни системи на територията на РБългария, както и наличието на сериозни деформации в границите на зоните, което се прояви в сериозни площни деформации. Това предизвика сериозни административни, юридически и граждански проблеми.

За да се отстранят недостатъците на БГС2005 по отношение на приложимостта й за кадастрални цели беше въведена модифицираната БГС2005 Кадастрална, като за основа отново се използва предложената в БГС2000 Ламбертова проекция (проф. Вълев) с два стандартни паралела. В БГС2000 стандартните паралели са изчислени с точност до секунда, а в БГС2005 Кадастрална са закръглени. Налице е една единна за цялата територия на РБългария координатна система. Централен меридиан $25^0$30', централен паралел 42.66787568333332, южен стандартен паралел 42^0, северен стандартен паралел 43.20'.



Фиг. 2. Секуща конична проекция

Секущите конични проекции образуват два стандартни паралела. Тази проекция има по малка деформация спрямо допирателната.



Фиг. 3. Координатна система в нормалната конична проекция

За малки територии избора на проекция не е от съществено значение но за глобални територии отговорността е съществена.

3. Заключение

Подборът на подходяща картографска проекция и геодезическа координатна система е важен проблем при моделирането в среда ГИС. В съвременните геоинформационни системи и платформи се предлагат различни картографски проекции които се използват в целия свят. За територията на РБългария основно се използва БГС2005 UTM (34 и 35 зона) и БГС2005 Кадастрална, но понякога се използват система 1970 г (Ламбертова конична система с 4 зони) и Гаус-Крюгерова цилиндрична проекция.

References

1. Андреев, А. И., А. Ст. Ангелов. Автоматизирани картографски системи. ВТС, Шумен, 1993.
2. Беджева М., Т. Игнатова, Analysis -f the accuracy of geodetically maps prepared by the means -f UAVs, Proceedings -f university -f Ruse – 2019, volume 58 (на български), ISSN 2603-4123 (-n-line)
3. Закон за геодезията и картографията, изм. ДВ бр.14 0т 20.02. 2015 г
4. Иванова, Ил. Отново за специализираните карти. София. “Геодезия, картография, земеустройство”,кн.3-4. 2005.
5. Наредба №2 от 30.07.2010 г. за дефиниране, реализация и поддържане на БГС 2005
6. Прокопов Я. Възможности на наземното лазерно сканиране – основа за геодезическо моделиране. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2021, Faculty of Artillery, Air Defense and Communication and Information Systems.
7. Прокопов Я. Сателитната радарна интерферометрия като алтернатива за някои задачи от приложната геодезия. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2021, Faculty of Artillery, Air Defense and Communication and Information Systems.
8. Тикунов В.С. Моделирование в картографии: Учеб. М.: Изд-во МГУ, 1997.
9. Serving Maps -n the Internet. ISBN 1–879102-52-8. ESRI Press. 380 New Y-rk Street, Redlands, Calif-rnia 92373-810. WWW.esri.c-m/gisst-r.

ON THE ASSESSMENT OF GEODATA QUALITY AND THE CONTROL OF ERRORS IN THE DATABASE

Petina A. Andreeva

Department Artillery and Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levsky" petiand@abv.bg

Abstract: *It is very important to assess the quality of geodata in geoinformation systems and to establish the presence of errors in the geodata database. For this purpose, methods that are applied geodetic, cartographic, photogrammetric and other types of measurements are used in the extraction of geodata. In addition, different standards apply. Errors can be presented by a matrix that classifies them.*

Key words: *GIS, geodata, database*

ВЪРХУ ОЦЕНКАТА НА КАЧЕСТВО НА ГЕОДАННИТЕ И КОНТРОЛА НА ГРЕШКИТЕ В БАЗАТА ДАННИ

д-р инж. Петина А. Андреева

1. Въведение

Много важно е качеството на геоданните, тяхната точност и оценката на грешките при създаването на базата данни (БД).

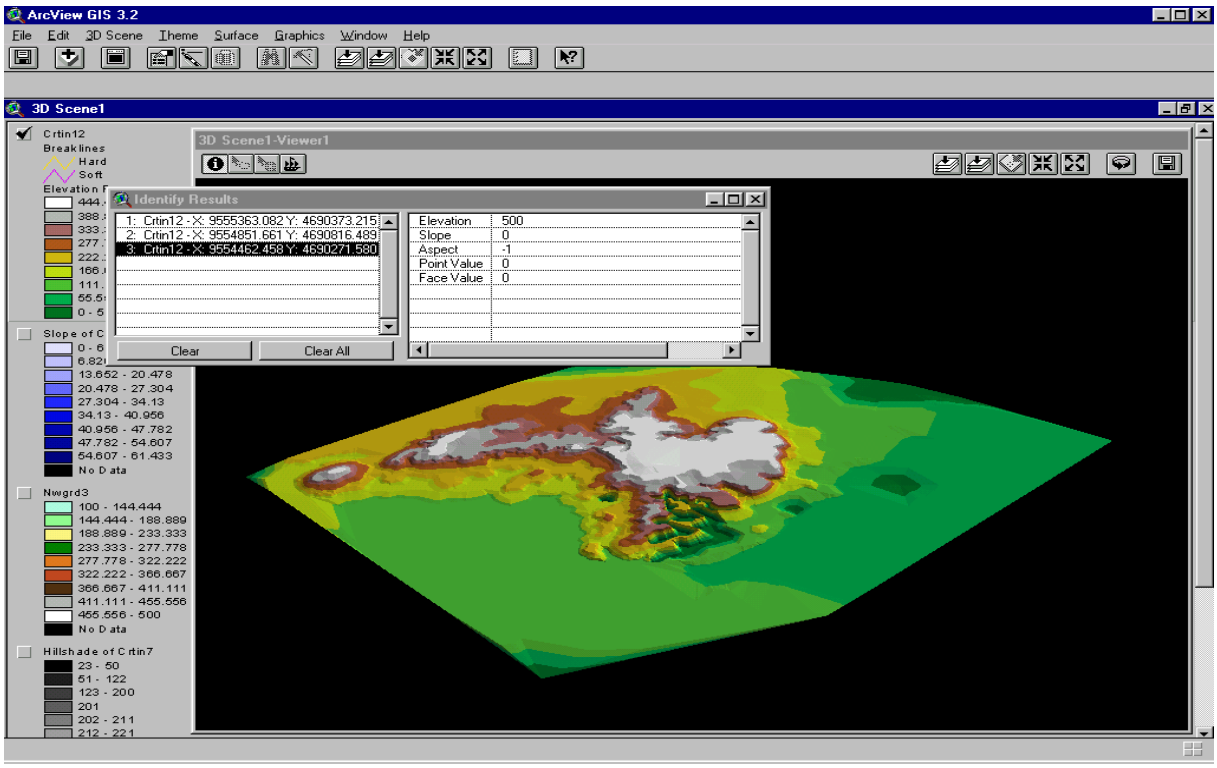
Методите за определяне на точността на геоданните са добре разгледани в геодезическата литература. Показателите за качеството на геоданните се дефинират чрез стандарти. Основните показатели за качество на данните са: *позиционна точност, точност на атрибутите на обектите, логическа непротиворечивостта, пълнотата, произход* и др.

2. Показатели за точност на геоданните

А). Позиционната точност се определя като разлика между измерените данни и тяхното истинско значение. При нейното определяне се отчита мащаба на изходния материал. Точността на координатите се определя, като разлика между растерното и векторното изображение.

Точността на растера зависи от размерите на пиксела. В повечето случаи е неясно дали координатите представени в растерен вид, са отнесени към центъра на пиксела или към един от ъглите на клетката. Във векторна форма координатите могат да се координират с желаната точност, но по принцип се фиксира положението на векторния обект. (фиг. 1) [1]

Б).Оценката на точност на базата данни е важен фактор при създаването и поддръжката на БД. При оцифряването на картите грешките им автоматично се пренасят в БД и при генерализацията на картите не винаги точно се фиксира местоположението на обектите и др. Ръчното въвеждане на цифрови данни винаги е съпроводено от субективни грешки. За снижаване на грешките от измерванията се използва геодезически контрол и глобални навигационни спътникови системи (ГНСС). При аерофотоснимките точността зависи от правилното подбиране на контролните точки.[3]



Фиг. 1. Дефиниране на позиционната точност на модела

На всички геоданни оказват влияние грешките при регистрацията и определянето на:

- контролните точки;
- грешки при трансформацията на координатите;
- грешки при обработката на данните;
- неправилен подход, генерализация и интерполация;
- математически грешки;
- загуба на точност при представянето на резултатите от изчисленията;
- преобразуване на векторни данни в растерен формат и др.

В. Точността на атрибутните данни се определя като близостта им до истинските показатели. В общия случай за оценка точността на атрибутите е полезно да се състави *матрица класифицираща грешките*.

За целта се вземат няколко случайни точки, определя се тяхната категория по БД, след това на местността се определя истинския клас и се попълва *матрица за класификация*.

Ако броя на класовете е 4 (A, B, C, D) и изследваните точки са 100. От тях на местността са определени: клас A – 25; клас B – 18; клас C – 24; клас D – 33.

Грешката на пропуска – възниква когато точките от класа на местността са неправилно фиксирани в БД.

В матрицата броя на грешните точките от клас B е равна на сумата от записите в стълбовете A, C и D на ред B (3+3+2=8) (броя на точките е 18 на местността, а в БД 10) .

Грешка на добавянето (лъжлив клас) – възниква когато в БД е фиксиран клас, който го няма на местността.

В клас A – това е сумата от записите на редове B, C и D за колона A (3+3+4=10) съответства на броя на точките, които са неправилно отнесени към клас A в БД.

Таблица 1

Клас на местността	Клас в БД				
	A	B	C	D	Всичко
A	12	7	3	3	25
B	3	10	3	2	18
C	3	5	15	1	24
D	4	4	4	21	33
Всичко	22	26	25	27	100

За обобщение на матрицата на съответствието се използва *показател на достоверност на класификацията* – количеството правилно класифицирани точки, разположени по диагонала на матрицата в %. Броят на тези точки може да бъде случаен и за да се отчете този факт се използва индекс к за внасяне на поправка за случайност:

$$\kappa = \frac{d-q}{N-q} \quad (1)$$

където d е брой на случаите с правилно получаване на резултатите (сума на значенията по диагонала); q е брой случайни резултати, изчислени чрез случайните резултати в стълб n_c и истинските – на ред n_r на матрицата на съответствието като:

$$q = \frac{n_c n_r}{N}; \quad (2)$$

N – общ брой на точките.

За абсолютно точни резултати (всички N точки са на диагонала) к=1, а при чисто случайно попадение к=0.

q=(22.25/100 +26.18/100+25.24/100+27.33/100)=25.09

q=(58-25)/(100-25)=0.44

Показателят за достоверност е равен на 44%, което е по-малко от полученото значение по диагонала 58%.

Г. Логическата непротиворечивост е свързана с вътрешната непротиворечивост на структурата на данните и топологическото им представяне. Тя е свързана с отговорите на въпросите:

- затворени ли са полигоните?
- има ли полигони без отбелязка?
- има ли възли на всяко пресичане на дъгите?

Логическата противоречивост може да се предизвика от проблеми в съгласуването на информацията за географските граници при съвместяване на данни от различни източници.[1]

Пълнотата е свързана със степента на обхвата на даденото множество от обекти, необходими за представяне на реалността. Тя зависи от правилата за подбор на обектите или явленията, генерализацията и мащаба.[2]

Произходът включва сведения за източника на данни, времето за събиране на данни, точността на източниците и цифровите данни, организацията която ги е събирала, операциите по

създаването на БД и др. Обикновено тази информация се съдържа в специален файл с метаданни. [5, 6]

3. Заключение

Оценката на качеството на геоданните в БД и минимизирането на грешките е от изключително значение за последващите процеси на моделирането и създаването на изходни материали. Ето защо е необходимо да се приложат подходящи методи за оценка, като например представените в доклада.

References

1. Андреев, А. Андреева П. Геоинформатика, геоинформационни системи, геоинформационни технологии. НВУ „В. Левски“ В. Търново 2021.
2. Андреев А. Марков М. Географски информационни системи. НВУ“В. Левски“ – Шумен, 2009 г 190 с.
3. Беджева Моника, Стефан Добрев, Експериментална оценка на точността на първичната фотограметрична информация, получена от БЛА, Pr-ceedings -f University -f Ruse - 2020, v-lume 59, ISSN 2603-4123 (-n-line)
4. Иванова, Ил. Кадастърът в България. Замисъл и изпълнение ISBN 978-619-90684-0-3 издателство "ACMO-Acadenic Press"
5. Прокопов Я. Възможности на наземното лазерно сканиране – основа за геодезическо моделиране. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2021, Faculty of Artillery, Air Defense and Communication and Information Systems.
6. Прокопов Я. Сателитната радарна интерферометрия като алтернатива за някои задачи от приложната геодезия. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2021, Faculty of Artillery, Air Defense and Communication and Information Systems.

SOURCES OF GEODATA ON GEOINFORMATION SYSTEMS

Petina A. Andreeva

Department Artillery and Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levsky" petiand@abv.bg

***Abstract**: GIS data sources are the basis of their information provision. The losses for information provision with geodata and geoinformation for the development of geoinformation projects is about 80% of the total cost. When analyzing and evaluating the different sources, account should be taken of spatial scope, scale, quality, presentation form (analogue or digital), period of data entry, actuality and renewal, digital transformation, accessibility, form of presentation in the necessary standards and their descriptive characteristics (metadata – data data), etc.*

***Key words**: GNSS, remote sensing, metadata, maps, database, GIS*

ИЗТОЧНИЦИТЕ НА ГЕОДАННИ ЗА ГЕОИНФОРМАЦИОННИТЕ СИСТЕМИ

д-р инж. Петина А. Андреева

1. Въведение

Изборът на източника на геоданни и геоинформация и технологията на събирането й е на базата на анализа на външната информационна среда и техническите средства с които се разполага. За критерии при този вид анализ се използват следните характеристики: [1]

- Надеждност и достъпност на източника;
- Необходимост и достоверност на предоставянето на информацията;
- Цена на информационната услуга;
- Съвместимост на формата на информацията с изискванията на информационната система на потребителя и др.

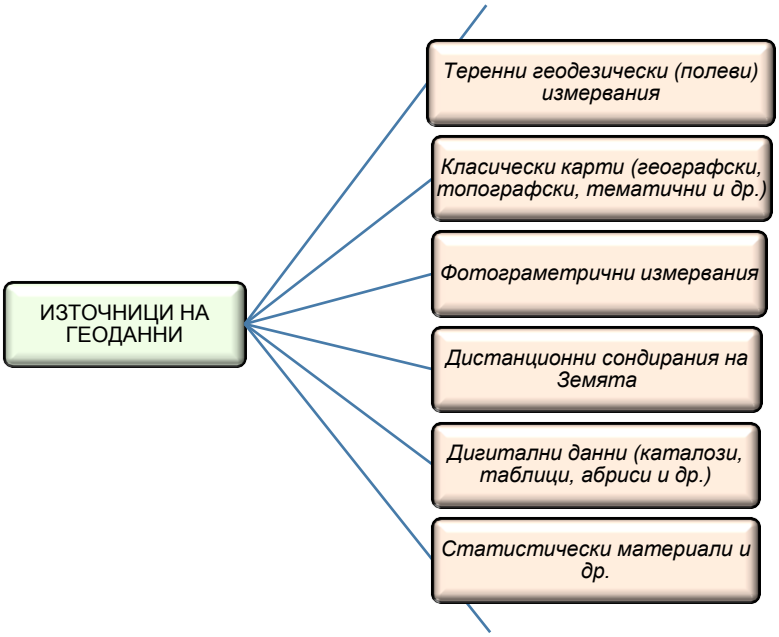
В геоинформатиката основните източници на геоданни и геоинформация са: *Теренни геодезически (полеви) измервания; Класически карти (географски, топографски, тематични и др.); Фотограметрични измервания; Дистанционни сондирания на Земята* ; *Дигитални данни (каталози, таблици, абриси и др.); Статистически материали и др.*

В геоинформатиката данните в зависимост от източниците се разглеждат като *първични*, *вторични* и *унифицирани*.

Първични данни се получават непосредствено при наблюдението или измерването на пространствените обекти. Такива данни се получават, чрез аерокосмически снимки, дистанционно сондиране на Земята, ГНСС технологиите и др.

Вторичните данни се получават на базата на обработката на първичните данни. Например вторични данни се получават при геодезическа снимка по полярен метод, обрата геодезическа засечка, сканиране на карти и др.

Унифицираните данни се получават при преобразуването на различните видове данни в единен вид, който дава възможност за създаване на единен информационен модел.



Фиг. 1. Източници на геоданни

2. Теренни геодезически (полеви) измервания

Получените геоданни чрез класически геодезически измервания, съвременни ГНСС методи или комбинация от двата вида за обектите от местността – релеф, хидрография, комуникационна мрежа, растителна покривка, населени места и др. е актуална и с висока точност. [3]

Чрез геодезическа снимка, непосредствено на местността се определя хоризонталното и вертикално положение на обектите, като се измерват ъгли и разстояния. Използват се геодезически инструмент – теодолити, нивелири, тотални станции и др. Тази първична информация се подлага на обработка и унификация.

Фиг. 2. Теренни геодезически (полеви) измервания

Съвременна технология е използването на ГНСС за непосредствено определяне позицията (координатите) на обектите от местността. Днес масово се използват ГНСС като: GPS (САЩ), ГЛОНАС (Русия), BEDU (Китай), Галилео (Европейски съюз) и др.

Недостатък на теренните геодезически измервания е, че се изисква повече време за измерване и обработка на данните, необходими са обучени екипи и подходящи геодезически инструменти.

3. Класически карти

Картите са основен източник на геоданни за ГИС. Всяка карта е информационен източник и дава:

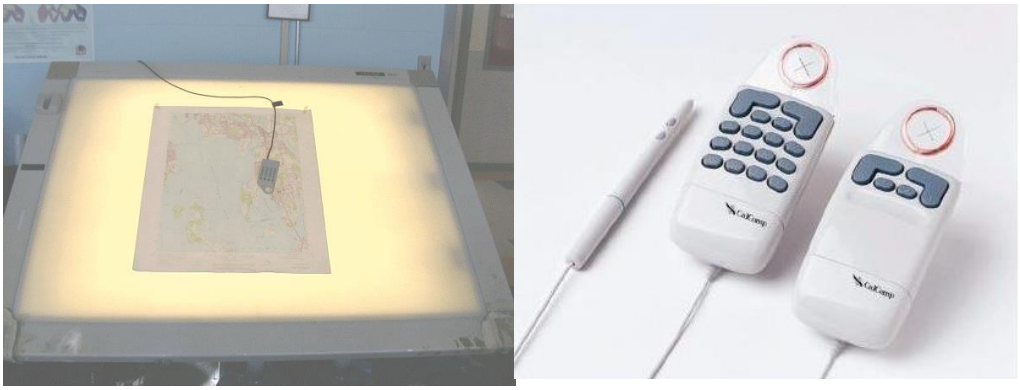
- Информация за разположението на обектите и тяхната взаимовръзка – *позиционна* (*метрична) информация*;
- Информация за типа, вида, класа на обектите, топологическите свойства на обектите и др. – *атрибутна информация*.

За извличане на картографската информация се използват периферни компютърни устройства – *дигитайзери* и *скенери*. Технологиите се наричат съответно *дигитализация* и *сканиране*.

Дигитализацията е дискретно преобразуване на аналоговата графична информация съдържаща се на картата в цифров вид (координати x,y).

Технологията на дигитализирането включва:

- Поставяне и закрепване на картата върху работното поле на дигитайзера;
- Избор на координатите на контролните точки (равнинни координати от план-квадратната мрежа или от каталог);
- За всеки картен лист се избират минимум 3-4 контролни точки равномерно разположени в областта;
- Чрез подходящ софтуер се извършва трансформация между координатната система на дигитайзера и координатната система на картата;
- Задава се атрибутна информация за обектите (тип линия, дебелина, цвят, начало-край на линията и др.);
- Обхождането на обектите се извършва с помощта на визир.



Фиг. 3. Дигитайзер

Дигитализацията се осъществява ръчно или полуавтоматизирано.

Недостатък на технологията е, че размера на дигитайзера е необходимо да съответства на размера на картата. Технологията е трудоемка и продължителна по време. Точността е в рамките на графическата точност (0.2 мм от мащаба на картата).

Сканирането е съвременна технология за извличане на картографска аналогова информация и преобразуването и в растерен вид и включва следните етапи:

- Картата се сканира с помощта на скенер (планшетен или барабанен тип) и се получава растерно изображение. Данните в цифровото изображение са кодирани с цели числа – за черно-белите изображения (*gray scale*) с 256 байта (от 0 до 255 за нюансите на сивото). Цветните изображения се кодират в три скали – съответно за нюансите на червеното (*red, R*), зеленото (*green, G*) и синьото (*blue, B*) в т.нар. *RGB model*;
- Прилага се геометрична корекция на растерното изображение;
- Избират се контролни точки и се определят техните координати от каталог или друг източник;
- С помощта на дисплей и мишка се оцифряват 3-4 контролни точки равномерно разположени на картата и се избира базовата картографска проекция;
- С помощта на софтуер се трансформира растерното изображение в координатната система на картата с помощта на контролните точки (георефериране);
- Извършва се векторизация на растерното изображение в ръчен, полуавтоматичен или автоматичен режим;
- Редактира се векторната карта в интерактивен режим;
- Резултатите се съхраняват в базата данни.

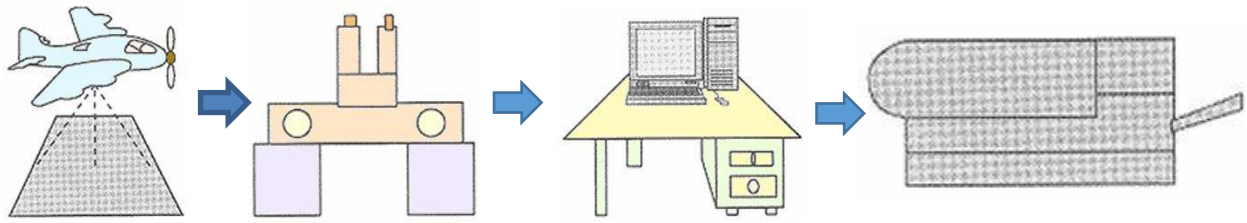
Фиг. 4. Скенери

4. Фотограметрични измервания

Аерофотоснимките и *космическите снимки* са източник на геоданни и геоинформация. Те играят важна роля за изследването на различни природни фактори – антропологични нарушения на природната среда, морфометричната система, екологичното състояние на територията и др. Аерофотоснимките може да послужи за оперативен контрол и мониторинг [2].

Фотограметричните методи за събиране на геоданни допълват другите източници на геоинформация. Получените фотоснимки изискват към тях да се приложи фотограметрична обработка, в резултат на което се получава трансформирано изображение, ортофото карти, височинни карти (DTM, DSM) и др.[4, 5, 6]

За осигуряване на обработката на снимките е необходимо наличието на определено количество наземни контролни точки (GCP), които се използват при аналитическата фототриангулация или в цифровата равнинна фототриангулация. Днес при интензивното развитие на цифровата фотограметрия, цифровите фотоснимки се получават в цифров вид и се съхраняват на различни магнитни носители.



Фиг. 5. Технология на обработка на аерофотоснимки

Цифровата фотограметрия се базира на аналитическата обработка на цифровите снимки. Цифровите снимки се получават по два начина:

- Обикновените аерофотоснимки се сканират и се получава растерно изображение;
- Внедряването на цифрови камери на летателните апарати (самолети, БЛА и др.) позволяват директно да се получи цифрово растерно изображение, което може да се обработва с компютърни технологии [9].

Недостатък на фотограметричният метод е, че се основава на получаването на снимки на базата на отражението на светлината. Това изисква добро осветяване на обектите по време на експозицията. Този недостатък се компенсира с въвеждането на специални камери, които не изискват такова осветление – инфрачервени, многоспектрални и др.

5. Дистанционни сондирания

Днес при наличието на специализирани изкуствени спътници на Земята успешно се прилагат методите на дистанционното сондиране (*remote sensing*), като за тази цел се използват различни технически средства като [10]:

- цифрови фотокамери с висока резолюция;
- сканиращи системи в реално време предаващи информацията на Земята по комуникационни канали;
- радиолокационни (*радарни*) снимачни системи - радари със синтетическа ареатура (РСА) – SAR (*Synthetic Aperture Radar*);[7]
- системи за получаване на инфрачервени (*топлинни*) снимки и др.[8]

6. Заключение

Познаването на източниците на геоданни е изключително важно. За постигане на по-добри резултати при моделирането в ГИС е необходимо да се отчитат предимствата и недостатъците на различните източници. Съчетаването на информацията от различни източници дава възможност за повишаване на качеството на геоинформацията от гледна точка на критерии за точност, надеждност, достоверност и др.

References

1. Андреев, А. Андреева П. Геоинформатика, геоинформационни системи, геоинформационни технологии. НВУ „В. Левски“ В. Търново 2021.

2. Беджева Моника, Стефан Добрев, Експериментална оценка на точността на първичната фотограметрична информация, получена от БЛА, Proceedings -f University -f Ruse - 2020, volume 59, ISSN 2603-4123 (-n-line)

3. Иванова, Ил. Кадастърът в България. Замисъл и изпълнение. ISBN 978-619-90684-0-3 издателство "АСМО - Academic Press"

4. Петров Д., Създаване на орторектифицирани изображения с използване на програмна система за цифрова фотограметрия - ERDAS – LPS, „Епископ Константин Преславски“, Шумен, 2013

5. Петров Д., М. Беджева, Използване на безпилотни летателни апарати във факултета по технически науки на шуменски университет „Епископ Константин Преславски“, Научна конференция с международно участие „Ден на безпилотната летателна система“, СУ „Св. Климент Охридски“, 2017 г.

6. Петров Д., М. Беджева, Статистически модели на запълването на депо за битови отпадъци, Научна конференция с международно участие „MATTEX 2018“, Шумен, ISSN 1314-3921

7. Прокопов Я. Възможности на наземното лазерно сканиране – основа за геодезическо моделиране. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2021, Faculty of Artillery, Air Defense and Communication and Information Systems.

8. Прокопов Я. Сателитната радарна интерферометрия като алтернатива за някои задачи от приложната геодезия. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2021, Faculty of Artillery, Air Defense and Communication and Information Systems.

9. Bedzheva M., D-brev St. Estimating the area -f the irregular dung-hills in Shumen municipality by using unmanned aerial vehicles. Annual -f Konstantin Preslavsky University -f Shumen, Faculty -f Technical Sciences, 2019

10. Коберниченко В. Г., Иванов О. Ю., Зраенко С. Обработка данных дистанционного зондирования Земли: практические аспекты. М. и др. ; Екатеринбург : Изд-во Урал. ун-та, 2013. — 168 с. ISBN 978-5-7996-0867-5

EXPLORING AND MODELING THE MAGNETIC FIELD IN POLAR REGIONS USING THE DATA FROM THE SWARM MISSION

Violeta R. Yordanova, Andrey I. Andreev

Department Geodesy, University of Architecture, Civil Engineering and Geodesy, Sofia, Bulgaria, violeta.yordanova91@gmail.com
Department Artillery, Air Defense and Communication and Information Systems/NMU "Vasil Levsky", Shumen, Bulgaria, andreev_an@abv.bg

***Abstract**: The European Space Agency's SWARM mission continues to be a huge success. The obtained data is part of numerous scientific discoveries and provide long-sought answers. The created magnetic models are with extremely high accuracy and give a new look at many scientific problems. They help in the exploration and study of Earth processes, the evolution of the Earth and a better understanding of the magnetic field.*

***Keywords**: SWARM, earth's magnetic field, north magnetic pole, south magnetic pole, asymmetry, supercontinents*

ИЗСЛЕДВАНЕ И МОДЕЛИРАНЕ НА МАГНИТНОТО ПОЛЕ В ПОЛЯРНИТЕ РАЙОНИ ЧРЕЗ ДАННИ ОТ МИСИЯТА SWARM

Виолета Р. Йорданова, Андрей И. Андреев

Въведение

Магнитно поле на Земята е тема, която вълнува научното общество от десетилетия. Неговият произход и развитие са от съществено значение за разбирането на процесите на планетата. То заляга във всеки един аспект и сфера от живота на Земята.

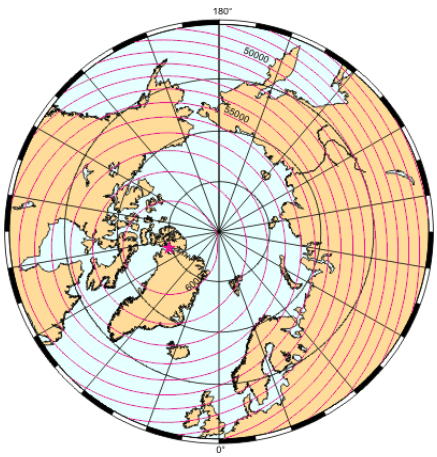
С развитието на космическите технологии през последните години и с невероятния успех на сателитната магнитна мисия SWARM на Европейската космическа агенция, учените имат възможност да надникнат по-дълбоко от всякога в дълбините на Земята, както и да получат отговори и доказателства на редица въпроси, касаещи характеристиките на геомагнитното поле - обръщане на магнитната полярност, блуждаене на магнитните полюси, произход на полето във вътрешността на Земята, механизмите, които го поддържат повече от милиард години и еволюция на планетата са само част от последните открития, с които може да се похвали научната общност.

1. Северен магнитен полюс

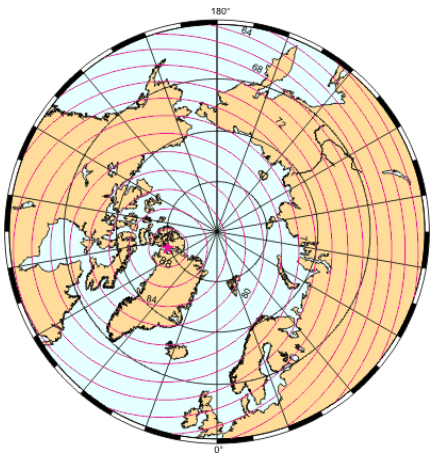
Земното магнитно поле се апроксимира като дипол в почти 90% от своята същност. В много малка, но изключително съществена част, полето на Земята е недиполно. В тези места то може да бъде в такава голяма зависимост спрямо диполното поле, че забележимо да променя формата му.

Това е изключително осезаемо в близост до Северния магнитен полюс, като това има сериозни последствия. За да може се онагледи как недиполната част на магнитното поле493 изкривява магнитното поле, е нужно първоначално да се разбере как изглежда самото диполното поле.

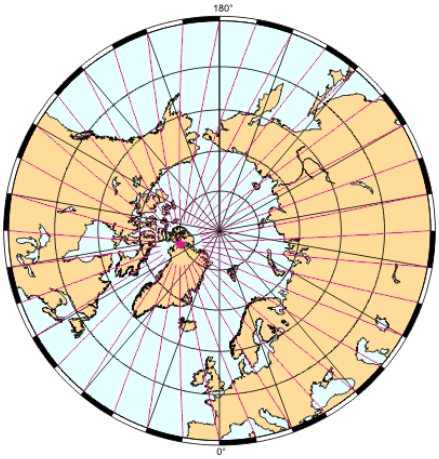
Трите диаграми на фиг. 1. илюстрират интензитета (фиг. 1*а*), инклинацията (фиг. 1*б*) и меридианите (фиг. 1*в*) на стандартно диполно магнитно поле в полярните региони:



Фиг. 1*а*



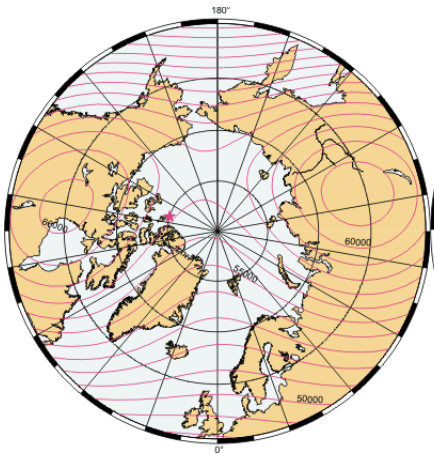
Фиг. 1*б*



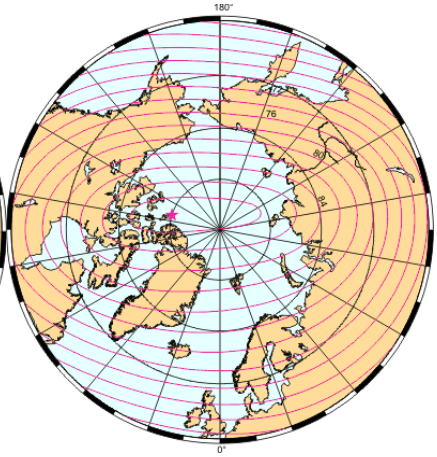
Фиг. 1*в*

Диполното поле е симетрично спрямо магнитния полюс. Изолиниите са концентрични кръгове с център в полюса. Силата на магнитното поле е най-голяма в магнитния Север, като при полюсите е два пъти по-силна отколкото на Екватора. Магнитните меридиани се събират радиално в Северния магнитен полюс или с други думи – стрелката на компаса директно показва магнитния Север.

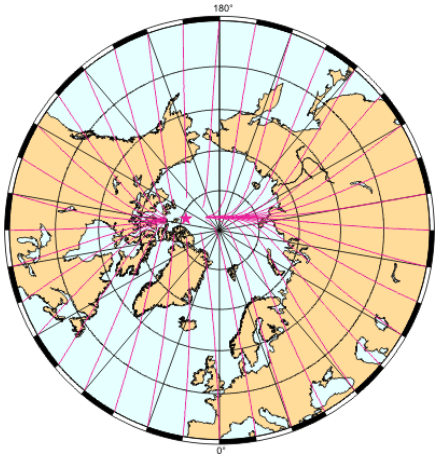
В действителност земното магнитно поле е различно и може да бъде описано по различен начин. На фиг. 2 може да се види, че недиполното поле има съвсем други характеристики. Наблюдаваното магнитно поле е изключително несиметрично (фиг. 2*а*). Изолиниите са силно елиптични, като магнитният Север е ситуиран близо до единият край на елипсата (фиг. 2*б*). Прави впечатление, че максималната силата на магнитното поле не е в Северния магнитен полюс, а има два пика – над централна Канада и над Сибир. На фиг. 2*в* се вижда, че магнитните меридиани не се събират радиално в полюса, което означава, че стрелката на компаса не сочи директно към магнитния север. Това не означава, че ако се следва пътя на магнитната стрелката, тя няма да ни отведе до северния магнитнитен полюс. Тя ще ни отведе до него, но определено няма да бъде по най-краткия път. Отклоненията, особено за Европа, са изключително големи с нарастването на ширината. Тръгвайки от Централна Европа в посока на 80°N, стрелката на компаса дава отклонение от около 46° от пътя.



Фиг. 2*а*

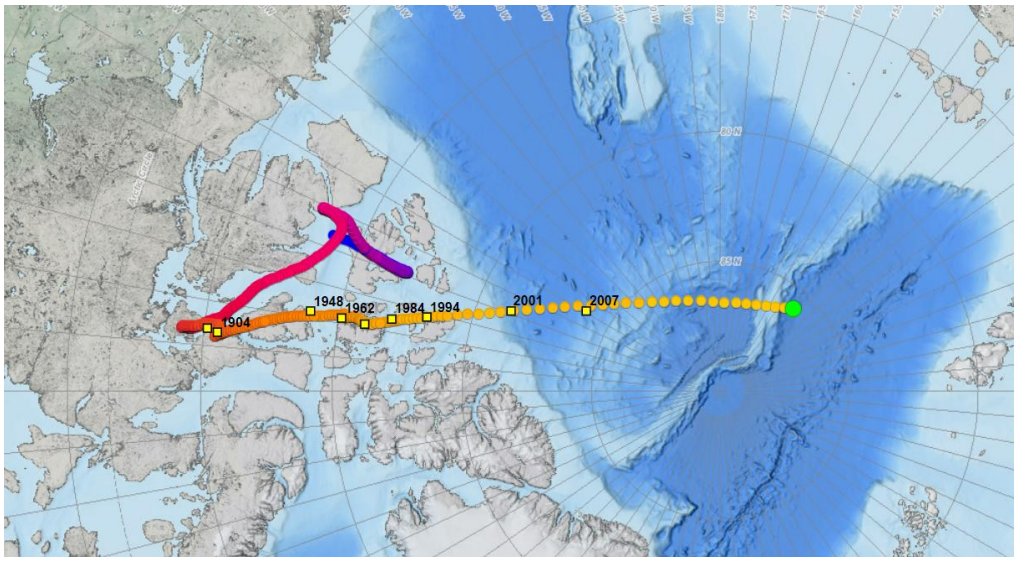


Фиг. 2*б*



Фиг. 2*в*

Позицията и „лутането" на Северния магнитен полюс винаги са били изключително интересна тема. Още при първоначалното му определяне през 1831 г. в полярните зони на Канада, полюсът се движи категорично към Сибир, като в интервала между 1990 и 2005 г. той значително увеличава скоростта си на преместване от 0-15 км/г. на рекордните 50-60 км/г. През октомври 2017 г. магнитният полюс пресича линията на смяна на датата, преминавайки на около 390 км от географския полюс и продължава движението си на юг. През последните 50 години той се движи по изключително линеен път, което, в сравнение с криволичещата траектория от преди 70-те години на миналия век, е безпрецедентно явление в исторически план и вече определено не изглежда като „лутане" (фиг. 3.)



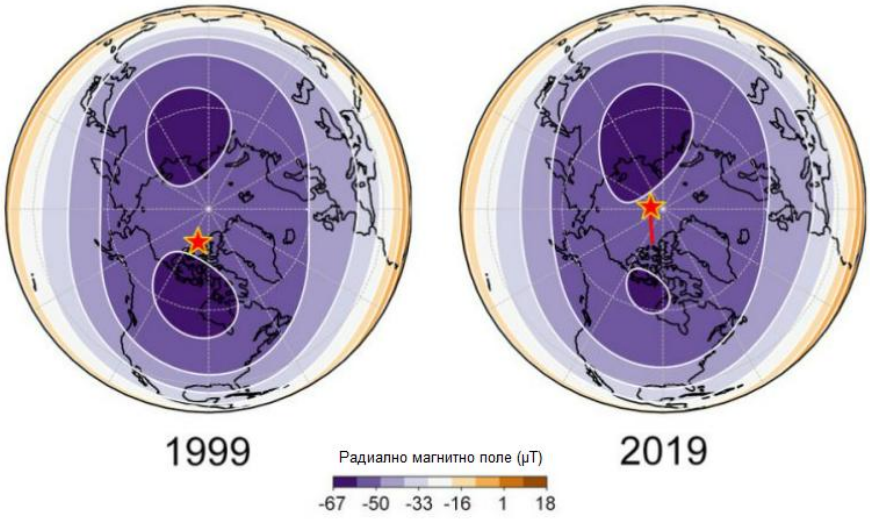
Фиг. 3. Движение на северния магнитен полюс за последните 400 години. Синята точка маркира положението на полюса за 1590 г. Зелената точка характеризира настоящето положене на магнитния полюс. (Източник: NCEI)

Местоположението на магнитния полюс е характеристика на генерираното от ядрото магнитно поле, което е сферично-радиално, отслабващо през мантията. Позицията му е само косвен индикатор за състоянието на земното динамо. Въпреки това геометрията на магнитното поле на Земята е от съществено значение за обществото, предвид че световния магнитен модел е основна компонента в методите за навигация в мобилните устройства и в средствата за навигация като цяло.

Последните изследвания на магнитните модели, показват че позицията на магнитния полюс до голяма степен се определя от два широкомащабни региона с отрицателен магнитен поток на границата между ядрото и мантията под Канада и Сибир (фиг. 4). Резки промени в движението на потока в земното ядро, между 1970 и 1999 г., водят до смаляване на канадския регион, като по този начин значително отслабва неговия отпечатък върху земната повърхност, което кара полюса драстично да се ускорява към Сибир.

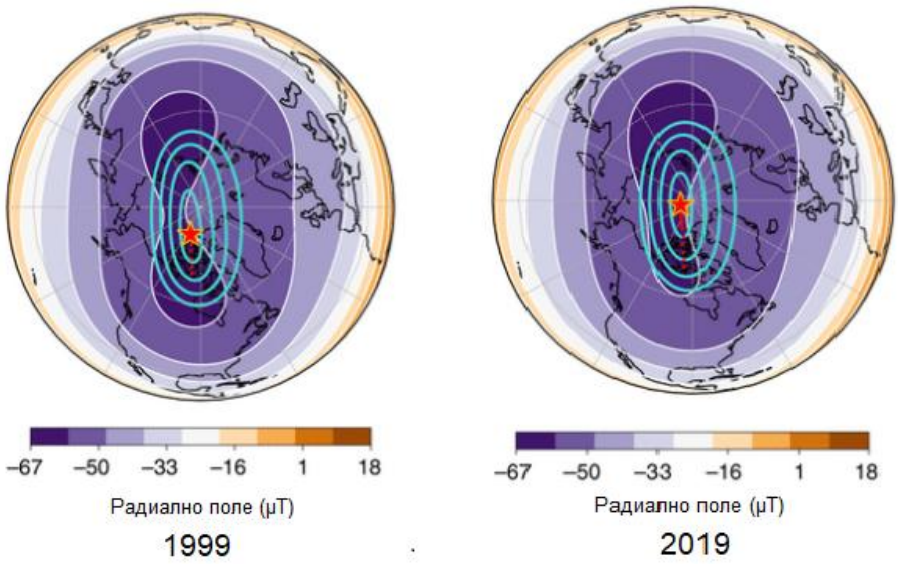
Разглеждани поотделно, спрямо общото магнитно поле, всеки от двата региона би генерирал собствен магнитен полюс в близост до централната си точка. При настоящата структура обаче, с два региона, разпростиращи геомагнитното поле на голяма ширина, се дефинират двата края на линеен поток, по който северният полюс може да се движи свободно.

В период от 20 години, между 1999 г. и 2019 г., ясно се откроява рязкото отслабване на канадския регион и лекото засилване на сибирския. Тези две промени в поведението на полетата, водят след себе си до драстичното увеличение в скоростта на движението на северният полюс, като съответно по-силното поле го придърпва към себе си, а именно - посока Сибир.



Фиг. 4. Региони с отрицателен магнитен поток, разположени под Канада и Сибир. Червената звезда маркира положението на северния магнитен полюс, а червената линия показва траекторията на преместване за период от 20 години. (Източник: ESA)

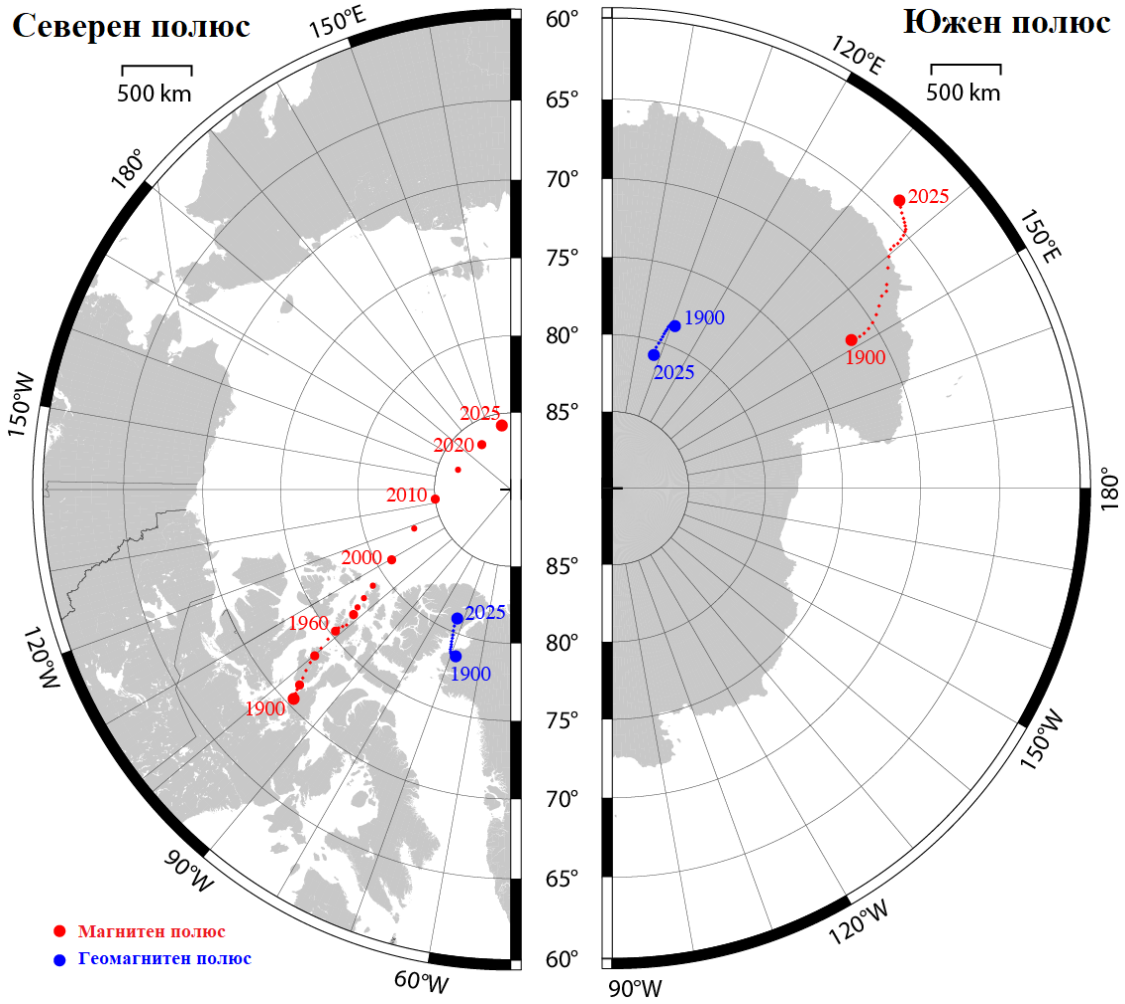
Въпреки че магнитното поле на земната повърхност е линейно свързано с полето на границата между ядрото и мантията, геометричното затихване през мантията означава, че тази връзка не е толкова лесна за картографиране. Например, северният магнитен полюс не съответства на място, където хоризонталното поле изчезва на границата ядро-мантията, а по-скоро е нелокално осредняване на полето, както е показано на фиг.5а и 5б. Канадските и сибирски повърхностни петна също са средни пространствени стойности за региони, доминирани от широкомащабни интензивни магнитни потоци под Канада и Сибир на границата ядро-мантия, които сами по себе си са основни характеристики на геодинамото. Става ясно, че временната позиция на северният полюс върху линейният поток всъщност зависи от силата на привличане между двата конкуриращи се региона върху границата между ядрото и мантията.



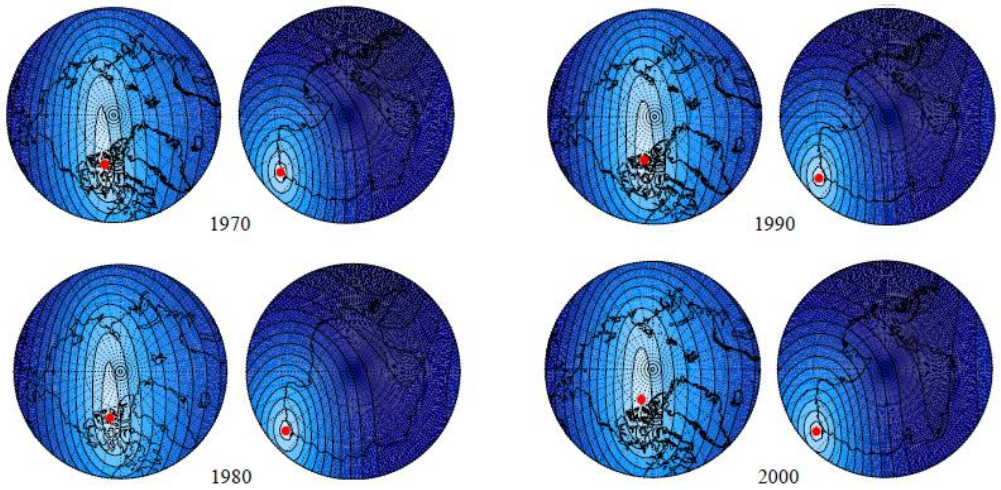
Фиг. 5. Радиалното поле, покрито с контурите на магнитното поле в тюркоаз. Червената звезда маркира положението на северния магнитен полюс, а червената линия показва траекторията на преместване за период от 20 години.

2. Северно-южна асиметрия

Изключително видима е разликата между движението на северния и южния магнитен полюс, както и липсата на каквато и да била зависимост между тях (фиг. 6). Това поведение може да се обясни чрез директно представяне на хоризонталния компонент на полето от модела на основното поле. На фиг. 7 се вижда, че полето проявява лек градиент по посоката на движение на полюса, когато става дума за северният магнитен полюс (СМП). От друга страна, при южния магнитен полюс (ЮМП), градиентът на полето е по-остър и изотропен. Това означава, че малките вариации в полето могат да доведат до значително изместване в положението на СМП, правейки позицията му недобре дефинирана. Местоположението на ЮМП е силно ограничено и много слабо се влияе от малките вариации в амплитудата на полето. Неговата позиция би се повлияла само от значителни промени в основното поле. Докато СМП, разчитайки на настоящата морфология на полето, остава свободно движещ се в областта със слаб интензитет и подвластен на малките вариации. Това го прави изключително лесен и удобен за изследване на бързите, малки и внезапни промени на основното поле.

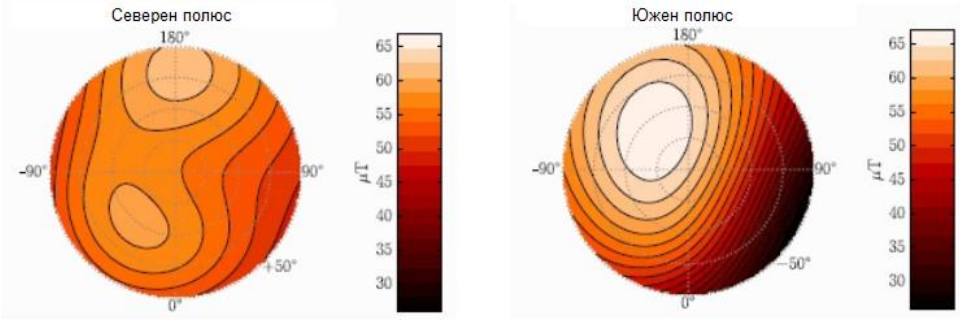


Фиг. 6. Движение на магнитните полюси



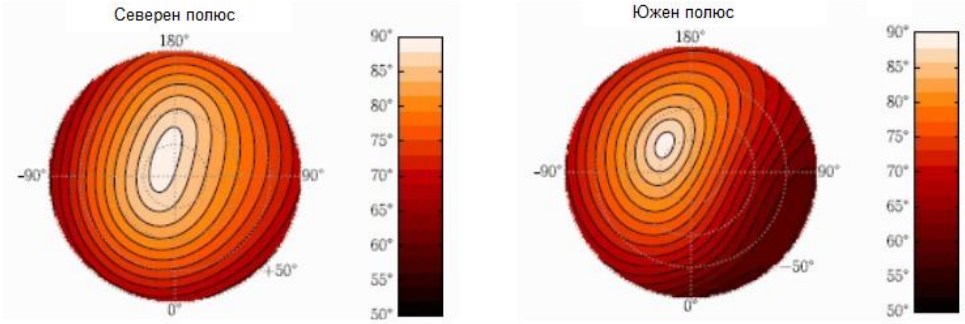
Фиг. 7. Стойности на хоризонталния компонент на магнитното поле в полярните зони за период от 40 години. Лява колона – Северен полюс, дясна – Южен полюс.

На фигури 8 и 9 могат да се видят разликите в силата на земното магнитно поле и в инклинацията за двете полярни зони. Плътността на потока на север може да се определени като поравномерна, както и ясно се разграничават двата максимума, дължащи се на магнитните региони под Канада и Сибир. В южното полукълбо полето е с един максимум и по-високи върхови стойности.



Фиг. 8. Разлики в сила на магнитното поле за двата полюса

Инклинацията също е различена в двете полукълба. Разликата между двете полусфери следва приблизително същия модел като силата на магнитното поле, като линиите на полето в северното полукълбо са по-вертикални в регионите, където полето е най-силно.



Фиг. 9. Разлики в инклинацията за двата полюса

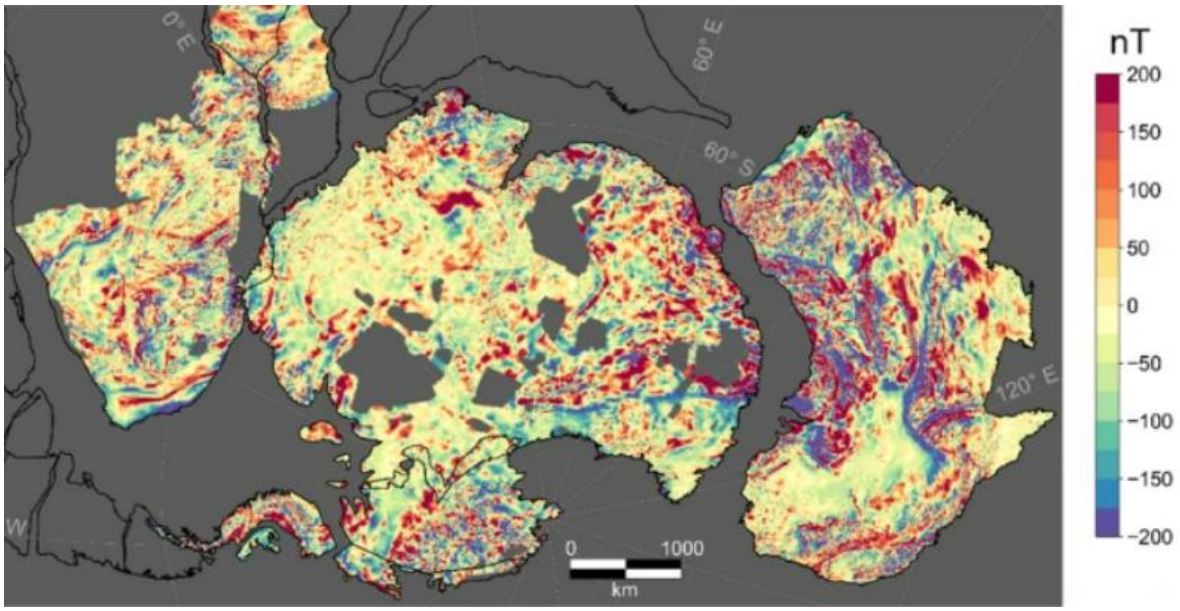
3. SWARM и опознаването на Антарктида

Тайните на Антарктида от десетилетия вълнуват научният свят. Със своята отдалеченост, сурови атмосферни условия и изключително дебелата си ледена обвивка, континентът се явява огромно предизвикателство пред учените. Изучаването и разбирането му играят фундаментална роля в разбирането за еволюцията на Земята и процесите свързани с нея. През последните десетилетия технологичният напредък на научната общост спомага все повече и повече за вдигането на завесата над леденият континент.

Мисията SWARM и магнитното поле се оказват ключов фактор в последните научни открития и дават отдавана търсени отговори. Използвайки магнитните данни, предоставени от космическата мисия се разкриват тайните на геологията, скрити под километричната ледена обвивка на Антарктида и доказват връзката между континента и суперконтинента Гондвана. Този изключителен научен прогрес използва магнитнитно поле, за да разгадае дълбоко скритата геология и да свърже континента с предишните му съседи. Това е от значение не само за разбирането на глобалните цикли на суперконтинента, продължили милиони години и формирали еволюцията на Земята, но също така хвърля светлина върху влиянието на самата твърда земя върху ледената покривка над нея.

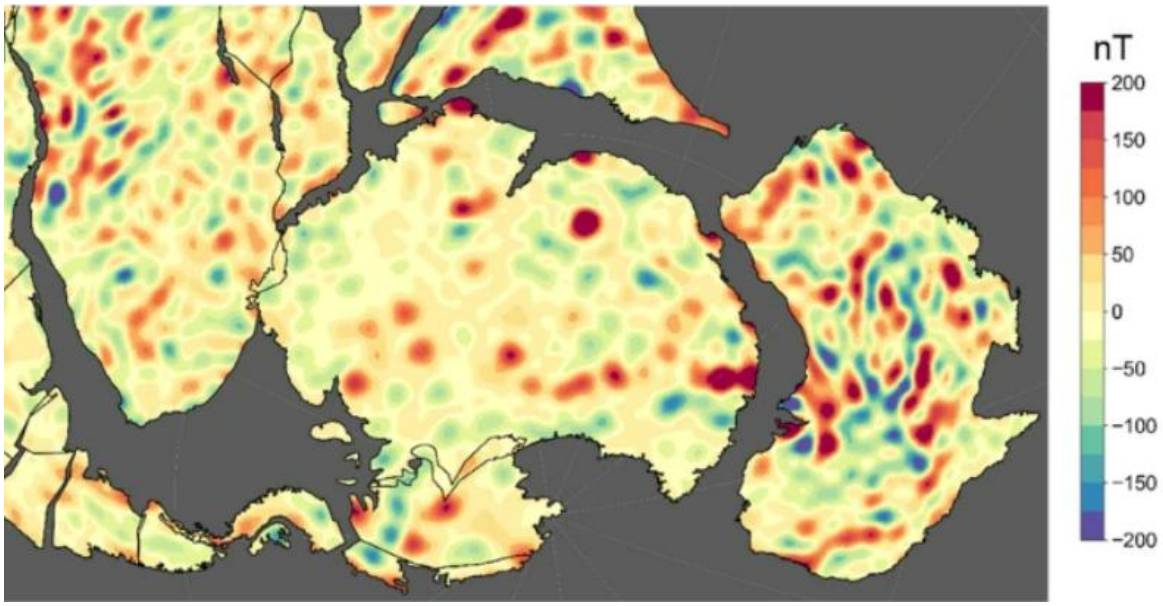
Чрез комбиниране на сателитни и аеромагнитни данни се осигурява ключова връзка между сегментите на суперконтинента Гондвана, като се свързва геологията на Антарктида с бившите ѝ съседни континенти, а именно Австралия, Индия и Южна Африка, с които е споделяла дълга тектонична история.

Гондвана е смесица от континенти, включващи Южна Америка, Африка, Арабия, Мадагаскар, Индия, Австралия, Нова Зеландия и Антарктида. При сблъсъка на тектоничните плочи през прекамбрийските и ранните камбрийски времена (преди около 600–500 милиона години), те изграждат огромни планински вериги, сравними със съвременните Хималаи и Алпи. Суперконтинентът започна да се разпада в началото на юрския период, преди около 180 милиона години, оставяйки в крайна сметка Антарктида блокирана и изолирана на Южния полюс и покрита с лед за около 34 милиона години.



Фиг. 10. Аеромагнитни модели на сегментите от суперконтитена Гондвана

Магнитните данни, събрани през последните 50 години, макар и с различна разделителна способност и точност, обхващат Антарктида и нейните древни континентални съседи. Предишни проучвания показват, че магнитните данни, особено когато се интерпретират съвместно с геохронологични, геохимични, геофизични и палеомагнитни набори от данни, помагат за идентифицирането на фундаментални връзки между бивши съседни земи в суперконтинентите. Тези връзки са много подходящи за изучаване и определяне както на относителните позиции, така и на тектоничните процеси, които са засегнали различните континенти.



Фиг. 11. Магнитен модел на сегментите от суперконтитена Гондвана, получен чрез данни от мисията SWARM. Сателитните данни запълват липсващата информация, като дават по-пълна и точна картина за магнитното поле

Реконструирането на магнитни модели спомага за позиционирането на Антарктида като част от Гондвана и дава възможност да се екстраполира геологията ѝ от бившите ѝ съседни земи. Подобни реконструкции свързват Източна Антарктида с Южна Австралия и магнитните данни ясно показват продължението на австралийската геология под антарктическите ледове. Основен проблем за създаването на подобни модели се оказват нискокачествените аеромагнитни данни, както и липсата на такива. Такива проблеми настъпват при реконструкциите на връзките на Антарктида с Южна Африка и Индия.

Тъй като максималната дължина на вълната, съдържаща се във всеки набор от аеромагнитни данни, е ограничена, често се говори за спектрални празнини. За да се преодолеят тези празнини, обхватът на дългите вълни се заменя със сателитни данни поради повишената им точност. Разделителната способност на получените сателитни модели на магнитно поле е ограничена от височината на орбитата, инструментите и периода на мисията. Добавянето на данните, получени от мисията SWARM, към предишни сателитни мисии спомага за повишаването на спектралната точност на литосферните модели.

Заключение

Благодарение на информацията, получена от сателитната мисия SWARM на Европейската Космическа Агенция, могат да се проследяват бурните промени в магнитното поле, както и да се наблюдават и изучават неговите основни характеристики. Данните от мисията подпомагат за изучаването на еволюцията на Земята. Моделите генерирани от получените данни, се използват за анализ и съпоставка на компонентите на полето във всяка точка и епоха. Това води до улесняване на процесите на изследване на магнитната история, тектониката на земните плочи, обръщането на полюсите, както промените настъпващи в земното ядро и тяхното отражение на повърхността на Земята.

References

1. Government of Canada https://geomag.nrcan.gc.ca/mag_fld/arctics-en.php
2. Livermore, P.W., Finlay, C.C. & Bayliff, M. Recent north magnetic pole acceleration towards Siberia caused by flux lobe elongation. Nat. Geosci. 13, 387–391 (2020). https://doi.org/10.1038/s41561-020-0570-9
3. Korte, M. & Mandea, M. *Magnetic poles and dipole tilt variation over the past decades to millennia.* Earth Planets Space 60, 937–948 (2008)
4. *Mandea, M. & Dormy, E. Asymmetric behavior of magnetic dip poles*. Earth Planets Space 55, 153–157 (2003)
5. British Geological Survey http://www.geomag.bgs.ac.uk/education/poles.html
6. Ebbing, J., Dilixiati, Y., Haas, P. et al. *East Antarctica magnetically linked to its ancient neighbours in Gondwana.* Sci Rep 11, 5513 (2021). https://doi.org/10.1038/s41598-021-84834-1
7. *Nagarajan, N.* (2020). *Earth's Magnetic Field and its Wandering Magnetic Poles.* Resonance. 25. 363-379. 10.1007/s12045-020-0951-9.

INFLUENCE AND ANALYSIS OF GEODETIC PRIMARY DATA MEASUREMENTS DURING THE IMPLEMENTATION OF A MONITORING SYSTEM IN AN OPEN MINE - ADAPTIVE PERIOD

Yasen T. Prokopov

Department Artillery and Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levsky" jasen_prokopov@abv.bg

***Abstract**: The Open pit mining method of mineral resources is a priority in the mining industry. Ensuring reliability and safety in mine operation can be controlled and guaranteed by reliable continuous geodetic observations and has an essential role. The overall monitoring is related to the control and management of the deformation processes in the rock massif, provided by qualitative and reliable measurements, which are the basis of this methodology.*

***Key words**: monitoring, analysis, deformation process, geodetic measurements*

ВЛИЯНИЕ И АНАЛИЗ НА ПЪРВИЧНИ ДАННИ ОТ ИЗМЕРВАНИЯ ПРИ РЕАЛИЗАЦИЯ НА МОНИТОРИНГОВА СИСТЕМА ЗА УСЛОВИЯТА НА ОТКРИТ РУДНИК – АДАПТИВЕН ПЕРИОД

д-р инж. Ясен Тр. Прокопов

1. ВЪВЕДЕНИЕ

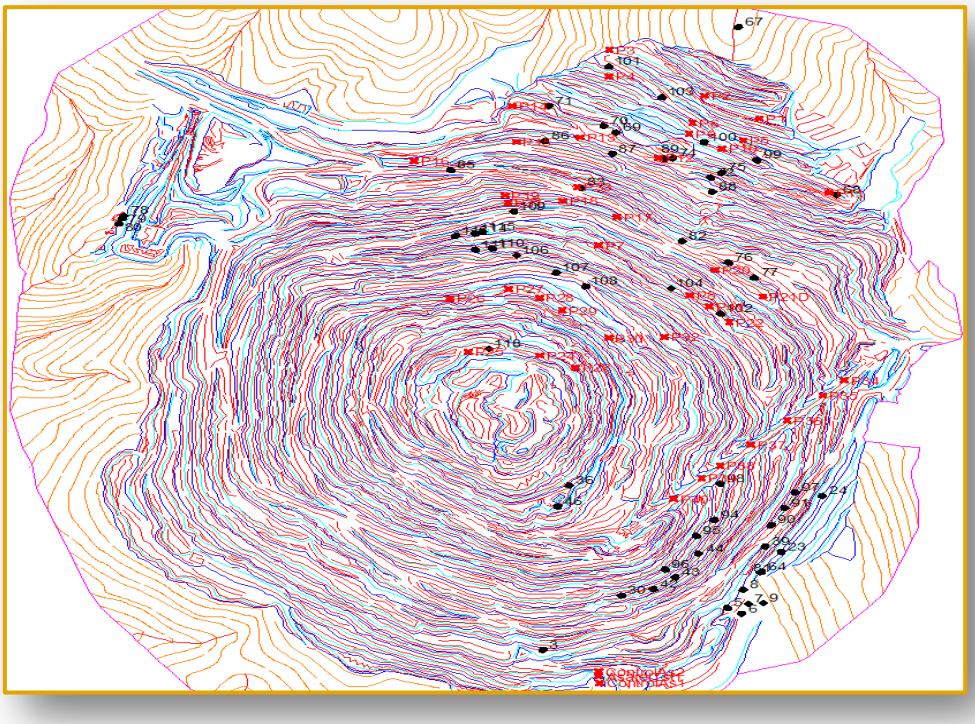
Поради спецификата на минните работи [4] в открити рудници и заради тяхната форма, изземването на природни богатства в дълбочина, налага оптимално разполагане на изходните точки за наблюдение. Следенето на деформации по бордовете на по-високите стъпала е улеснено, а промяната на работните участъци налага поставяне на нови и премахване на някои от съществуващите контролни точки.

Мониторингът на деформационните процеси е с цел предотвратяване на опасни (катастрофални) промени в масива и прогнозиране при управление на тези процеси. Основен начин за проследяване на положените контролни точки е тяхното непрекъснато денонощно наблюдение, свързано с голям брой измерени посоки и дължини (десетки хиляди), което позволява надеждност при анализа на тези данни.

Типичен пример за такава мониторингова система е контрола при експлоатацията за условията на рудник "Асарел - Медет" [2].

2. ОРГАНИЗАЦИЯ НА ИЗМЕРВАНИЯТА И КОНТРОЛНИ ТОЧКИ

Периодичните наблюдения на контролните точки, разположени в целия котлован на рудника (фиг. 1, в червено) обхващат период от около една година. По-голямата част от точките, с монтирани върху тях отражателни призми са извън зоната на предпазния целик. Измерванията не са със строго фиксирани моменти от денонощието, много пъти с повторна регистрация, а обемът на направените измервания включва над 20 000 координати на контролните точки.



Фиг. 1. Разположение на контролните точки

Основните наблюдения се отнасят за точките от северния борд на рудника, при наблюдателна станция разположена в стабилен участък на южния борд. Използваната роботизирана тотална станция Trimble S8 Long Range AutoLock DR HP FineLock осигурява ъглова точност от 1” и измерва разстояния с точност от 0.8 mm+1 ppm $*$ S.

Използването на прецизен инструмент и надежден софтуер за обработка свежда до минимум грешките от измерванията, а основно точността при полярното определяне положението на контролните точки зависи от грешките от външните условия. Инструкционните ограничения [3] за високоточни измервания са в противоречие с идеята за непрекъснатите денонощни целогодишни измервания, но количествените данни са надеждна основа за анализ.

3. ВЛИЯНИЕ НА ПРЕЦИЗНИТЕ ИЗМЕРВАНИЯ ВЪРХУ ПЛАНОВОТО И ВИСОЧИННО ПОЛОЖЕНИЕ НА КОНТРОЛНИТЕ ТОЧКИ

При мониторинга преместванията на наблюдаваните точки се определят като разлика в положението им при два цикъла измервания. Във всеки цикъл положението на точките се определя с координати X, Y и H. При изчисляването им освен измерените ъгли и дължини, се използват допълнително метеорологични и геометрични корекции за отразяване на влиянието на атмосферните условия, рефракцията, константата на далекомера, кривината на Земята, неправолинейността на визурата, надморската височина, проекционната равнина и др.

Тъй като станциите и наблюдаваните точки са трайно стабилизирани, почти всички геометрични корекции са с едни и същи стойности при различните цикли измервания. Така при намирането на разликата между измерванията от два цикъла, определящи премествания на наблюдаваните точки, по-голямата част от корекциите (които са събираеми) се елиминират. Това позволява използването на опростени формули за определяне на преместванията:

$$\Delta X_i=\Delta S_i*\cos\Delta\alpha_i$$
$$\Delta Y_i=\Delta S_i*\sin\Delta\alpha_i \qquad (1)$$
$$\Delta H_i=\Delta S_i*\mathrm{ctg}\Delta Z_i\ ,$$

където:

- ΔX_i, ΔY_i, и ΔH_i са преместванията на наблюдаваната точка през i-тия цикъл в условна координатна система, една от осите на която съвпада с малката ос на елипсата на грешките;
- $\Delta\alpha_i$ е разликата в посочните ъгли към наблюдаваната точка между i-тия цикъл и 0-вия цикъл;
- ΔS_i е разликата в наклонените разстояния към наблюдаваната точка между i-тия цикъл и 0-вия цикъл;
- ΔZ_i е разликата в зенитните ъгли към наблюдаваната точка между i-тия цикъл и 0-вия цикъл.

При някои анализи вместо посочният ъгъл, наклоненото разстояние и зенитният ъгъл от 0-вия цикъл се използват тези от някой от предходните цикли.

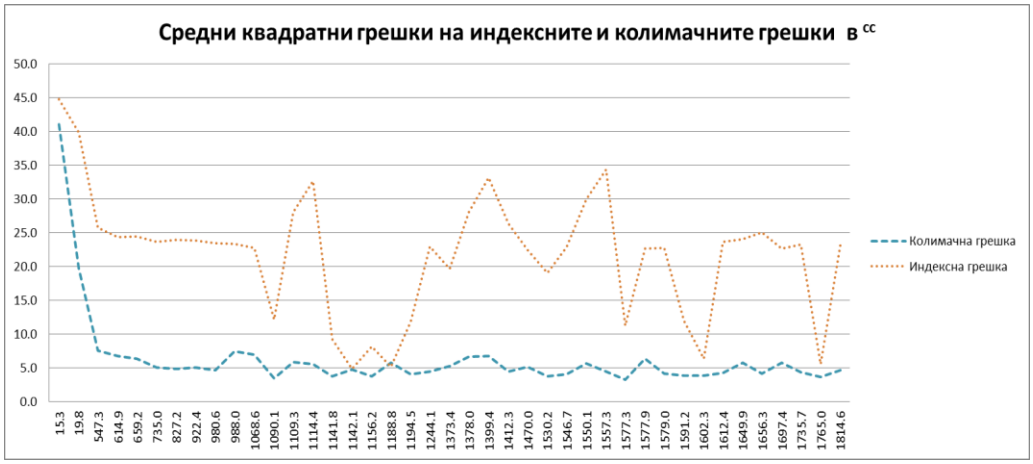
За определяне на точността в план и във вертикално отношение се използват средните квадратни грешки определени по формулите [1]:

$$m_{\text{хор.}} = \pm \sqrt{\frac{m_{\Delta\alpha i}}{\rho} S^{\,2} + m_S^2} \qquad (2)$$

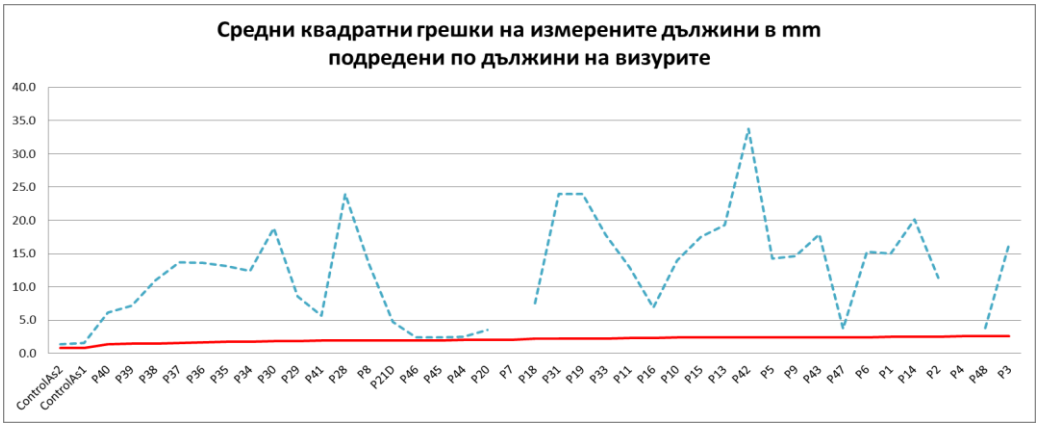
$$m_{\text{верт.}} = \pm \sqrt{m_S \cos Z^{\,2} + S\frac{m_Z}{\rho}\sin Z^{\,2}} \ . \qquad (3)$$

Тъй като контролните точки са в условно нестабилен участък, промяната на техните координати във времето, предизвикана от промени в състоянието на бордовете, в случая се игнорира. По този начин фактическата точност на измерванията при използване на този инструмент за условията на рудник "Асарел" и при този подход не е обвързана с положението на точките.

От над 450 000 измервания за 39 контролни точки (при различен брой измервания за отделните точки), получените стойности за СКГ на индексните и колимачните грешки са показани на фиг. 2 (причина за по-значимите разлики е вертикалната рефракция), а тези за дължините – на фиг. 3 (с червено е техническата точност).



Фиг. 2. Средни квадратни грешки при ъгловите измервания



Фиг. 3. Средни квадратни грешки на измерените дължини

Върху точността при определяне в пространството на наблюдаваната точка влияе не само точността, но и стойностите на измерените разстояния и ъгли. Анализът на това влияние при определяне на превишенията е направен в табл. 1. На базата на всички измервания са определени средните дължини на визурите към наблюдаваните точки и средните зенитни ъгли. В началото на таблицата са определени влиянието върху превишението (котата) на изменението на измереното разстояние (стъпка 30 mm), при постоянен зенитен ъгъл и на изменението на измерения зенитен ъгъл (стъпка 1^{cc}), при постоянно разстояние, за средни стойности на измерените величини.

От таблицата се вижда, че ако се приеме паспортната точност на измерените ъгли (3^{cc}), то грешката в превишението (котата) при среден зенитен ъгъл е 6.1 mm. Същата такава неточност при определяне на превишението би се получила при грешка в определеното разстояние от 580 mm. Ако вместо паспортната точност се използва определената от измерванията, чак грешка в измереното разстояние от 2000 mm би повлияла със същата стойност както точността на измерването на ъглите.

От направения анализ може да се твърди, че за средни разстояния и зенитен ъгъл към наблюдаваните точки в рудник “Асарел“ точност на измерените разстояния от порядъка на 1-2 m не влияе върху определянето на котите повече от точността на определянето на зенитните ъгли. Аналогични изследвания могат да се направят и за точността при определяне на положението на наблюдаваните контролни точки по направление перпендикулярно на визурата.

В табл. 1 е направен аналогичен анализ за измерванията към точки с максимални и минимални наклонени разстояния и зенитни ъгли. От него се вижда, че макар и не с такива стойности, както при средните разстояния и зенитен ъгъл, влиянието на точността на измереното наклонено разстояние е значително по-малко отколкото точността на измерените ъгли.

4. ИЗВОДИ И ЗАКЛЮЧЕНИЕ

На база обобщените резултати от дължинните измервания, точността на измерените наклонени разстояния е близка до тази в техническата спецификация на инструмента при занижено влияние на страничните фактори. Това определя значително по-точното установяване на преместванията на наблюдаваните точки по направление на визурите. Поставянето на мониторинговата станция по направление на очакваните деформации и използването на условна координатна система, на която една от осите съвпада с това направление, би повишило значително точността на преместванията на точките.

Основно влияние върху точността при определяне на наблюдаваните точки в план оказва точността на измерените посоки. Върху точността, при определяне на техните коти, измерените наклонени разстояния практически не влияят, а тя зависи основно от точността на измерените зенитни ъгли. Резултатите от мониторинговите измервания следва да се използват след критична оценка на първичните данни от измерванията.

Добрата оценка на състоянието на един рудничен масив, която се осигурява от мониторинговите измервания, гарантира надеждни прогнози и планиране на минните работи. Част от нея са първичните данни, чиято обработка гарантира сигурността на оценките.

References

1. Димитров Д., Инженерна геодезия, ДИ „Техника“, София, 1989 г.

2. Изграждане на мониторингова геодезична система от призми за рудник “Асарел“ за автоматично следене на деформации посредством роботизирана тотална станция, GNSS референтни станции и интеграция на данните в софтуерен продукт Trimble 4D Control, Работен проект, „Солитех“ АД, 2015.

3. Инструкция за изследване на деформациите на сгради и съоръжения чрез геодезически методи, София, Главно управление по геодезия, картография и кадастър, 1980.

4. Инструкция за опазване на обектите и съоръженията от вредното влияние на минните работи във въглищните басейни, М-во на енергетиката, София, 1983.

Таблица 1

Контролна точка със средна дължина на визурата и среден зенитен ъгъл

Зенитен ъгъл (Z) 100.6725 Накл. разстояние S 1302.611 Превишение -13.760

Стъпка по S в mm	10	40	70	100	130	160	190	220	250	280	310	340	370	400	430	460	490	520	550	580	610	640	670	700	730	760
Промяна в H в mm	-0.1	-0.4	-0.7	-1.1	-1.4	-1.7	-2.0	-2.3	-2.6	-3.0	-3.3	-3.6	-3.9	-4.2	-4.5	-4.9	-5.2	-5.5	-5.8	-6.1	-6.4	-6.8	-7.1	-7.4	-7.7	-8.0
Стъпка по Z в ^{cc}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Промяна в H в mm	-2.0	-4.1	-6.1	-8.2	-10.2	-12.3	-14.3	-16.4	-18.4	-20.5	-22.5	-24.6	-26.6	-28.6	-30.7	-32.7	-34.8	-36.8	-38.9	-40.9	-43.0	-45.0	-47.1	-49.1	-51.2	-53.2

Контролна точка с максимална дължина на визурата

Точка (призма) P3 Зенитен ъгъл (Z) 94.3262 Накл. разстояние S 1814.702 Превишение 161.519

Стъпка по S в mm	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120	125	130
Промяна в H в mm	0.4	0.9	1.3	1.8	2.2	2.7	3.1	3.6	4.0	4.5	4.9	5.3	5.8	6.2	6.7	7.1	7.6	8.0	8.5	8.9	9.3	9.8	10.2	10.7	11.1	11.6
Стъпка по Z в ^{cc}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Промяна в H в mm	-2.8	-5.7	-8.5	-11.4	-14.2	-17.0	-19.9	-22.7	-25.6	-28.4	-31.2	-34.1	-36.9	-39.7	-42.6	-45.4	-48.3	-51.1	-53.9	-56.8	-59.6	-62.5	-65.3	-68.1	-71.0	-73.8

Контролна точка с минимална дължина на визурата и максимален зенитен ъгъл

Точка (призма) P40 Зенитен ъгъл (Z) 114.801 Накл. разстояние S 547.257 Превишение -126.091

Стъпка по S в mm	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120	125	130
Промяна в H в mm	-1.2	-2.3	-3.5	-4.6	-5.8	-6.9	-8.1	-9.2	-10.4	-11.5	-12.7	-13.8	-15.0	-16.1	-17.3	-18.4	-19.6	-20.7	-21.9	-23.0	-24.2	-25.3	-26.5	-27.6	-28.8	-30.0
Стъпка по Z в ^{cc}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Промяна в H в mm	-0.8	-1.7	-2.5	-3.3	-4.2	-5.0	-5.9	-6.7	-7.5	-8.4	-9.2	-10.0	-10.9	-11.7	-12.5	-13.4	-14.2	-15.1	-15.9	-16.7	-17.6	-18.4	-19.2	-20.1	-20.9	-21.7

Контролна точка с минимален зенитен ъгъл

Точка (призма) P1 Зенитен ъгъл (Z) 93.0708 Накл. разстояние S 1649.921 Превишение 179.229

Стъпка по S в mm	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120	125	130
Промяна в H в mm	0.5	1.1	1.6	2.2	2.7	3.3	3.8	4.3	4.9	5.4	6.0	6.5	7.1	7.6	8.1	8.7	9.2	9.8	10.3	10.9	11.4	11.9	12.5	13.0	13.6	14.1
Стъпка по Z в ^{cc}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Промяна в H в mm	-2.6	-5.2	-7.7	-10.3	-12.9	-15.5	-18.0	-20.6	-23.2	-25.8	-28.3	-30.9	-33.5	-36.1	-38.6	-41.2	-43.8	-46.4	-49.0	-51.5	-54.1	-56.7	-59.3	-61.8	-64.4	-67.0

MONITORING OF CONTROL POINTS POSITION IN AN OPEN MINE - SPACE-TIME RELATIONS BETWEEN THE DEFORMATION FIELD COMPONENTS

Yasen T. Prokopov

Department Artillery and Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levsky" jasen_prokopov@abv.bg

Abstract: *For the analysis of the deformation processes during the open mine extraction of mineral resources the statistical methods are applied, supplemented with the geodynamic processes assessments. In such an approach, all factors affecting stability are analyzed and the coordinates and altitudes of the points are used as input information. Secondary indicators in this analysis are two-dimensional distributions, displacement rates, diurnal and seasonal variations, etc.*

Key words: *moving, analysis, deformation process, statistical valuations.*

МОНИТОРИНГ НА ПОЛОЖЕНИЕТО НА КОНТРОЛНИ ТОЧКИ В ОТКРИТ РУДНИК - ПРОСТРАНСТВЕНО-ВРЕМЕВИ ЗАВИСИМОСТИ МЕЖДУ КОМПОНЕНТИТЕ НА ДЕФОРМАЦИОННОТО ПОЛЕ

д-р инж. Ясен Тр. Прокопов

1. ВЪВЕДЕНИЕ

Мониторингът на деформационните процеси при експлоатацията на открити рудници е свързан с непрекъснатото следене на контролни точки, разположени по работни и неработни бордове.

При това точността на измерванията пряко зависи от фактори от околната среда, влияещи върху праволинейността на оптическия сигнал - изменение на температурата и атмосферното налягане, прозрачност на въздуха, наличие на дисперсни частици и др. Това влияние е както във времето, така и като разпределение в пространството между наблюдателната станция и съответните контролни точки.

За условията на рудник "Асарел" използваните данни са за 28 контролни точки, а измерените деформации са обусловени от обективни фактори. Наблюденията се отнасят за период от около 8 месеца – от месец септември, до месец май [1].

2. ИНФОРМАТИВНОСТ НА ПРИЗНАЦИТЕ

Измереният сигнал (координатите на точките) по всяка от осите се разглежда като сума от премествания на масива под влиянието на различни фактори и сума от грешки при измерването, предизвикани от процеси с различна физическа природа

$$F = \sum_{i=1}^{n} f_i + \sum_{j=1}^{m} n_j \ , \qquad (1)$$

където f_i е влиянието на отделните фактори, а n_j са грешките при измерването.

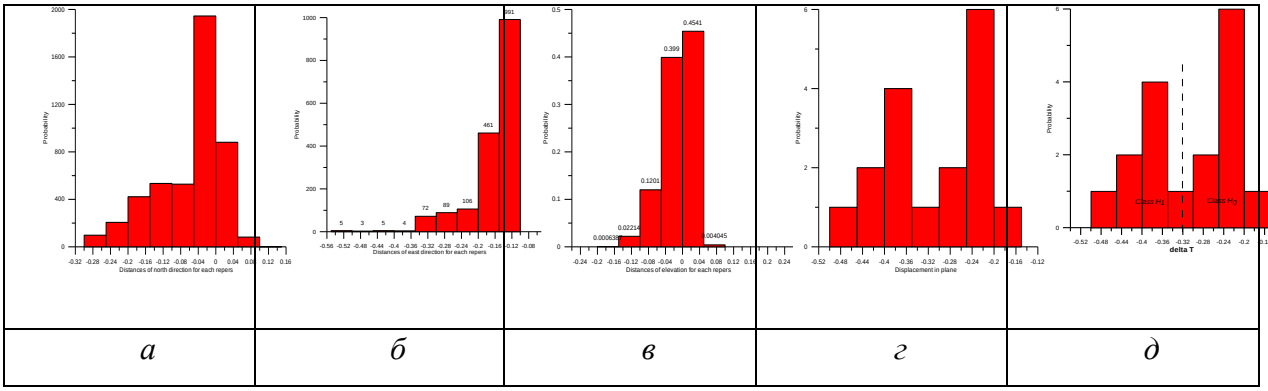
По принцип масива (работния участък от рудника) се намира в определено напрегнато-деформирано състояние. В резултат на минните работи реакцията му към изменението на това първично състояние, към определени тектонски движения и към циклични геодинамични процеси предизвиква преместванията в този масив, респективно на контролните точки. Освен от евентуалната “деформирана“ траектория на оптическия лъч, грешките (точността) при определяне на преместванията зависят и от влиянието на редица екзогенни фактори – оводняване, замръзване, топлинно разширение и др.

Факторите, които влияят върху устойчивостта на масива могат да бъдат корелирани и некорелирани, стационарни и нестационарни, разпределени във времето и пространството. Самите промени в контролните точки се характеризират с амплитуда, скорост на преместванията и времеви корелационни отношения.

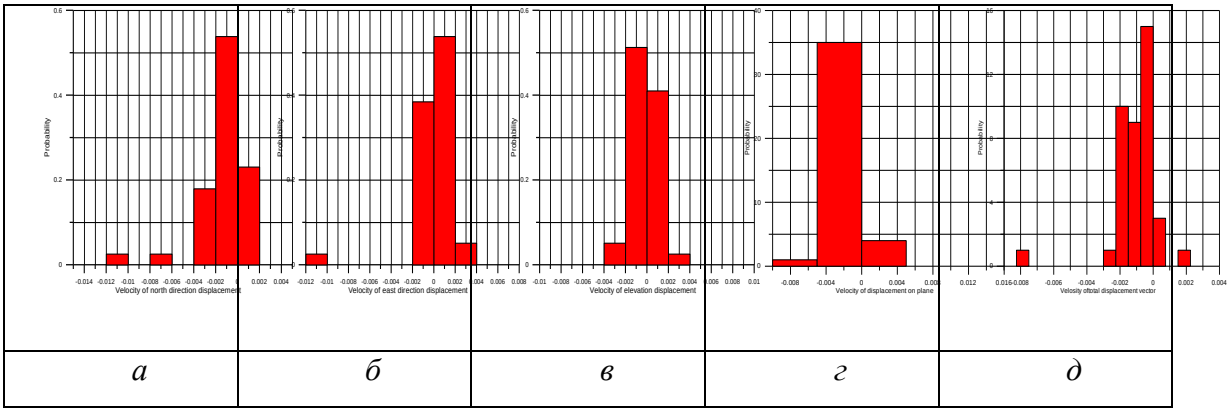
Представянето в обобщен вид на наличните данни е чрез плътностите на разпределенията на вероятностите. Това се отнася както за самите премествания, така и за техните средни скорости, като са включени данните за всичките 28 точки (фиг. 1 и 2).

Всички хистограми се характеризират с определена асиметрия и добре изразени максимуми, като с определена условност биха могли да се апроксимират с нормалния закон за разпределение. Наличие на статистически значими класове се наблюдава в полето на вектора на преместване в план и в тоталния вектор (фиг. 1 *г* и *д*), което позволява да се предположи наличието на две групи контролни точки с различна кинематика.

В разпределенията на скоростите на преместване се наблюдават както пикове с незначителна вероятност извън областта на основното разпределение, така и вътрешно-групова структура, особено при скоростта на преместване на тоталния вектор (фиг. 2 *д*).

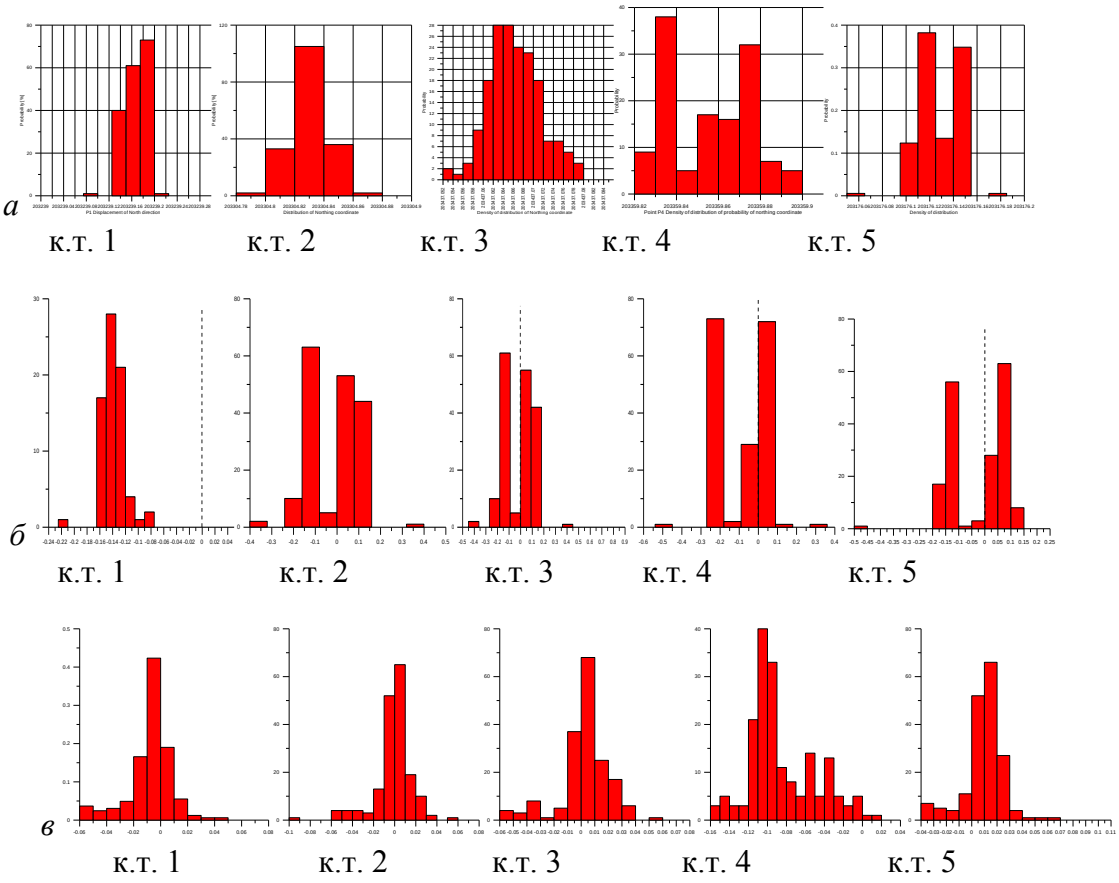


Фиг. 1. Разлики (премествания) спрямо началните показания с плътност на вероятностите:
а - *в* северна посока, *б* - в източна посока, *в* - вертикални премествания, *г* - в хоризонтална равнина, *д* - тотален вектор на преместванията (в пространството)



Фиг. 2 Скорости на преместване по направления с плътност на вероятностите:
а - в северна посока, *б* - в източна посока, *в* - по вертикала, *г* - в план, *д* - в пространството

По-детайлното изследване на сигнала е чрез хистограми, показващи разпределението на компонентите на деформационното поле по отделни точки (показани са само 5 от тях). На фиг. 3*а* са деформациите N в северна посока (отговаря на X), на 3*б* – деформациите E в източна посока (отговаря на У), а на 3*в* - H във вертикално направление Видът на разпределението позволява да се извърши класифициране на точките.



Фиг. 3. Хистограми на преместванията

Всяка от модите на разпределенията съответства на определен клас състояния, обусловени от хидрогеодинамични или техногенни процеси. При наличието на бимодално разпределение се

предполага изменение на въздействието на различните фактори, водещи до изменение на компонентите на преместване на контролната точка във времето.

За интерпретацията на бимодалните разпределения би била полезна и допълнителна информация за динамиката и обемите на добивните работи, дренирането на рудничните води и тектонската структура в изследвания участък (пространството между станцията и контролните точки).

Многомодалните разпределения се апроксимират като набор от нормално разпределени класове. Класифицирането на всеки от класовете се извършва чрез сравняването на разстоянията между техните моди, а също така по отношение на нулевата стойност.

3. ТОЧНОСТ НА ИЗМЕРВАНИЯТА – СТАТИСТИЧЕСКИ АНАЛИЗ

Оценката на точността на измерванията е на база извършване на повторни измервания в стабилни, безаномални точки, в които външните въздействия са минимални. Статистическата обработка на получените резултати след това е със съответните оценки - средна стойност, стандартно отклонение, ексцес, асиметрия и други показатели, където *n* е броя на точките, от които са получени оценките [3].

Табл. 1

Дата	n	N	σ_N	E	σ_E	H	σ_H
04.10.	6	-0.00865	0.000383	0.03708	0.001674	-0.003642	0.0018399
17.10.	6	-0.01752	0.002136	0.08308	0.00557	0.018555	0.0115509
24.10.	6	-0.0237	0.0007563	0.0848	0.002184	-0.005351	0.005057
31.10.	6	-0.002232	0.001306	0.08788	0.00392	-0.01001	0.0048337
07.11.	6	-0.02955	0.002065	0.09398	0.002178	0.0023398	0.0104003
20.11.	5	-0.01382	0.002853	0.0557	0.01504	-0.023853	0.0139552
29.11.	5	-0.0285	0.001046	0.08632	0.004442	0.0007812	0.0047813
16.12.	6	-0.03808	0.001281	0.10527	0.002406	0.0119833	0.0068687
31.12.	6	-0.02085	0.0005206	0.06393	0.002258	-0.012044	0.0012909
08.01.	6	-0.02732	0.002195	0.0647	0.005893	0.0028483	0.0143274
28.01.	6	-0.02585	0.0004461	0.05123	0.003391	-0.004211	0.0014376
12.02.	8	-0.01791	0.00506	0.02649	0.0266	-0.034378	0.0088178
21.02.	6	-0.02052	0.00293	0.05352	0.006923	-0.03892	0.0125544
28.02.	6	0.00687	0.00129	-0.1192	0.002994	-0.001567	0.0025318
08.03.	5	0.00932	0.001279	-0.13362	0.0026546	0.0029786	0.0085741
17.03.	6	0.00862	0.00126	-0.13135	0.0027443	-0.005453	0.0019524
28.03.	6	0.01123	0.001582	-0.14107	0.0038749	-0.006104	0.0116064
05.04.	7	0.00777	0.000544	-0.13406	0.0015789	-0.004517	0.0016528
16.04.	6	0.00232	0.000703	-0.13332	0.0022013	0.0122273	0.0037508
30.04.	6	0.01657	0.001127	-0.15598	0.0045653	0.007772	0.0048532
05.05.	6	0.01167	0.003799	-0.16307	0.0036968	0.0082192	0.0039807
10.05.	6	0.01225	0.002025	-0.16488	0.0035835	-0.00061	0.0021616

От анализа на разпределенията на плътностите на вероятностите, имайки предвид компонентите на преместванията й, контролна точка 1 се определя като относително стабилна, както и района около нея.

Статистическите оценки на компонентите на вектора на преместванията за условно стабилен участък са показани в табл. 1. Периодът на измерване има продължителност около 8 месеца и обхваща три сезона – есен, зима и пролет, но не се забелязва съществена зависимост на флуктуациите от сезонните условия.

Средните стойности на стандартните отклонения от повторните измервания по съответните компоненти на вектора на преместванията са както следва:

- северна посока - 0.0017 m;

- източна посока - 0.0050 m;
- по височина - 0.0063 m.

Дневните флуктоации на хоризонталните компоненти на вектора на преместванията варират в сравнително тесни граници, което е пряко свързано с факта, че промените в осветеността, температурата и атмосферното налягане не оказват съществено влияние върху точността на измерванията. Малко по-високи стойности на флуктуациите се наблюдават за вертикалната компонента, което може да се обясни с влиянието на вертикалната рефракция.

Данните от повторните денонощни измервания показват необходимостта от спазване на изискванията на методиката за геодезични наблюдения [2] за осигуряване на еднообразни условия, в частност измерванията да се извършват по едно и също време.

Измерванията с честота по-висока от честотата на изследваните процеси води до по-големи грешки поради проявление на корелираност на шумовете. С цел намаляване влиянието на вертикалната рефракция, честотата на измервания през един час подобрява координатните определяния, поради по-големия брой измервания през тъмната част от денонощието, когато влиянието на рефракцията е минимално.

Прилагането на ГНСС технологията косвено влияе и значително подобрява точността при определяне на преместванията, заради прецизното и непрекъснато следене на неизменното положение на наблюдателните станции.

4. ЗАКЛЮЧЕНИЕ

Прилагането на непрекъснати наблюдения за следене на деформационни процеси в открити рудници, с търсене на пространствено-времеви закономерности между отделните компоненти на деформационното поле, гарантира надеждни изводи и препоръки. Качествения статистически анализ е в основата на маркиране и уточняване на проблемните зони. Това улеснява препоръките за безопасна експлоатация и планирането на минните работи за по-дълъг период.

References

1. Изграждане на мониторингова геодезична система от призми за рудник “Асарел“ за автоматично следене на деформации посредством роботизирана тотална станция, GNSS референтни станции и интеграция на данните в софтуерен продукт Trimble 4D Control, Работен проект, „Солитех“ АД, 2015.
2. Инструкция за изследване на деформациите на сгради и съоръжения чрез геодезически методи, София, Главно управление по геодезия, картография и кадастър, 1980.
3. Костадинов, К., Вълчинов, В., Математическа обработка на геодезически измервания, учебник, Университет по архитектура, строителство и геодезия, София, 2012.

IDENTIFICATION OF LAND PROPERTY

Ilinka Ivanova, Yasen T. Prokopov

Department Artillery and Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levsky" ilinkaivanova@mail.bg, jasen_prokopov@abv.bg

Abstract: *Many of the ownership documents were drawn up under plans that have long been canceled for various reasons. In their place, others are approved, in which the boundaries of the properties of the previous plan have been changed. When establishing the right of ownership of land property for the purpose of professing transactions, amendments to the regulatory plans, etc. it is often necessary to determine the boundaries of a land property from one plan whether they coincide with its boundaries under another or are included in part of it. Therefore, the identification of land properties is an important task decided by the surveyor.*

Key words*: land property, cadastral map, cadastral plan, property*

ИДЕНТИФИЦИРАНЕ НА ПОЗЕМЛЕН ИМОТ

Илинка Иванова, Ясен Прокопов
НВУ „Васил Левски"

Идентифицирането на поземлен имот е често срещан случай в геодезическата практика, особено актуален при възстановяване на собствеността върху земеделските земи и на земите и горите от горския фонд, така и при изработването на кадастралната карта (КК). Проблема с идентифицирането на поземлените имоти в България възниква след освобождението от турско робство. Това е време когато започва разграбване на земи от българските чорбаджии и е необходимо идентифициране на държавните имоти. Османската империя съставяла крепостни актове при извършените сделки с недвижими имоти, които по-късно се наричат нотариални.

Документите даващи право на собственост (различни видове нотариални актове, завещание, договор за делба, решение на поземлена комисия заедно със скица и др.) се изготвят в зависимост от действащото към момента законодателство. В крепостните и по-късно в нотариалните актове описанието на поземлените имоти е по различен начин, с различни параметри, които са общи, пространствени, понякога нееднозначно определени като, площ, вид на поземления имот (нива, ливада, лозе, лавандула, двор, и др.), местност и съседи - при извършване на разпоредителни сделки и при установяване на собствеността.

Особен проблем е въпросът с местностите, които нямат определени граници, често една местност е известна с няколко имена и то различни във времето за поколенията.

Към настоящият момент за голяма част от територията на страната е създадена кадастрална карта в числен вид, където пространственото положение на поземлените имоти е еднозначно определено с координатите на границите и идентификатора им. В условията на динамични промени собствеността на имотите и при налична числена кадастрална карта описателните характе-

ристики в старите нотариални актове (и крепости актове) вече губят значението си като параметри указващи еднозначно за кой имот се отнасят, къде е точното му местонахождение.

Идентифицирането на поземлен имот се налага, когато по данни от представен документ за собственост не е възможно еднозначно да се определи пространственото положение на имота (да се определят координатите на неговите гранични точки).

Основната цел на експертното търсене при идентификацията на поземлен имот е да се направи изследване, чрез което изхождайки от описателните характеристики на имота в документа да собственост и наличните картографски материали да се даде заключение за кой идентификатор в действащата кадастрална карта (планоснимачен номер в съответния кадастрален план) се отнася старият нотариален акт.

Трябва да се отбележи, че в много от случаите няма пълно припокриване границите на имота от стария документ за собственост изготвен по скица към тогава действащия план (кадастрален или регулационен) и действащия към момента на проверката за идентичност. Понякога между плана, по който е съставен нотариалния акт и актуалния план към годината на идентифициране на имота има и други планове – кадастрални, регулационни и др. В този случай имота освен, че си променя идентификатора (планоснимачен номер или на урегулирания поземлен имот) променя и границите си, а понякога и собственика. Очевидно идентифицирането на поземлен имот е свързано със събиране и анализ на различен картен материал създаден през годините и на документите за собственост.

Освен на база планове и карти, и документи за собственост, имот може да се идентифицира на място като се използва описанието на имота, съществуващите на терена трайни елементи от топографски и площта на имота. Необходимо е на място да съществуват поне три от границите на имота и да е известна неговата площ. Тогава имота се заснема по съществуващите трайни топографски елементи и се нанася в КК или кадастралния план (в координатна система на КК или на кадастралния план) като неговите очертания се затварят в съответствие с площта му [1-5].

Необходими документи и процедури при идентифициране на поземлен имот:

- документ за собственост или друго вещно право върху недвижимия имот;
- скица-копие от кадастралната карта;
- скица-копие от кадастрален план или други планове действали по време на издаването на документа за собственост;
- събиране на налични графични материали;
- оглед и заснемане на място - при необходимост.

Идентифицирането на поземлен имот се извършва на два етапа:

1. Изработване на комбинирана скица

Комбинираната скица представлява съвместно изчертаване в няколко слоя на всички съществуващи планове и карти за имота - кадастрална карта; архивен кадастрален план; стар кадастрален план към помощен план; стар кадастрален план; действащ регулационен план; стар регулационен план; застроителен план; план на подземни проводи и съоръжения; карта на възстановената собственост; извадка от ортофотопланове и др. Изработва се след като са събрани всички налични планове и карти за поземления имот [8].

Използваните планове и карти могат да са на различна основа (носител) – традиционна (кадастрон или на недеформируем материал) или в числен вид. Освен това може да са в различни координатни системи.

Плановете, които са на традиционен носител трябва да се сканират, мащабират и векторизират. Когато са преобразувани в числен вид, ако са в различни координатни системи те се трансформират в една и съща, за предпочитане е в координатната система, с която работи Агенцията по геодезия, картография и кадастър (АГКК). След трансформирането им се извършва съвместяване на различните планове [6, 7].

Ако няма достатъчно данни за трансформиране на числените модели на съответния имот в една и съща координатна система, те се съвместяват като се използват едни и същи елементи на ситуацията, отразени в различните планове и карти, т. е. съвместяването на плановете и картите се извършва по ситуация. В комбинираната скица всеки план се изчертава с различен цвят и със същия цвят се надписват планоснимачните номера, идентификаторите и номерата на урегулираните поземлени имоти (УПИ), както и други пояснителни надписи.

В легенда се записва кой цвят за кой план се отнася и заповедта за одобряването му (ако няма такава се записва годината на изработване и „неодобрен"). В заглавие се надписва „Комбинирана скица", за кой поземлен имот се отнася, плановете, които са обединени, населено място, община, област и мащаб.

На фиг. 1 е показана комбинирана скица на поземлен имот (ПИ) с идентификатор 38978.900.5216 по кадастрална карта одобрена със заповед № РЗ-18-42/13.08.2015 г., УПИ VIII-605 по регулационен план (РП) от 1983 г., изменение на РП със заповед № 17-354/21-12.2017 г. на кмета на община Костинброд и на кадастрална карта одобрена със заповед № РД-18-40/04.01.2021 г. на началника на СГКК Софийска област.

2. Идентифициране на имота

Възможни са два варианта:

- Частична идентичност – когато части от имота попадат в различни имоти от друг план;
- Пълна идентичност - съвпадение на имотите от различните планове – пълна идентичност.

При идентифицираме Урегулиран поземлен имот (УПИ) VI-3281 по регулационен план от 1983 г. на гр. Костинброд с кои имоти е идентичен от кадастралната карта № РЗ-18-42/13.08.2015 г. на ИД на АГКК наличните обстоятелства са отразени по-долу.

УПИ VI-3281 от регулационния план от 1983 г. е изчертан както следва - със син цвят вътрешно регулационните линии и с червен уличната регулационна линия. Площта му е 814.59 m^2. Част от УПИ VI-3281 в размер на 117.71 m^2 попада в ПИ с идентификатор 38978.900.3503, част в размер на 48.06 m^2 попада в ПИ с идентификатор 38978.900.5217 и част в размер на 648.06 m^2 в ПИ с идентификатор 3281. В заключение УПИ VI-3281 от рег. план от 1983 г. **е частично идентичен** с имоти с идентификатори 38978.900.3503, 38978.900.5217 и 38978.900.3281.

Пълна идентичност на имоти има при условие, че границите на ПИ от различните планове напълно съвпадат. Когато няма числен модел на плановете се проверява съвпадането им в границите на допустимата графична точност.

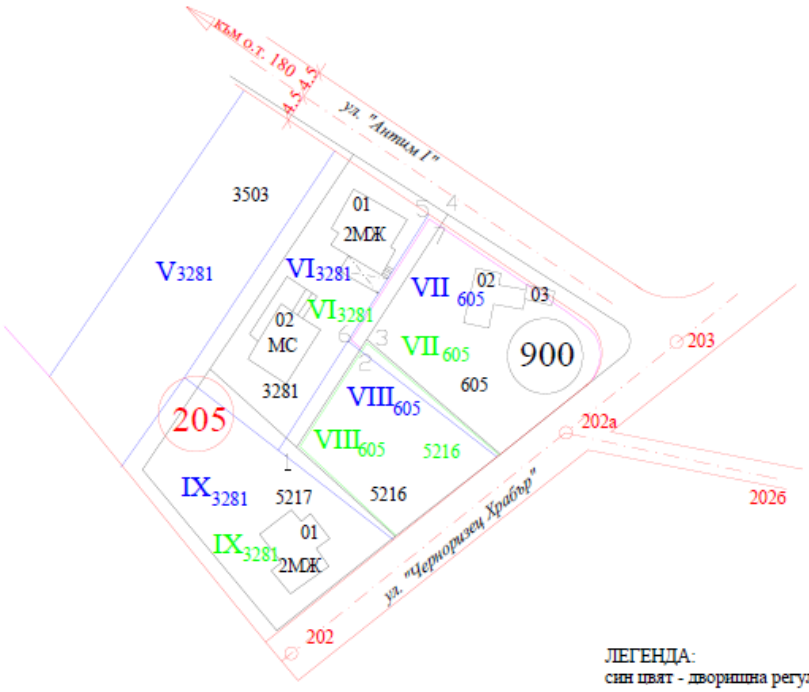
На комбинирана скица (фиг. 1) пример за такава идентичност са УПИ VI-3281 от рег. план от 1983 г. (изчертан и надписан в синьо) и УПИ VI-3281 от рег. план от 2017 г. (надписан в зелен цвят, като границите не са показани, защото напълно съвпадат с границите на същия УПИ от 1983 г.).

След като се изготви комбинираната скица и се идентифицира имота, определен от възложителя, правоспособното лице по кадастър издава удостоверение за пълна или частична идентичност. Когато идентичността е частична се изписват площите и номерата на имотите от съответния план, в който попада имота за идентифициране.

КОМБИНИРАНА СКИЦА

на ПИ 38978.900.5216 по кадастрална карта одобрена със заповед № РД-18-42/13.08.2015 г., УПИ VIII-605 по регулационен план от 1983 г., изменение на ПР одобрено със заповед № РД 17-354/21.12.2017 г. на кмета на общ. Костинброд, изменение на кадастрална карта одобрено със заповед РД-18-40/04.01.2021 г. на н-ка на СГКК Софийска област.

М 1:1000



ЛЕГЕНДА:
син цвят - дворищна регулация от 1983 г.
червен цвят - уличка регулация от 1983 г.
черен цвят - кадастрална карта 2015 г.
зелен цвят - изменение на ПР на УПИ VIII-605 от 2017 г.
Розов цвят - изменение на КК от 2021 г.

ЗАБЕЛЕЖКА:
Зелените и розовите линии са отместени, за да се виждат.
Източната граница на ПИ 38978.900.3281 е означена с числата 1, 2, 3,4, съгласно КК от 2015 г.
С одобреното изменение на КК от 2021 г. границата на ПИ 38978.900.3281 минава през числата 2, 6, 5, 7.

юни, 2021 г.

Изработил:
инж. И. Иванова

Фиг. 1

References

1. Андреева П., Андреев А. Обзор на информационни системи за кадастъра в България. Proceedings of International Scientific Conference 2020, Faculty of Artillery, Air Defense and Communication and Information Systems - Shumen. 388- 396 p. ISSN 2367-7902.

2. Андреев А., Андреева П. Създаване на цифров модел на местността на базата на съществуващи топографски карти в средата на ГИС. сп. Артилерийски преглед кн. 3 стр. 17- 31, 2009 ISBN 1314-0388.

3. Андреева П., Иванова И. Анализ и оценка на ефективността на вътрешната среда на ИИСКИР. ШУ „Еп. К. Преславски“ – МАТТЕХ 2016. ISSN: 1314-3921

4. Петрова П. Информационни системи за кадастър у нас и в чужбина. Трета международна конференция „Наука, образование, иновации” кн. II Шумен, 21-23 май 2014 г., стр. 196-204. ISBN: 978-954-577-969-5.

5. Петрова П., Андреев А. Систематичен подход за оценка на ефективността на информационните технологии за кадастър. III Международна научна конференция. 21-23 май 2014 г. Шумен т. II стр. 205-210. ISBN 978-954-577-969-5.

6. Закон за кадастъра и имотен регистър, ДВ бр. 34, 2000 г.

7. Наредба № РД 02-20-5 от 2016 г. за Съдържанието, създаването и поддържането на кадастралната карта и кадастралните регистри, ДВ. бр. 4 2017 г.

8. Andreeva P., Iliev M. Theoretical basis of a methodology for conducting empirical sociological studies on the efficiency of operation of the cadaster information system. PROCEEDINGS OF UNIVERSITY OF RUSE - 2020, volume 59. Copyrights© 2020 ISSN 1311-3321 (print), ISSN 2535-1028 (CD-ROM), ISSN 2603-4123 (on-line). ISSN 2367-7902

CERTAIN ASPECTS OF GEOSPATIAL ANALYSIS IN GEOINFORMATION SYSTEMS

Petina A. Andreeva

Department Artillery and Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levsky" petiand@abv.bg

Abstract: *Geospatial analysis is an important process in which a search is carried out in the distribution of geodata and related spatial objects. As a result of the analysis of geoinformation, quality new information is obtained that enriches the previous information. Geospatial analysis is oriented towards activities related to the Earth's surface, its shell, the parts above and below the Earth's surface. The temporal nature of the analysis focuses on the past, present and future, asking questions such as "where", "when", "why", "how", "who", etc. The methods of spatial analysis are unlimited in time and space.*

Key words: *Geospatial analysis Digital maps, map projection, GIS.*

НЯКОИ АСПЕКТИ НА ГЕОПРОСТРАНСТВЕНИЯ АНАЛИЗ В ГЕОИНФОРМАЦИОННИТЕ СИСТЕМИ

д-р инж. Петина А. Андреева

1. Геопространствени анализи в геоинформационните системи

Геопространственият анализ е важен процес в който се извършва търсене на закономерности в разпределението на геоданни и свързаните с тях пространствени обекти. В резултат на анализа на геоинформацията се получава качествено нова информация, която обогатява предишната информация.

Геопространственият анализ е ориентиран към дейностите свързани с повърхността на Земята, нейната обвивка, частите над и под земната повърхност. Времевият характер на анализа е насочен към миналото, настоящето и бъдещето, като се поставят въпроси като „къде", „кога", „защо", „как", „кой" и др. Методите на пространствения анализ са неограничени във времето и пространството.

Пространственият анализ се осъществява интерактивно между човека и компютъра, като се залага на човешката интуиция и експертните системи заложени в програмното осигуряване на компютъра.

В геоинформационните системи се използва картографско моделиране, което се използва за анализ на пространствените и тематични характеристики на геопространствените явления и обекти [1],[2].

При реализирането на геопространствения анализ се следва логическа последователност на дейности:

1. Представяне на проблема

При формулирането на проблема се задават целите на анализа и въпросите на които трябва да се отговори. Освен това е необходимо да се определи: типа и метода за анализ и способът за представяне на резултатите. На този етап се определят и критериите, които определят параметри-

те за използване на базата геоданни за получаване на отговори на запитванията.

2. Оценка на изходните данни

За да се получи качествена информация е нужно да се осигури качествено ниво на изходните геоданни. Оценката на изходните данни, които се съхраняват в базата геоданни е много важен етап от геопространствения анализ, с което се дава отговор на въпроса дали е възможно да се приложат избраните методи за анализ.

3. Избор на метод за анализ

Почти винаги са налице два или три метод за получаване на информация, която е необходима. Често даден метод е много бърз и дава приблизителна информация. Други могат да използват повече време и усилия за обработка но са по-точни. Избора на методът за анализ зависи от поставените проблеми и как ще се използват резултатите. Например ако се изпълнява оперативен анализ на геодинамиката на дадена територия за да се определят критичните участъци, ситуацията може да се оцени елементарно, като се изобразят на картата тези участъци. Ако информацията се готви, като доказателство за изготвяне на анализ, оценка и прогноза, тогава се придава по голяма тежест на точното обосноваване на местата където са регистрирани деформации в конкретен период от време, колко често те се случват и колко големи са щетите.

Освен избраният метод е необходимо да се построи и схемата на неговата реализация в ГИС. Резултатите от анализа могат да се представят във вид на карти, таблици и диаграми. Необходимо е да се реши каква информация е необходимо да се изведе на картата, как да се групират значенията за най-добро представяне на данните.

В процеса на оценката на резултатите може да се определи обективността и необходимостта от получената информация, да се вземе решение за повторение на анализа с други параметри или да се използва друг метод. ГИС позволява сравнително лесно да се направят необходимите изменения и да се получат нови резултати. Може оперативно да се сравнят резултатите от различните методи и да се оцени кой метод е най-точен.

При подбора на метода за анализ винаги е необходимо да се отговори на следните въпроси:

- *На какво да се заложи*: на *оперативност* или *точност на анализа*? Когато е необходимо бързо изпълнение на анализа, решение на задачата и да се вземе решение се прилага оперативен анализ. Когато е необходимо да се получат качествени резултати, които са валидирани и оценени се прилага точен анализ.
- *Какъв е модела на данните?* Когато се разполага с векторен модел на данните може точно да се съхрани местоположението на обекта, да се работи с дискретни обекти, граници и линии. При растерните модели на данни е целесъобразно да се използват данните за анализ на непрекъснати явления. Триангулачните мрежи се използват за анализ на повърхнини.
- *Какви са средствата за обработка на геоданните?* В съвременните геоинформационни системи има голямо количество аналитични средства за обработка на пространствени и атрибутни данни. Употребата на едни или други средства зависи от конкретната задача.

4. Обработка на данни

Когато е избран метода за анализ, необходимо е да се състави алгоритъм за реализацията му със средствата на ГИС. В повечето случаи анализа изисква прилагане на операции с множество слоеве. При работа с векторни данни е необходима информация от два входни слоя за формиране на един нов слой. Този слой може да се групира с трети слой за получаване на следващ промеждутъчен слой и т.н. При растерният модел на данни има възможност едновременно да се обработят няколко слоя чрез растерен калкулатор.

5. Оценка и изобразяване на резултатите

В процеса на оценка на резултатите се извършва интерпретация на резултатите. Ако е необходимо се извърши повторен анализ с друг метод или параметри, като това се реализира в среда ГИС лесно и бързо. Възможно е да се сравнят резултатите от различните анализи и да се подберат достоверни и точни резултати. Резултатите се представят във вид на: карти, диаграми, таблици, схеми и др.

2. Задачи на геопространствения анализ

Най-общите задачи на геопространствения анализ се представят като(*Анализ на местоположението на обектите* - (Mapping where things are) [3]. ГИС разполага със зададения пространствен обект съгласно въведените в компютъра данни по геодезически координати (B,L) или по проекционни координати (x,y). Картата често се използва, за да се види къде е разположен или как изглежда обекта. На картата нагледно се представя пространственото разположение на обектите, което позволява да се открият връзките между тях и по-добре да се възприеме изследваната област.

Анализът на местоположението помага да се определи областта, съответстваща на критериите или мястото, в което е необходимо да се вземат срочни мерки [4, 7].

Когато се открият местата на разположението на обектите, може да се започне да се установява причината за възникване на пространствените взаимовръзки. Ако картата е съставена правилно, на нея може да се видят определени закономерности в разпределението на данните. Ако се изобразява една категория може да се отбележи, че обектите са сгрупирани, разположени равномерно или разпръснати безпорядъчно. Определянето на закономерността на разпределение на обектите частично зависи от мащаба на картата. Увеличаването или намаляването на мащаба може да доведе до разпознаване на нови зависимости, които не са били различими преди това. Обектите от определена категория могат да се сгрупират или обединят с други обекти.

1. *Анализ на разпределението на числовите показатели* –(Mapping the most and least). ГИС изпълнява автоматизирано построяване на тематични картограми, както на всички така и само на избрани обекти.

На картата се нанасят обекти в съответствие с техните числени значения. За да се определят обектите, отговарящи на определени критерии, трябва да се определят местата им и да се установи закономерността на разпределение на количествените показатели на обектите. За да се нанесе на картата зададен числов интервал, това означава да се укажат обектите и количествените показатели, които се намират в неговите предели.

Изобразяването на обектите, основани на анализа на техните количествени показатели, добавя ново ниво на информация към информацията за местоположението им. Например, информацията за разположението на работниците може да е полезна за планирането на транспортните потоци.

При изобразяване на числовите показатели може да се определи видът на символа в зависимост от значението на атрибута на обекта. Числените показатели могат да бъдат представени количествено, с относителни величини, категории и рангове. Познаването на типа на числените показатели помага да се избере най-добрия способ за изобразяване на данните. Количеството и величината се явяват обобщени характеристики на обектите. Количеството (Count) означава фактическото число на обектите на картата. Величината (Amount) е обобщеното значение, което характеризира всеки обект. Използването на количеството или величините позволява числено да се съпоставят отделните обекти.

Количеството и величината може да се изобрази като дискретен обект, например броя на служителите във всяко предприятие и др. Ако се обобщават данни по площ, като се използват категориите „количество" и „величина" може да се получи разминаване с реалната закономерност на разпределение, ако размерите на областите много се различават. В тези случаи е по добре да се използват *отношения*. Например: може да се изобразят предприятията в зависимост от броя на служителите им, но не може да се покажат кварталите в зависимост от броя на работещите в тях хора, защото кварталите имат различни размери. Големите квартали имат голямо количество работници. За да се покажат обективно разпределенията, следва да се изчисли броя на работниците на квадратен километър.

Отношенията представят връзката между две величини и се образуват по пътя на делението на една величина на друга. Използването на отношението позволява да се изгладят резките различия между размерите на областите или количеството на обектите в тях така, че представя-

нето на разпределението на тези величини става разбираемо. Това свойство прави прилагането на отношението особено полезно при използването на обобщени по площ величини.

Най-известните относителни величини това са: *средното, отношението* и *средноквадратното отклонение*.

Средното значение е удачно да се приложи за сравнение на величини, характеризиращи дадено място. За да се получи средното значение е необходимо да се раздели сумарното значение на обектите на техния брой. Например броя на хората в даден район се дели на броя на домовете и дава средният брой на хората в един дом.

Отношението показва, каква част от цялото съставлява дадено количество. За да се изчисли отношението е необходимо да се разделят едномерни величини. Например делението на броя на 30 годишните жители, на даден район на броя на цялото население в района дава относителния брой на хората на възраст от 30 години в дадения район. Отношението (относителния дял) често се изразява в проценти (отношението се умножава по 100).

Средноквадратното отклонение е статистически показател, който определя величината на отклонението на всеки клас обекти от средноаритметичното за дадена извадка. Първоначално се определя средноаритметичното по формулата:

$$x = \frac{\sum_{i=1}^{n} x_i}{n} \quad (1)$$

където x –средноаритметично; x_i - i-тия обект, n – брой обекти.

Средноквадратното отклонение S се получава по формулата:

$$S = \sqrt{\frac{\sum_{i=1}^{n}(x_i - x)^2}{n-1}} \quad (2)$$

2. *Построяване на картографската плътност* - (Mapping density). Показателят за плътност представя степента на концентрация на обектите на дадена площ. За да се изчисли плътността е необходимо да се раздели значението на параметъра изразен с площ на цялата площ. Резултатът е количеството на единица площ. Например, разделянето на броя на населението на областта на нейната площ в квадратни километри. Получава се броят на хората на квадратен километър. Малките и големите райони могат да имат приблизително еднакво количество хора, но различна плътност.

За изобразяване на плътността на картата може да се използват цветни заливки на области – *повърхност на плътността*. Друг способ за изразяване на плътността е чрез *разпределение на дискретни обекти* по пътя на обобщението в условна точка. Всяка точка представлява указаното количество обекти и са разхвърлени случайно вътре в областта. Колкото по голяма е концентрацията на точките, толкова по голяма е плътността на реалните обекти в областта.

3. *Търсене на обекти вътре в областта* - (Finding what's inside). Извършва се автоматизиран разчет на разстояния, площи, периметър, буферни зони на обектите и др.

Обикновено се анализират обектите намиращи се в пределите на дадена област, за да се контролира произхода на събитията в нея или да се сравнят различните области на основание на тяхното съдържание. Когато се контролира пространството в пределите на областта се оценява адекватността за прилагане на мерки. Например, общинската администрация може да глоби нарушителите на реда, извършващи замърсявания в 1000 метровата санитарна зона около водоизточника.

Обобщението на обектите по признака за принадлежност към дадена област позволява да се сравнят територии по количествени критерии. Например, ръководството на полицията може да добави ежемесечната сводка за кражбите направени в различните райони на града, за да се контролират горещите точки.

За да се намерят обектите, попадащи вътре в областта, трябва да се нанесе границата на областта. След това може да се оцени попадат ли избраните обекти в областта.

Съществуват три метода за определяне на обекти в областта.

Таблица 1. Методи за определяне на обекти в областта

№	Метод	Кога се прилага	Типове обекти	Компромиси
1.	**Визуално съпоставяне на границата на областта и обектите**	За визуална оценка на обектите попадащи в областта.	Точки, линии, полигони, повърхности.	Бърз и прост метод, но визуалния подход не позволява да се оценят атрибутите на обектите.
2.	**Построяване на пространствено запитване**	За получаване на частични или общо обектите в областта.	Точки, линии, полигони.	Добър за оценка на съдържанието на една област, но не може едновременно да се анализират на няколко области.
3.	**Анализ по метода на налагането на слоеве.**	Количествена оценка на пълното или частично попадение на обектите в пределите на различни области.	Точки, линии, полигони, повърхности.	Ефективен за всички случаи, само че изисква големи усилия за реализация.

4. *Анализ на обкръжението* - (Finding what's nearby), ГИС автоматически определя съседството, отделяне на полигони, като позволява стъпка по стъпка да се оцени по установени критерии условията на местността.

Чрез ГИС може да се определи, какво се намира в пределите на установено разстояние от обекта или да се оцени диапазона на неговото пространствено изменение.

Таблица 2. Методи за анализ на обкръжението

№	Метод	Използва се за	Обекти	Измерват се	Преимущества	Недостатъци
1.	**Използване на крайно разстояние**	Определяне на областта на влияние около обекта, създаване на граница или избор на обекти в нейните предели	Точки, линии, полигони.	Дистанционно	Сравнително бърз и лек.	Дава само приблизително представяне за реалната дължина на пътя.
2.	**Измерване на разстояния или загуби по мрежата**	Измерване на дължини по пътя с отчитане на фиксирана инфраструктура.	Точки, линии.	Дължина на пътя или време за придвижване	Дава по точно представяне на фактическата дължина на пътя.	Изисква слой с мрежата на точните маршрути за придвижване.
3.	**Разчет на загубите по повърхността.**	Оценка загубата при придвижване по пресечена местност и диапазона на пространственото преместване на обектите.	Площен растер на повърхността.	Време за придвижване	Позволява да се комбинират няколко слоя за оценка загубата на време за придвижване по повърхността.	Изисква определена подготовка на данните за построяване на повърхността и загубите.

5. Анализ на пространствените изменения - (Mapping change).

На картата се нанасят измененията на явленията и обектите за да се прогнозират промени-

те, да се вземат решения за действия и оценка на резултатите от тези действия. По този начин динамиката на явленията и обектите може да се оцени и да се установят причините и бъдещото поведение.

Типовете изменения на пространствените обекти са на: *местоположението, геометрията и свойствата*. Отразяването на картата на местоположението на обекта дава възможност да се определи закономерността на неговото поведение и да се предвидят измененията на състоянието му. Измененията на размерите или свойствата на обекта дават възможност да се проследи как се изменят условията в дадено място. В резултат на отразяването на изменението на размера или свойствата на обектите, може да се определи мащаба и скоростта на изменението.

Съществуват три способа за нанасяне на измененията на картата: *създаване на временни редове, създаване на карта на проследяването и количествена оценка на изменението*.

Решението на тези задачи със средствата на ГИС и с други средства дават следните възможности [5, 6]:

- Да се обоснове местоположението на обектите с отчитане на пространствения фактор;
- Да се прогнозира развитието на явленията във времето;
- Да се намери оптималното трасе на комуникационния обект който се проектира;
- Да се определи оптималното място за разполагане на обект, като се определи икономическата ефективност;
- Да се оцени ефективността на действията на службите за сигурност и др.

Таблица 3. Анализ на пространствени изменения

№	Метод	Тип измерване	Модел на временните редове	Предимства	Недостатъци
1	Временни редове	Движение или изменение на свойствата	Тенденция Цикъл „до“ и „после“	Силен визуален ефект, при значителни промени; Отразява обекта във всеки момент от време	За потребител оценката на промените е достъпна само при визуално възприемане на картата.
2	Карта на проследяването	Движение	Тенденция Цикъл „до“ и „после“	По-лесно е да се види движението и слабите промени, отколкото при използването на временни редове.	Може да е трудно за възприемане при голям брой обекти.
3	Количествена оценка на изменението	Изменение на свойствата	Тенденция „до“ и „после“	Показва действителната разлика в количеството или значенията	Не отразява валиден условия във всеки момент от време, сравнява само между две дати

Заключение

Геоинформационните системи позволяват да се решат информационно-справочни задачи свързани с търсенето и уточняването на местоположението и характеристиките на пространствените обекти.

Другите задачи са свързани с анализа, моделирането и прогнозирането на природни и техногенни процеси. Решението на тези задачи позволява в нагледна и удобна картографска форма да се получи обобщена или детайлна геопространствена информация.

References

1. Андреев, А. Андреева П. Геоинформатика, геоинформационни системи, геоинформационни технологии. НВУ “В. Левски“ В. Търново 2021. ISBN 987-619-7531-24-4
2. Андреев А. Марков М. Географски информационни системи. НВУ“В. Левски“ – Шумен, 2009 г 190 с.
3. Беджева М., Т. Игнатова, Analysis of the accuracy of geodesical maps prepared by the means of UAVs, Proceedings of university of Ruse – 2019, volume 58 (на български), ISSN 2603-4123 (on-line)
4. Митчелл Энди. Руководство по ГИС Анализу. Часть 1: Пространственные модели и взаимосвязи / Энди Митчелл; пер. с англ. – Киев, ЗАО ECOMM Co; Стилос, 2000. – 198 с.):
5. Прокопов Я. Възможности на наземното лазерно сканиране – основа за геодезическо моделиране. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2021, Faculty of Artillery, Air Defense and Communication and Information Systems.
6. Прокопов Я. Сателитната радарна интерферометрия като алтернатива за някои задачи от приложната геодезия. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2021, Faculty of Artillery, Air Defense and Communication and Information Systems.
7. Якубайлик О.Э Методы и приемы пространственного анализа в геоинформационных системах: Учебное пособие / Красноярск: Издательство Крас ГУ, 2001

RASTER ANALYSIS IN GEOINFORMATION SYSTEMS

Petina A. Andreeva

Department Artillery and Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levsky" petiand@abv.bg

Abstract: *With the help of raster models in GIS, construction of surfaces such as relief, temperature distribution, etc. is performed. The surfaces contain a variety of information that can be used to prepare spatial analysis e.g. DTM construction, slope and exposure estimates, etc.*

Key words: *Relief, Digital maps, map projection, DTM.*

РАСТЕРЕН АНАЛИЗ В ГЕОИНФОРМАЦИОННИТЕ СИСТЕМИ

Петина А. Андреева

1. Въведение

С помощта на растерните модели в ГИС се изпълнява построяване на повърхности например релеф, разпределение на температурата и др. Повърхностите съдържат разнообразна информация, която може да послужи за изготвяне на пространствен анализ например построяване на ЦМР, разчет на наклона и експозицията и др.

2. Видове растерни анализи

На практика при решаването на геозадачи с растерния модел се изпълняват следните видове анализи [1],[2]:

- *Анализ на повърхнини*

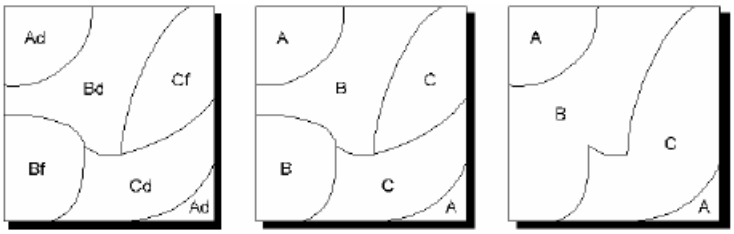
За анализа на повърхнини на растерния модел се включват: функции за построяване на изолинии, показва се местоположения с еднакви значения, функция за изчисляване на наклона, функция за определяне на експозицията на слоновете, функции за определяне на оттичането на водата по релефа и др.

- *Интерполация на растера*

Интерполацията позволява да се изчисли значенията за всяка клетка на растера по значението на ограничен брой точки. Това може да се използва за прогнозиране значението на произволни данни – височина, количеството на валежите, концентрацията на химическите вещества, нивото на шума и др. Използваните методи за интерполация са: обратни тежести на разстоянията, крекинг, сплайн и др. [3].

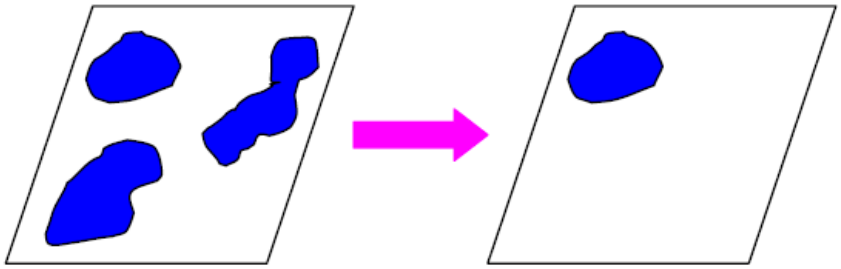
- *Прекласификация на растера*

Прекласификацията е аналитична операция, която преобразува картния слой по зададени условия. При класификация на еднородни почви без допълнителни подробности се получава:



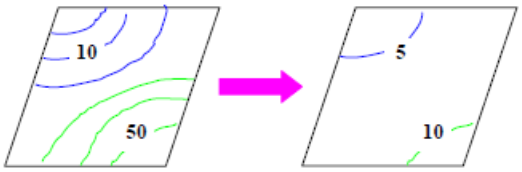
Фиг. 1. Аналитическа операция за прекласификации на почви

Друга операция е отсичане на обекти, на които пространственото положение не съответства на зададените позиции:



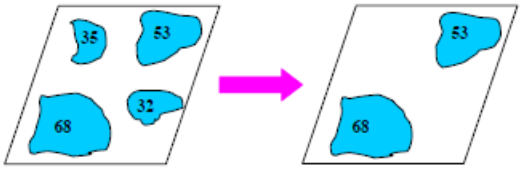
Фиг. 2. Позиционна прекласификация

Следващата прекласификация е на някаква величина от една дименсия в друга:



Фиг. 3. Прекласификация на височините на топографската карта от футове в метри

Прекласификацията на обектите по зададен размер е често срещана задача (отпадане на области с размер по-малък от величината A):



Фиг. 4. Прекласификация по размер на обекта по малък от 50 км^2

- *Картиране на плътността*

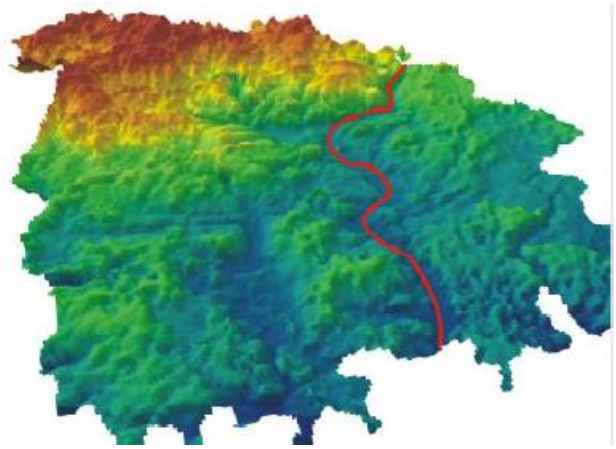
Изчисляването на плътността на разпределението е полезно, когато е необходимо да се покаже концентрацията на точкови и линейни обекти.

- *Картиране на разстояния*

Обикновено растерните данни, които са получени в резултат на функцията картиране на разстояния, се използват за изчисляване на минималния по стойност път, като се отчитат ограниченията.

- *Ранговка*

Ранговката позволява да се подредят обектите в интервала от високото към ниското или обратно. Рангът е полезен, когато преките измервания са затруднени или количествената характеристика зависи от редица фактори. За да се укаже ранга, може да се използват описателни признаци (висок, нисък) или числа (от 1 до 10). Рангът често се присвоява на основния атрибут на обекта (тип, клас) или комбинация от атрибути.



Фиг. 5. Избор на оптимален път върху растерен модел

- *Мрежови анализ*

Мрежовият анализ позволява да се решат различни задачи на пространствените мрежи, свързани с линейни обект (реки, пътища, проводи и др.)

Отчитането на типа на мрежата и особеностите на техните съединения са важни за провеждане на пространствения анализ. Обикновено мрежовия анализ е предназначен за задачи за откриване на най-близкия път, определяне на нивото на натоварване на мрежата, за определяне на зоните на влияние на обектите от мрежата на други обекти и др. С участъците на мрежата са свързани понятия, като направление на движение, данни за което се съхраняват в БД. Други данни са мощност на потока, временните интервали и др.

Обикновено функциите на мрежовия анализ се реализират допълнителни и пълнофункционални ГИС. За системата ArcView GIS това е модула Network Analysis, а за GeoMedia Professional – GeoMedia Network [5],[6].

3. Технология на решаване на задачите при растерния анализ

При решаването на задачите на растерният анализ се извършва [4], [7]:

- ✓ Търсене на близък пункт за обслужване;
- ✓ Избор на най-кратък маршрут;
- ✓ Подготовка на маршрута за придвижване;
- ✓ Определяне на зоната на обслужване и др.

В геоинформационните системи за осъществяване на пространствения растерен анализ се отправят *запитвания* към системата. По принцип, като се изходи от структурата на обектите и тяхното разположение в слоеве по класове, запитванията се формират по два способа:

1. Запитвания с използване на пространствени функции;
2. Запитвания с използване на пространствени оператори.

При първият способ се анализират пространствените характеристики на обектите. Всяка пространствена характеристика от скаларен тип може да се представи във вид на функции, аргументите на които се явяват пространствения обект, а значението на функциите определя пространствената характеристика на този обект. Типични пространствени функции са:

- *Координатите X и Y (обект)* – като отговор на запитването връщат значението на координатите *X и Y* на точков обект;
- *Площ (обект)* – изчислява се значението на площта на площен обект;
- *Периметър (обект)* – изчислява се периметъра на площен обект;
- *Дължина (обект)* – изчислява се значението на дължината на линеен обект;
- *Разстояние (обект1, обект2)* – изчислява се разстоянието между два обекта.

Общият вид на запитването с използване на пространствени функции може да се представи така:

Намери обект от множество обекти, къде <пространствена функция>, <оператор за сравнение>, <числово значение>.

Пример на запитване с използване на пространствени функции:

- ✓ *Намерете езеро с площ по голяма от 100 км^2 – функция <площ>.*
- ✓ *Намерете път с дължина не по малка от 10 км –функция <дължина>.*
- ✓ *Намерете магазините, които са отдалечени от станцията на метрото не повече от 500 м – функция <разстояние>.*

В повечето съвременни ГИС такива пространствени функции се изпълняват в явен вид при формиране на запитванията.

При втория способ се използват пространствени оператори. В тези запитвания се анализират пространствените отношения между обектите, които още се разглеждат като бинарни отношения. Общата форма на пространственото запитване с използване на пространствени оператори изглежда така:

- ✓ *Намери обекти от множество А, които се намират в отношение <пространствен оператор> с обекти от множество В.*
- ✓ *Намери държави, които имат излаз на море – оператор <граничи с>.*
- ✓ *Намери път, който се пресича с ж. п. линия – оператор <пресичане>.*
- ✓ *Намери район, на територията на който има лозови масиви – оператор <съдържа в себе си>.*

В ГИС се срещат два варианта за формиране и изпълнение на запитвания: *интерактивно приложение на инструменти за избор и използване на построител на запитвания (чрез диалог с програмата).*

При *интерактивно прилагане на инструменти* се използват инструменти, които са внедрени в ГИС като:

- ✓ *Избор* – осъществява търсене на обекти, съдържащи в себе си търсената точка (оператор <съдържа в себе си>).
- ✓ *Избор в правоъгълник* – осъществява се търсене на обект, който се намира вътре в областта на правоъгълника (оператор <съдържа се в>).
- ✓ *Избор в радиус* - осъществява се търсене на обект, който се намира вътре в окръжността (оператор <съдържа се в>).
- ✓ *Избор в полигон* - осъществява се търсене на обект, който се намира вътре в полигона (оператор <съдържа се в>).
- ✓ *Избор на пресечница* - осъществява се търсене на обект, който пресича друг обект (оператор <пресича се>).

При *използване на построител на запитване* се осъществява във вид на диалогов прозорец. При използване на пространствени функции, ползвателя задава множеството обекти, които подлежат на анализ, задава се оператора за сравнение и числовото му значение. При използване на пространствени оператори ползвателя задава първото множество от обекти, оператора и второто множество от обекти. Множеството от обекти може да съответства на един слой от картата или на определена извадка от слоя, извършена от ползвателя.

В ГИС се реализират основно два типа езици на запитвания*: QBE и SQL*.

QBE запитването е запитване по образец. Образеца представлява таблица със запитвания и съдържа един или няколко реда и толкова колони колкото са основанията за построяването на запитването. Запитването позволява да се търсят данни в атрибутната таблица по някакви условия. Ако е необходимо да се изберат от таблицата записи на данни с определено значение, то това значение се въвежда в съответното поле.

QBE езика, предоставя възможност най-бързо и ефективно да се изрази логическо условие, по което е необходимо да се подберат елементите на обектите. Затова за релационната база дан-

ни, с достатъчно проста структура, за връзка между таблиците този език е за предпочитане от ползвателя. Всеки от атрибутите на обекта характеризира типа на данните, които той представлява и те се свеждат до: числов тип, текст, дата и комбинация от предходните.

Оператори на QBE –запитване:

- Аритметически оператори;
- Оператори за сравнение;
- Оператори за заменяне;
- Специални оператори;
- Статистически оператори.

SQL запитването се формира с помощта на езика за запитване, който се изразява в условията на търсенето.

Езикът SQL (*Structured Query Language)* се използва за анализа на релационна база данни, като при запитването е необходимо да се избере атрибутна таблица с данни. Използва се СУБД (MS ACCESS, Oracle, Sybase, Paradox), като механизъм, който ще се използва за съставяне на запитването. Основните конструкции на SQL езика са: SELECT, FROM, WHERE, ORDER WY, HAVING, операции за агрегация: SUM, AVG, MIN, MAX, COUNT и операторите: +, -, *, /, +, <, >, IS NULL, INSERT, UPDATE, DELETE.

4. Заключение

Растерният анализ в геоинформационните системи е особено полезен при обработката на данните от дистанционното сондиране на Земята. Тези данни са актуални и дават възможност след прилагане на анализ да предложат оперативни решения при нормални и екстремни ситуации. Този анализ подпомага действията на кризисните щабове при бедствия, аварии и катастрофи.

References

1. Андреев, А. Андреева П. Геоинформатика, геоинформационни системи, геоинформационни технологии. НВУ “В. Левски“ В. Търново 2021. ISBN 987-619-7531-24-4
2. Андреев А. Марков М. Географски информационни системи. НВУ“В. Левски“ – Шумен, 2009 г 190 с.
3. Беджева М., Т. Игнатова, Analysis of the accuracy of geodesical maps prepared by the means of UAVs, Proceedings of university of Ruse – 2019, volume 58 (на български), ISSN 2603-4123 (on-line)
4. Митчелл Энди. Руководство по ГИС Анализу. Часть 1: Пространственные модели и взаимосвязи / Энди Митчелл; пер. с англ. – Киев, ЗАО ЕСОММ Со; Стилос, 2000. – 198 с.):
5. Прокопов Я. Възможности на наземното лазерно сканиране – основа за геодезическо моделиране. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2021, Faculty of Artillery, Air Defense and Communication and Information Systems.
6. Прокопов Я. Сателитната радарна интерферометрия като алтернатива за някои задачи от приложната геодезия. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2021, Faculty of Artillery, Air Defense and Communication and Information Systems.
7. Якубайлик О.Э Методы и приемы пространственного анализа в геоинформационных системах: Учебное пособие / Красноярск: Издательство Крас ГУ, 2001

AGAIN, THE DILEMMA ARISES TO CREATE A MODEL OF GEOID OR QUASIGEOID

Andrey I. Andreev

Department Artillery and Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levsky" andreev_an@abv.bg

Abstract: *The Republic of Bulgaria with the introduction of BGS 2005 defines the use of the normal heights system aligned to the Amsterdam High Altitude (NAL) and the European High Reference System (EVRS), which is a zero-tide system. The high components are the differences between the potential of the Earth's gravitational field and the potential of conventional zero EVRS start. The potential difference is the geopotential number. Very often in the area where GNSS measurements are carried out after determining the geodetic height, there is a need for an immediate calculation of the normal height of the points on the physical ground. This requires the appropriate transformational formulae to be applied and transformation coefficients to be produced to solve the problem, albeit locally.*

Key words: *normal heights system, zero-tide system, EVRS, NAL, geoid, quasigeoid*

ОТНОВО ВЪЗНИКВА ДИЛЕМАТА ЗА СЪЗДАВАНЕ НА МОДЕЛ НА ГЕОИД ИЛИ КВАЗИГЕОИД

Андрей И. Андреев

1. Въведение

В Р България с въвеждането на БГС 2005 се дефинира използването на системата нормални височини приведени към Амстердамският височинен пегел (Normal Amsterdam Level (NAL)) и Европейска височинна референтна система (EVRS), която е нулево-приливна система (zero – tide system). Височинните компоненти са разликите между потенциала на земното гравитационно поле и потенциала на конвенционалното нулево EVRS начало. Потенциалната разлика е геопотенциалната кота (geopotential number) [2, 3].

Много често в района, където се извършват ГНСС измерванията след определяне на геодезическата височина възниква необходимост от непосредствено изчисляване на нормалната височина на точките от физическата земна повърхност. Това налага да се приложат подходящите трансформационни формули и да се изведат трансформационни коефициенти, с които да се реши проблемът макар и локално. В сайта на Агенцията по геодезия, картография и кадастър е поместен софтуер BGSTrans с който се извършва трансформацията.

2. Трансформация на височини

Трансформирането на височините в приетата за РБългария височинна система се осъществява по два начина [1]:

1. Ако се разполага с модел на геоида (квазигеоида)

Ондулацията (N) или аномалията на височината (ζ) се отчита от модела на геоида (квазигеоида) с аргументи координатите (*B, L*) на точките, определени с ГНСС. Условието е всички измервания да са в единна референтна система GRS80 (WGS84). Отчетените аномалии е необходимо да съответстват по точност на височинните определения с ГНСС, а тези от разликите между аномалиите на съседните точки - на елипсоидните превишения, определени с ГНСС. Нормалните височини се определят от формули (1) и (2).

$$H^{\Gamma} = H^{o} + N \tag{1}$$

$$H^{\Gamma} = H^{N} + \zeta \tag{2}$$

2. Ако липсва модел на геоида (квазигеоида)

а) Ондулацията (N) или аномалията на височината (ζ) се изчислява по формулите:

$$N = H^{\Gamma} - H^{o} \tag{3}$$

$$\zeta = H^{\Gamma} - H^{N} \tag{4}$$

H^{o}, H^{N} се получават от геометричната (тригонометрична) нивелация или се отчитат от цифровия модел на релефа с необходимата точност.

б) Ондулацията (N) или аномалията на височината (ζ) за изследвания район може да се интерполира числено и да се получи в новите точки .

За трансформационните изчисления са необходими повече от 4 точки, в които са известни аномалиите, за да се определят трансформационните коефициенти. Районът не трябва да надвишава 10 km^2, да е равнинен или хълмист.

Численото интерполиране се осъществява по формулите:

$$H^{\Gamma} = H^{N_0} + c_0 + c_1\varphi + c_2\lambda \tag{5}$$

$$H^{\Gamma} = H^{N_0} + c_0 + c_1\varphi + c_2\lambda + c_3\varphi^2 + c_4\varphi.\lambda + c_5\lambda^2 \tag{6}$$

т.е. повърхнинен интерполационен модел от първа и втора степен или повърхнинен интерполационен модел от трета и четвърта степен:

$$H^{\Gamma} = H^{N_0} + c_0 + c_1\varphi + c_2\lambda + c_3\varphi^2 + c_4\varphi.\lambda + c_5\lambda^2 + c_6\varphi^3 + c_7\varphi^2\lambda + c_8\varphi\lambda^2 + c_9\lambda^3 \tag{7}$$

$$\begin{aligned} H^{\Gamma} = H^{N_0} &+ c_0 + c_1\varphi + c_2\lambda + c_3\varphi^2 + c_4\varphi.\lambda + c_5\lambda^2 + c_6\varphi^3 + c_7\varphi^2\lambda + c_8\varphi\lambda^2 + \\ &+ c_9\lambda^3 + c_{10}\varphi^4 + c_{11}\varphi^3\lambda + c_{12}\varphi^2\lambda^2 + c_{13}\varphi\lambda^3 + c_{14}\lambda^4 \end{aligned} \tag{8}$$

От (5), (6), (7) и (8) може да се запише уравнението на поправките за всяка точка с известни H^{o} и H^{N}, т.е. поправките за аномалията на височината V_{ζ}.

$$V_{\zeta} = c_0 + c_1.\varphi + c_2.\lambda + ... + f_{\zeta} \tag{9}$$

където: V_{ζ} - поправка към аномалията на височината;

$c_0, c_1, c_2, \ldots$ - коефициенти на модела;

f_ζ - свободен член, разлика между приблизителната и „измерената” стойности на аномалията на височината.

След извеждане на трансформационните коефициенти $c_0, c_1, c_2, c_3, c_4, c_5, \ldots$ по МНМК за изследвания район се получават аномалиите на останалите точки от района:

$$H_i^{\Gamma} = H_i^{N_0} + c_0 + c_1\varphi_i + c_2\lambda_i + c_3\varphi_i^2 + c_4\varphi_i.\lambda_i + c_5\lambda_i^2 + \ldots \quad (10)$$

Оценката на точността от изравнението се получава по формулата:

$$m = \sqrt{\frac{[\Delta^2]}{n-u}} \quad (11)$$

където: n – общият брой на уравненията;

u – броят необходими уравнения.

При този повърхнинен интерполационен модел когато се увеличава степента, може да се явят някои неудобства, като: различни стойности на неизвестните коефициенти в сравнение с предходните, точността на коефициентите да намалява, броят на излишните елементи да намалява и да се получи погрешна представа за точността на модела и др.

Критерий за правилния подбор на степента на повърхнинен интерполационен модел е условието, че ако с увеличаване на степента се запазват стойностите, и точността на коефициентите се запазва спрямо предходните.

Чрез прилагане на метода на Чебишев, посредством линейни комбинации от избраните функции се определят нови функции, от които се образува нов повърхнинен интерполационен модел. Този подход дава възможност изчисленията да започнат от ниска степен и след това тя да се увеличава докато абсолютната стойност на поправките стане по-малка от пределната грешка, т.е. $|v_i| < \Delta_{пред}$.

Може да се използва диференциален геометричен трансформационен модел за получаване на разликата между Стоксовия гравиметричен геоид и ГНСС/нивелация геоид.

Абсолютният (точков) параметричен модел има вида:

$$H_i^{\Gamma} - H_i^{o} - N_i = l = c_i^t.x + v_i \quad (12)$$

където: c_i^t - вектор на известните коефициенти;

x - вектор на неизвестните параметри;

v_i - абсолютно остатъчно отклонение.

В това моделиране остатъчното отклонение ν се явява показател за точността на ГНСС, нивелачните и геоидни случайни грешки. Конкретно за ν може да се състави стохастичен модел:

$$c_i^t x = \cos\varphi_i.\cos\lambda_i.x_1 + \cos\varphi_i.\sin\lambda_i.x_2 + \sin\varphi_i.x_3 + x_4 \quad (13)$$

$$c_i = \begin{bmatrix} \cos\varphi_i.\cos\lambda_i \\ \cos\varphi_i.\sin\lambda_i \\ \sin\varphi_i \\ 1 \end{bmatrix} \quad , \qquad x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \tag{14}$$

Диференциалните тригонометрични трансформации може да се приложат в следния вид:

$$\begin{aligned} dH_i^{\Gamma} = dN_i = &-\cos\varphi_i.\cos\lambda_i.dX_0 - \cos\varphi_i.\sin\lambda_i.dY_0 - \sin\varphi_i.dZ_0 - \\ &- \frac{\sin\varphi_i.\cos\varphi_i.\cos\lambda_i}{\sqrt{1-e^2.\sin^2\varphi_i}} e^2 a.d\omega_y + \frac{\sin\varphi_i.\cos\varphi_i.\sin\lambda_i}{\sqrt{1-e^2.\sin^2\varphi_i}} e^2 a.d\omega_x - \\ &- (a.\sqrt{1-e^2.\sin^2\varphi_i}).ds - \frac{1-\alpha^2\sin^2\varphi_i}{\sqrt{1-e^2.\sin^2\varphi_i}}.da - \frac{\sin^2\varphi_i}{\sqrt{1-e^2.\sin^2\varphi_i}} a.\sqrt{1-e^2}\,d\alpha \end{aligned} \tag{15},$$

където: a, α, e - параметри на референтния елипсоид;

$\omega_x, \omega_y, \omega_z$ – малки ъгли на ротация.

Повърхнинният тригонометричен модел може да се запише по следния начин:

$$\begin{aligned} H_i^{\Gamma} - H_i^o - N_i = &\cos\varphi_i.\cos\lambda_i.x_1 + \cos\varphi_i.\sin\lambda_i.x_2 + \sin\varphi_i.x_3 + \\ &+ \frac{\sin\varphi_i.\cos\varphi_i.\cos\lambda_i}{\sqrt{1-e^2.\sin^2\varphi_i}} x_4 + \frac{\sin\varphi_i.\cos\varphi_i.\sin\lambda_i}{\sqrt{1-e^2.\sin^2\varphi_i}} x_5 - \\ &+ ((a.\sqrt{1-e^2.\sin^2\varphi_i}) + H_i^{\Gamma}).x_6 + \frac{1-\alpha^2\sin^2\varphi_i}{\sqrt{1-e^2.\sin^2\varphi_i}}.x_7 + \frac{\sin^2\varphi_i}{\sqrt{1-e^2.\sin^2\varphi_i}} x_8 \end{aligned} \tag{16}$$

Представеният повърхнинен тригонометричен модел дава възможност за преход от определените с ГНСС геодезически височини към нормални височини и създава условия за изключване на случайните грешки.

От анализа на резултатите, получени с интерполационните полиноми от втора и по-висока степен се получават сравнително добри точности, но те не решават проблемите в по-големи райони. И в двата модела за преобразуване на височинните измервания, реализирани с ГНСС, в подходяща височинна система, ясно се очертава необходимостта от наличието на локален модел на геоида в изследваната област [4, 5].

У нас, при възприетата съгласно теорията на Молоденски нормална височинна система, по-често се прибягва до построяване на модел на квазигеоида. В първокласните нивелачни репери и определени точки от ДГМ на базата на прецизна геометрична нивелация се разполага с нормалните им височини. Нормалните височини на повечето точки от ДГМ и ГММП са определени чрез тригонометрична нивелация със съответната точност, вариращa до няколко сантиметъра. Следователно използването на съответните нормални височини на точките като изходни данни ще окаже влияние върху точността на модела на геоида (квазигеоида) [6].

3. Статистически анализ

Предложените модели е необходимо да се подложат на статистически анализ с цел да се провери за наличието на систематически грешки, наличието на груби грешки, законът на разпределение на резултатите от моделирането и техните грешки [7], [8].

1. За определяне на постоянната грешка в резултатите от моделирането се изчислява средното аритметическо значение от разликите $N_{mod} - N_{ГНСС}$. Изчислява се :

$$\Delta = \bar{x} - a \quad , \tag{17}$$

където: $\bar{x}$ - средноаритметично от разликите;

a - разликата между двете ундулации.

Критерий на проверката и приемане на статистиката е условието:

$$\frac{|\Delta|}{M} \le z_q \, , \tag{18}$$

където: M – е средната квадратна грешка на средно аритметическото;

q – ниво на значимост обикновено q=0.05;

z_q – се определя по Стюдент с q и k=n-1 (степен на свобода).

2. Определяне на пределните грешки и бракуване на някой резултати.

При извършването на моделирането се налага да се отделят резултати, рязко отличаващи се от основната маса. Това може да е предизвикано като следствие от нарушаване на условията или на груби грешки на моделирането.

Ако σ е средноквадратното отклонение на резултатите от моделирането, то пределната допустима стойност на грешката при зададено ниво на значимост q е:

$$d_{доп} \le z_q \sigma \tag{19}$$

Може да се постави условието пределните грешки да не надвишават 2σ, 2.5σ или 3σ.

Може да се използва и критерият на Гребс за премахване на грубите грешки:

$$z = \frac{x_{\max} - \bar{x}}{\sigma} \, , \tag{20}$$

където x_{max} - е най-голямата разлика.

Критическата област се определя по формулата:

$$z > z_q \tag{21}$$

3. Проверка за нормално разпределение на резултатите от моделирането и техните грешки.

а) Проверка с помощта на асиметрията и ексцеса

Проверката на нулевата хипотеза се изпълнява, като се определи асиметрията $S(x)$ и ексцеса $E(x)$ по формулите:

$$S(x) = \frac{1}{n\sigma^3} \sum_{i=1}^{n} (x_i - \bar{x})^3 \quad , \tag{22}$$

$$E(x) = \frac{1}{n\sigma^4} \sum_{i=1}^{n} (x_i - \bar{x})^4 - 3 \, . \tag{23}$$

Емпирическите дисперсии на асиметрията и ексцеса се получават по формулите:

$$m^2(S) = \frac{6(n-1)}{(n+1)(n+3)}, \quad (24)$$

$$m^2(E) = \frac{24n(n-2)(n-3)}{(n+1)^2(n+3)(n+5)}. \quad (25)$$

Разпределението е нормално, ако са изпълнени условията:

$$|S(x)| \le 3m(S) \quad и \quad |E(x)| \le 5m(E). \quad (26)$$

В противен случай хипотезата се отхвърля или се смята за съмнителна.

б) Когато разликите са много на брой, за проверката на нулевата хипотеза се използва критерият на Колмогоров или критерия на Пирсан (χ^2).

- Критерий на Колмогоров

$$\lambda = D\sqrt{n}, \quad (27)$$

където: λ - величина на Колмогоров;

D – максимална стойност на разликата между теоретическата и емпирическата функция на разпределение;

n - брой на разликите.

Критерий за нормално разпределение е:

$$\lambda > \lambda_q \quad (28)$$

където λ_q е от таблица на Колмогоров с аргумент q.

- Критерий на Пирсън (χ^2)

$$\chi^2 = \sum_{i=1}^{l} \frac{(n_i - np_i)^2}{np_i}, \quad (29)$$

където: l - брой на интервалите;

$k = l - 3$ - степен на свобода;

n – брой на разликите,

n_i – брой на разликите в i –тия интервал;

p_i – вероятност за попадение в i –тия интервал.

Ако е изпълнено условието $\chi^2 \ge \chi_q^2$, хипотезата за нормално разпределение се отхвърля. χ_q^2 се получава от таблица по q и k.

При изследванията е необходимо да се покаже графиката на нормалната (Гаусова) крива, както и хистограмата на разпределението на разликите от модела.

Заключение

От физическа гледна точка избора на геоида за референтна повърхнина при височинното определяне на точките от физическата повърхнина е по-правилен подход. Въпреки проблемите които възпрепятстваха създаването на модела на геоида в глобален и регионален мащаб в близкото минало днес съвременните технологии позволяват той да се дефинира с достатъчна точност за нуждите на геодезията. Много страни във света използват успешно геоида и системата ортометрични височини, като се използват геопотенциалните коти. Създадоха се глобални модели на геоида, които намират приложение в практиката, а някои успешно се въвеждат в софтуера на съвременните ГНСС приемници под формата на модели.

Acknowledgments

This paper is written thanks to project BG05M2OP001-2.016-0003 “Modernization of Vasil Levski National Military University – Veliko Tarnovo and Sofia University “St. Kliment Ohridski” – Sofia in professional direction 5.3 Computer and communication technology”, financed by the operational program “Science and education for intelligent growth”.

References

1. Андреев А. Съвременни методи за локално моделиране на геоида. ВТС, НВУ „В. Левски“, Шумен, 2008 г.

2. Андреев А., Андреева П. Анализ на системите височини от гледна точка на физическата геодезия и приложението им в РБългария. 10 стр. Сборник научни трудове ФТН - „Геодезия” ШУ”Еп. К. Преславски” 2010.

3. Андреев А., Андреева П. Локално моделиране на геоида за територията на Североизточна България. 15 стр. Сборник научни трудове ФТН - „Геодезия” ШУ ”Еп. К. Преславски” 2010.

4. Андреева П., Димова Г., Андреев А. Приложение на ГИС и ГНСС в навигацията. Proceedings of International Scientific Conference 2021, Faculty of Artillery, Air Defense and Communication and Information Systems - Shumen. 511 - 517 p. ISSN 2367-7902

5. Андреева П., Андреев А. Върху проблемите на геоинформационните технологии у нас. Proceedings of International Scientific Conference 2021, Faculty of Artillery, Air Defense and Communication and Information Systems - Shumen. 492- 502 p. ISSN 2367-7902

6. Прокопов Я. Сателитната радарна интерферометрия като алтернатива за някои задачи от приложната геодезия. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2021, Faculty of Artillery, Air Defense and Communication and Information Systems.

7. Andreeva P., Iliev M. Theoretical basis of a methodology for conducting empirical sociological studies on the efficiency of operation of the cadaster information system. PROCEEDINGS OF UNIVERSITY OF RUSE - 2020, volume 59. Copyrights© 2020 ISSN 1311-3321 (print), ISSN 2535-1028 (CD-ROM), ISSN 2603-4123 (on-line). ISSN 2367-7902

8. Andreeva P. Technology for applying a methodology for conducting empirical sociological surveys of the effectiveness of the cadaster information system. PROCEEDINGS OF UNIVERSITY OF RUSE - 2020, volume 59. Copyrights© 2020 ISSN 1311-3321 (print), ISSN 2535-1028 (CD-ROM), ISSN 2603-4123 (on-line). ISSN 2367-7902

AN APPROACH TO INCREASE THE ACCURACY OF PHOTOGRAMMETRIC MEASUREMENTS IN THE ENVIRONMENT OF AGISOFT METASHAPE PROFESSIONAL

Dimitar D. Petrov

Department Artillery and Geodesy, Air Defense and Communication and Information Systems faculty - Shumen / NMU "Vasil Levsky" petrov_2@abv.bg

Abstract: *The use of digital photogrammetry based on aerial photographs obtained with the help of Unmanned Aerial Vehicles is no longer something unknown and inaccessible to a certain part of modern surveyors.*

In the periodical press and in reports of scientific conferences [31], [42], [2]there are a number of publications providing information on successfully completed tasks related to the use of this technology.

Today, most surveyors know about the usefulness of such aerial assistants, also called drones or flying robots. Their added value was also greatly appreciated in the surveying industry – a trend was born and a race began for the best performance, accuracy and innovative software and control solutions. In addition, the integration between classical linear-angular measurements, UAVs, digital photogrammetry and high-precision GNSS technology is increasingly becoming an important basis for creating a complex almost universally applicable technology for solving a wide range of geodetic tasks.

Key words: *digital photogrammetry, accuracy, point cloud.*

ЕДИН ПОДХОДА ЗА ПОВИШАВАНЕ ТОЧНОСТТА НА ФОТОГРАМЕТРИЧНИТЕ ИЗМЕРВАНИЯ В СРЕДА НА AGISOFT METASHAPE PROFESSIONAL

Доц. д-р инж. Димитър Петров

1. ВЪВЕДЕНИЕ

Използването на цифрова фотограметрия базирана на аерофотоснимки добити с помощта на Безпилотни Летателни Апарати за определена част от съвременните геодезисти вече не е нещо непознато и недостъпно.

В периодичния печат и в доклади на научни конференции [1], [2], [3], [4] се срещат редица публикации предоставящи информация за успешно изпълнени задачи свързани с използването на тази технология.

Днес голяма част от геодезистите знаем за полезността на такива помощници от въздуха, наричани още дронове или летящи роботи. Тяхната добавена стойност също беше значително оценена в геодезическата индустрия – роди се тенденция и започна надпревара за най-добро представяне, точност и иновативни софтуерни и контролни решения. В допълнение, интеграция-та между класическите линейно-ъглови измервания, БЛА, цифрова фотограметрия и високо

прецизна ГНСС технология все по-вече се превръща във важна база за създаване една комплексна почти универсално приложима технология при решаване на голям кръг геодезически задачи.

Това все по-масово навлизане на БЛА в геодезическата практика е обусловено от редица икономически и технологични предпоставки, като на последно място тях е почти пълното автоматизиране на производствения процес. Това важи особено за случаите когато БЛА е снабден с високо точна система RTK позволяваща определяне на част от елемнтите на външно ориентиране на а.ф.с. още по време на полета и елиминираща необходимостта от маркиране и координатно определяне наземни опорни GCP точки.

От друга страна, всички съвременни софтуерните продукти за цифрова фотограметрична обработка такива като Agisoft Metashape, Pix4Dmapper, 3DF Zephyr Aeria, PhotoModeler Technologies и много други, осигуряват висока степен на автоматизация на производствения процес, включително натройка на Batch процеси за изпълнение (Agisoft Metashape).

Всички тези обстоятелства на пръв поглед свеждат цифровата фотограметрия до една обикновена съвкупност от последователно изпълнение на строго регламетирани изчислителни процеси. Това като че ли е предпставката тази технология да е лесно достъпна и за хора без специално геодезическо образование и специализация, а притежаващи единствено средна компютърна грамотност.

Възприемането на такъв подход обаче, води до „сляпото“ прилагане на стандартните изчислителни обработки и процедури, заложени в използвания фотпграметричен софтуер. Това в комбинация с непознаването на теорията на геодезиятя и още по-вече на фотограметрията в нейната същност води до невъзможността за добиването на геопространствени данни притежаващи точност, които чрез сатндартно заложените в софтуерния продукт изчислителни процедури не могат или трудно могат да бъдат получени.

Обект на настоящото изложение е представяне на един подход в използването на софтуерния продукт Agisoft Metashape, с помощта на който и опирайки се на теорията на стереофотограметрията и по специално правата фотограметрична засечка можем да получим резултати в геопространственото определяне на точки от местността с изключително висока точност.

2. КРАТКА ТЕОРИЯ ЗА ПРАВАТА ФОТОГРАМЕТРИЧНА ЗАСЕЧКА

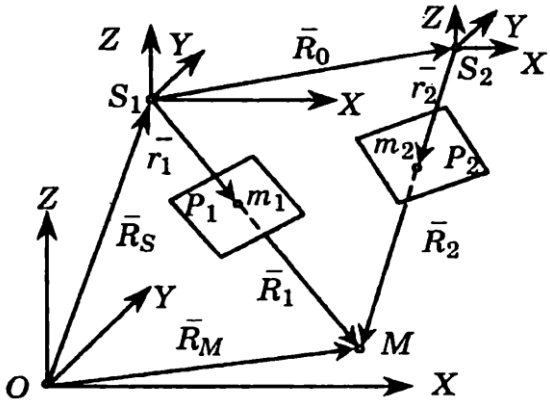
Постановка на задачата:

Нека имаме двойката аероснимки P_1 и P_2 (фиг.1) получени от центровете на проектиране S_1 и S_2 върху, които точки m_1 и m_2 са образите на т. M от местността.

Да се намерят координатите на т. M в местната координатна система OXYZ, при условие че линейните и ъгловите елементи на външно ориентиране на снимкитев са извевстни.

Решение:

На фиг. 1 с векторите $\bar{r}_1$ и $\bar{r}_2$ ще означим проектиращата връзка между центровете на проектиране S_1 и S_2 и изображенията на т. M върху снимките – т. m_1 и m_2 съответно. С векторите и - $\bar{R}_1$ ответно $\bar{R}_2$ означим проектиращите лъчи от центровете на проектиране S_1 и S_2 и точката от местността M, а с вектора - базата на фотографира $\bar{R}_o$ между центровете S_1 и S_2 .



Фиг. 1. Права фотограметрична задача

От съдържанието на фиг. 1 следва, че при известни елементи на външно ориентиране изискването за т.н. компланарност на едноименните проектиращи лъчи е изпълнено, което се представя с уравнението:

$$\bar{R}_o + \bar{R}_2 - \bar{R}_1 = 0 \qquad (1)$$

Във формула (1) векторът е известен по условие, тъй като са известни координатите на центровете на фотографиране: $\bar{R}_o$

Освен това чрез измерване на образните координати на точките m_1 и m_2 от лявата и дясната снимка и използвайки ъгловите елементи на външно ориентиране, то векторите $\bar{r}_1$, $\bar{r}_2$ могат да бъдат определени.

Изхождайки от факта, че векторите $\bar{r}_1$, $\bar{r}_2$ и $\bar{R}_1$, $\bar{R}_2$ са колинеарни два по два, следва, че е в сила равенството:

$$\bar{R}_1 = N_1 \bar{r}_1 \text{ и } \bar{R}_2 = N_2 \bar{r}_2 \qquad (2)$$

Където N1 и N2 са някакви скаларни множители функция на съставящите на базата на фотографиране - вектора и $\bar{R}_o$ координатите на т. m_1 и m_2 във фотограметричната координатна система.

Т.е. ако са известни стойностите на векторите $\bar{R}_1$ и $\bar{R}_2$ то координатите на т. M от местността могат да бъдат определени чрез измерване на образните координати на нейните образи - точките m_1 и m_2 върху съответната снимка от стереодвойката.

От тук следва и основното съдържание в същността на правата фотограметрична засечка, а именно: При известни линейни и ъглови елементи на външно ориентиране на аерофотоснимките в зададена координатна система, координатите на която и да е точка от местността могат да бъдат получени в тази координатна система, чрез измерване на нейните образни координати най-малко върху две припокриващи се аерофотоснимки.

3. ОСНОВНИ ЕТАПИ НА ИЗЧИСЛИТЕЛНИЯ ПРОЦЕС В AGISOFT METASHAPE PROFESSIONAL И НЕДОСТАТЪЦИ

Всички, които са запознати със софтуерния продукт за цифрова фотограметрия Agisoft Metashape Professiona, занят, че основните изчислителни етапи с чисто фотограметрично съдържание за този софтуер (всъщност те са анлогични и за повечето от другите софтуерни продукти) са три, а именно:

- Подреждане (взаимно ориентиране на аероснимките);
- Измерване на опорните GCP точки;
- Определяне на линейните и ъглови елементи на външно ориентиране на снимките.

Т.е. след приключването тези етапи са налице условията за прилагането на теорията и на правата фотограметрична засечка с цел създавнето на т.н. плътен облак от точки, а след това и алгоритмите за създаване на цифрови модели на терена TIN и DEM, ортофотоизображения и други фотограметрични продукти.

Основния продукт от тях, който оказва решаващо влияние върху точността и качеството на крайните профукти е формираният плътен облак от точки. В основата на този процес лежи автоматичната идентификация на съответните едноименни точки от снимките, която винаги се извършва с някаква степен на достоверност – различна от 100%

Както беше отбелязано по-горе всички тези технологични процеси са напълно автоматизирани и протичат без участието на оператора.

Разбира се за обикновения изпълнител това, което се генерира на изхода на програмата е окончателен продукт не подлежащ на допълнителна корекциа и подобряване на качеството.

В много случаи обаче се налага от обработваните аерофотоснимки да се извлича геопространствена информация за точки, за които чрез стандартна последователност на работа това е невъзможно.

Типичен пример в това отношение е и проблемът свързан с основната претенция на АГКК касаеща невъзможността за точното определянето на контурите на на сградите по генерираните ортофото изображения с цел създаване на кадастрални карти.

Като други подобни примери могат да се посочат:

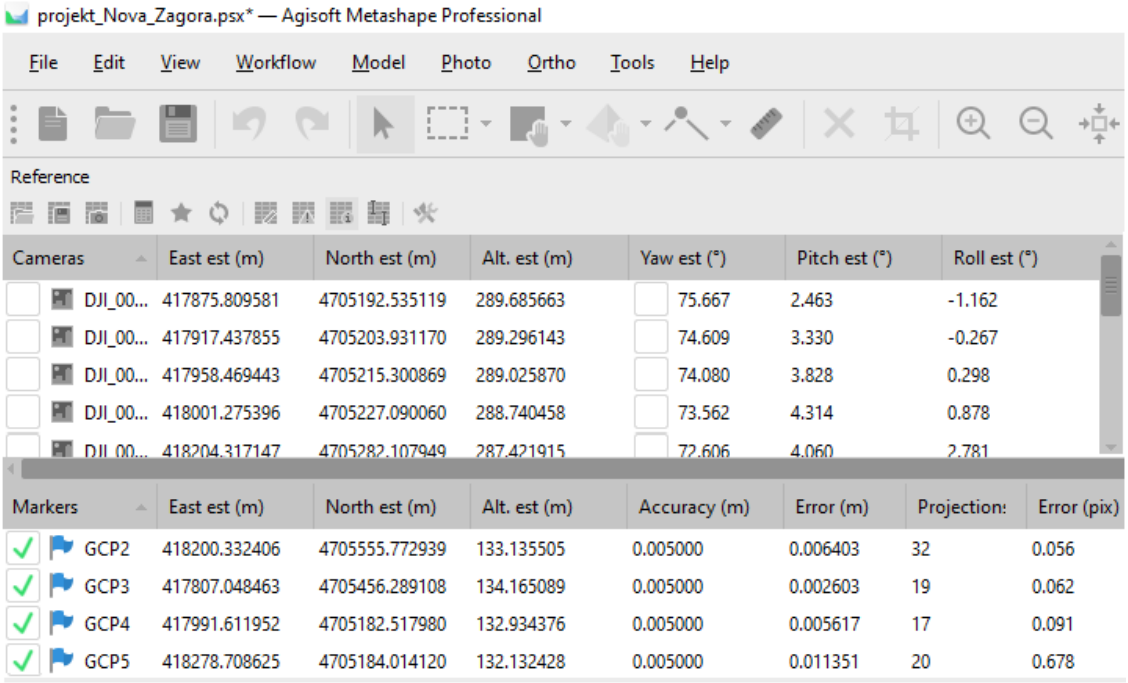
- Проблеми възникващ от невъзможността на софтуера автоматизирано да опознае едноименнтие точки върху различните снимки принадлежащи към тези някои високо стърчащи над терена обекти – такива високи комини, особено електрически стълбове и ферми, тесни и високи сгради и т.н., което прави невъзможно определянето на техните височини по генерирани, което прави невъзможно определянето на техните височини по генерираните 3D облаци от точки или създаваните TIN (DEM) модели;
- Затруднено автоматизирано създаването на точни 3D фасадни модели на сградите заради наличието на много паразитни шумове (регистрирани върху снимките обекти от вътрешността на помещенията, климатици, антени, висящи кабели и т.н.)
- Точното определяне на местоположението на високи масивни огради и т.н.

Именно решаването на тези проблеми е по силите на добре подготвения геодезист фотограметрист работещ с Agisoft и притежаващ добри познания по дешифриране на аерофотоснимките, чрез прилагане на правата фотограметрична засечка в режим на ръчно измерване на едноименните точки от аерофотоснимките.

4. СЪЩНОСТ НА ИЗМЕРИТЕЛНИЯ ПРОЦЕС

Същността на предлагания подход за работа се състои в генериране (измерване) след изпълнен етап „optimize cameras" на нови едноименни подробни точки изобразени върху по-вече от една аерофотоснимка (различни от GSP използвани при определяне на елемнтите на външно ориентиране на снимките)

На фиг. 2 е показано съдържанието на обекта подложен на фотограметрична обработка в среда на Agisoft Metashape Professional след етапа „изчисление на елементите на външно ориентиране“ (optimize cameras)



Cameras	East est (m)	North est (m)	Alt. est (m)	Yaw est (°)	Pitch est (°)	Roll est (°)
DJI_00...	417875.809581	4705192.535119	289.685663	75.667	2.463	-1.162
DJI_00...	417917.437855	4705203.931170	289.296143	74.609	3.330	-0.267
DJI_00...	417958.469443	4705215.300869	289.025870	74.080	3.828	0.298
DJI_00...	418001.275396	4705227.090060	288.740458	73.562	4.314	0.878
DJI_00...	418204.317147	4705282.107949	287.421915	72.606	4.060	2.781

Markers	East est (m)	North est (m)	Alt. est (m)	Accuracy (m)	Error (m)	Projection:	Error (pix)
GCP2	418200.332406	4705555.772939	133.135505	0.005000	0.006403	32	0.056
GCP3	417807.048463	4705456.289108	134.165089	0.005000	0.002603	19	0.062
GCP4	417991.611952	4705182.517980	132.934376	0.005000	0.005617	17	0.091
GCP5	418278.708625	4705184.014120	132.132428	0.005000	0.011351	20	0.678

Фиг. 2. Състояние на фотограметричния модел след етап optimize cameras

От фиг. 2 е видно, че с използването на геодезически определените координати на опорните GCP точки и след измерването на техните образни координати върху съответните снимки Agisoft Metashape Professional е определил елементите на външно ориентиране за всяка снимка – трите линейни елемента – X,Y,Z и трите ъглови елемента – ъгъл на завъртане χ, напречен ъгъл на наклона φ и надлъжен ъгъл на наклона ω. Т.е. на този етап вече е открита възможността за точното от математическа гледна точка определяне координатите на която и да е точка от заснетата земна повърхност, чрез измерване на нейните образни координати най-малко върху две припокриващи се аерофотоснимки.

На фиг. 3 *а,б,в,г* са показани измерените две едноименни точки 752 и 753 представляващи съответно върхът и основата на образът на електрически стълб изобразен на четири припокриващи се аероснимки.

а) измерни едноименни точки върху една аероснимка

point 752	564936.769	4742831.700	40.011
point 753	564936.695	4742831.754	32.407

б) измерени едноименни точки върху две аероснимки

point 752	564934.365	4742833.369	32.674
point 753	564935.169	4742833.235	32.599

в) измерени едноименни точки върху три аероснимки

point 752	564936.764	4742831.699	40.002
point 753	564936.699	4742831.749	32.409

г) измерени едноименни точки върху четири аероснимки

point 752	564936.761	4742831.710	40.015
point 753	564936.661	4742831.791	32.434

Фиг. 3. Резултати от определянето на плановите координати X,У,Z на основата и върха на електрически стълб изобразен върху четири припокриващи се аерофотоснимки.

От сравнението на получените стойности за геодезическите координати на двете точки 752 и 753 получени след измерването на техните образни координати върху една, две, три и четири снимки се вижда, че стойностите на X,У,Z получени при измерването върху една снимка се про-

менят значително след измерването на тези идентични точки върху две припокриващи се снимки (фиг. 3а и 3б). При това сходимостта между различните стойностите на координатите в рамките на 20-30 мм. се запазва при измерването на образните координати върху третата и четвъртата снимки.

На база гореказаното следва, че освен генерирането на т.н. облак от точки в средата на програмния продукт Agisoft Metashape Professional е възможно определянето на пространствените координати на отделни единични точки представляващи особен интерес за потребителя.

5. ЕКСПЕРИМЕНТАЛНА ПРОВЕРКА НА МЕТОДА

За оценка на приложимостта и надежността на предлагания метод е проведен експеримент в рамките на изработването на кадастралната карта на с. Попович, общ. Бяла, обл. Варна. В рамките на същия чрез метода на „правата засечка“ са определени плановите координатите на 383 точки от фасадите на сгради и трайно материализирани огради, чиито стойности в последствие са сравнени с тези получени чрез линейно-ъглови геодезически измервания.

За целта с помощта на безпилотен летателен апарат „Фантом 4“ снабден с малкоформатна метрична аерокамера DJI FC 330 с фокусно разстояние 3.61 мм е изпълнено аерофотографиране на населеното място. Аерозаниманието е изпълнено от височина 80 м с пространствена разделителна способност на получените аероснимки – GSD – 2.7 см.

За определяне на елементите на външно ориентиране в качеството на опорни GCP точки след извършено подходящо маркиране са използвани точките от развитата работна геодезическа основа, от които в последствие са извършвани и линейно-ъгловите измервания.

Визуално част от общото количеството измерени подробни точки е показано на фиг. 4.

Фиг. 4. Измерени подробни точки по фотограметричниа модел на с. Попович в средата на Agisoft Metashape Professional

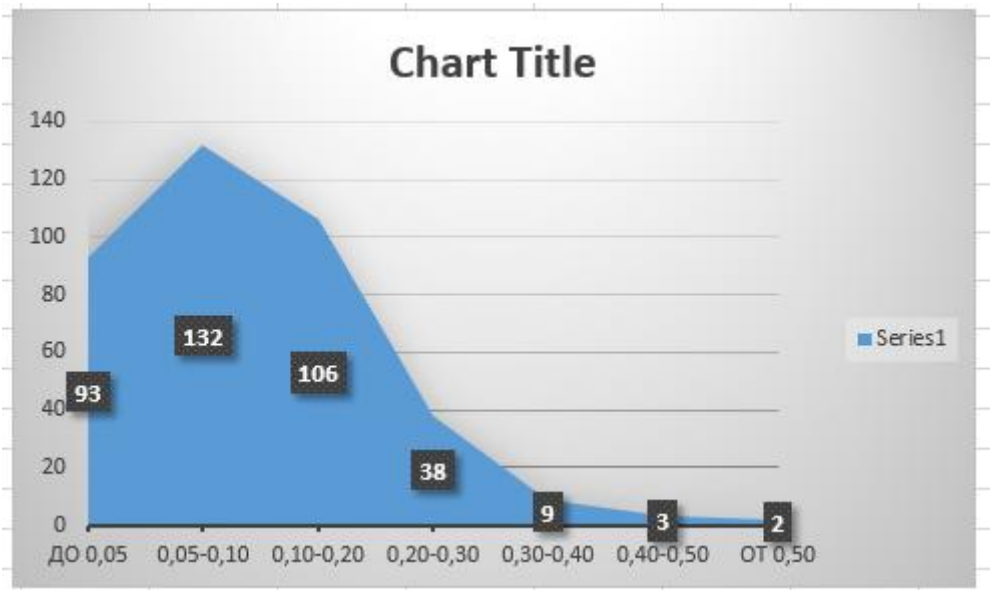
Сравнението на координатите определени по фотограметричн начин с прилагане на способа „Права фотограметрична засечка“ и тези чрез линейно-ъглови измервания са дадени в Таблица № 1

Таблица №1

A	B	C	D	E	F	G	H	I	J	K	L
		Координати получени чрез фотограметрични методи		Координати получени чрез линейно-ъглови измервания							
№		X [m]	Y [m]	X [m]	Y [m]	ΔX [m]	ΔY [m]	ΔX^2 [m]	ΔY^2 [m]	ΔS	ΔS^2
1	вт 1	4742717,99	564600,72	4742717,95	564600,76	0,0400	-0,0400	0,0016	0,0016	0,0566	0,0032
2	вт 2	4743185,02	565127,22	4743185,09	565127,11	-0,0700	0,1100	0,0049	0,0121	0,1304	0,0170
3	вт 3	4743176,85	565134,07	4743176,98	565134,01	-0,1300	0,0600	0,0169	0,0036	0,1432	0,0205
4	вт 5	4742833,67	565169,10	4742833,70	565169,07	-0,0300	0,0300	0,0009	0,0009	0,0424	0,0018
5	вт 6	4742832,50	565141,51	4742832,59	565141,48	-0,0900	0,0300	0,0081	0,0009	0,0949	0,0090
6	вт 7	4742831,30	565151,14	4742831,26	565151,10	0,0400	0,0400	0,0016	0,0016	0,0566	0,0032
7	вт 8	4742836,92	565142,39	4742836,96	565142,44	-0,0400	-0,0500	0,0016	0,0025	0,0640	0,0041
8	вт 10	4743205,46	565009,63	4743205,50	565009,58	-0,0400	0,0500	0,0016	0,0025	0,0640	0,0041
9	вт 11	4743194,89	564993,71	4743194,95	564993,71	-0,0600	0,0000	0,0036	0,0000	0,0600	0,0036
10	вт 16	4743192,38	564993,02	4743192,41	564992,99	-0,0300	0,0300	0,0009	0,0009	0,0424	0,0018
11	вт 17	4743158,85	564996,13	4743158,89	564996,19	-0,0400	-0,0600	0,0016	0,0036	0,0721	0,0052
12	вт 21	4743185,60	564990,73	4743185,63	564990,93	-0,0300	-0,2000	0,0009	0,0400	0,2022	0,0409
13	вт 23	4743087,73	564954,20	4743087,69	564954,22	0,0400	-0,0200	0,0016	0,0004	0,0447	0,0020
14	вт 24	4743095,63	564950,96	4743095,69	564950,84	-0,0600	0,1200	0,0036	0,0144	0,1342	0,0180
15	вт 25	4743091,96	564976,19	4743091,92	564976,22	0,0400	-0,0300	0,0016	0,0009	0,0500	0,0025
16	вт 30	4743092,38	564987,28	4743092,41	564987,31	-0,0300	-0,0300	0,0009	0,0009	0,0424	0,0018
17	вт 31	4743090,54	564986,89	4743090,86	564987,07	-0,3200	-0,1800	0,1024	0,0324	0,3672	0,1348
18	вт 32	4743091,58	564992,63	4743091,58	564992,59	0,0000	0,0400	0,0000	0,0016	0,0400	0,0016
19	вт 33	4743084,65	565011,55	4743084,58	565011,41	0,0700	0,1400	0,0049	0,0196	0,1565	0,0245
20	вт 34	4743088,28	565016,90	4743088,34	565016,96	-0,0600	-0,0600	0,0036	0,0036	0,0849	0,0072
21	вт 35	4743087,49	565022,35	4743087,57	565022,31	-0,0800	0,0400	0,0064	0,0016	0,0894	0,0080
22	вт 38	4743095,80	565023,51	4743095,85	565023,47	-0,0500	0,0400	0,0025	0,0016	0,0640	0,0041
23	вт 42	4743079,61	564974,31	4743079,59	564974,41	0,0200	-0,1000	0,0004	0,0100	0,1020	0,0104
24	вт 44	4743077,41	565007,59	4743077,49	565007,53	-0,0800	0,0600	0,0064	0,0036	0,1000	0,0100
25	вт 45	4743050,70	564969,82	4743050,69	564969,80	0,0100	0,0200	0,0001	0,0004	0,0224	0,0005
26	вт 47	4743057,78	564965,57	4743058,07	564965,37	-0,2900	0,2000	0,0841	0,0400	0,3523	0,1241
368	вт 681	4742762,00	564728,91	4742762,00	564728,89	0,0000	0,0200	0,0000	0,0004	0,0200	0,0004
369	вт 686	4742844,42	565144,71	4742844,46	565144,72	-0,0400	-0,0100	0,0016	0,0001	0,0412	0,0017
370	вт 687	4742853,05	565145,28	4742853,09	565145,28	-0,0400	0,0000	0,0016	0,0000	0,0400	0,0016
371	вт 688	4742848,26	565144,69	4742848,17	565144,92	0,0900	-0,2300	0,0081	0,0529	0,2470	0,0610
372	вт 692	4742838,63	565148,31	4742838,72	565148,21	-0,0900	0,1000	0,0081	0,0100	0,1345	0,0181
373	вт 700	4742853,07	564651,81	4742852,99	564651,79	0,0800	0,0200	0,0064	0,0004	0,0825	0,0068
374	вт 701	4742854,61	564654,61	4742854,62	564654,59	-0,0100	0,0200	0,0001	0,0004	0,0224	0,0005
375	вт 702	4742855,20	564657,99	4742855,18	564657,98	0,0200	0,0100	0,0004	0,0001	0,0224	0,0005
376	вт 703	4742849,20	564670,14	4742849,16	564670,25	0,0400	-0,1100	0,0016	0,0121	0,1170	0,0137
377	вт 705	4742848,20	564671,36	4742848,24	564671,35	-0,0400	0,0100	0,0016	0,0001	0,0412	0,0017
378	вт 706	4742851,02	564661,46	4742851,08	564661,52	-0,0600	-0,0600	0,0036	0,0036	0,0849	0,0072
379	вт 707	4742854,75	564659,45	4742854,71	564659,49	0,0400	-0,0400	0,0016	0,0016	0,0566	0,0032
380	вт 708	4742849,55	564663,71	4742849,60	564663,69	-0,0500	0,0200	0,0025	0,0004	0,0539	0,0029
381	вт 709	4742846,91	564677,40	4742846,84	564677,41	0,0700	-0,0100	0,0049	0,0001	0,0707	0,0050
382	вт 735	4742987,68	564764,52	4742987,72	564764,47	-0,0400	0,0500	0,0016	0,0025	0,0640	0,0041
383	вт 737	4742999,38	564754,10	4742999,17	564754,26	0,2100	-0,1600	0,0441	0,0256	0,2640	0,0697
						ΣΔX [m]	ΣΔY [m]	$\Sigma\Delta X^2$ [m]	$\Sigma\Delta Y^2$ [m]	ΣΔS	$\Sigma\Delta S^2$
						-0,4100	5,2300	3,9611	3,3515		7,3126
							m_X	0,102			
							m_Y	0,094			
							m_S	0,138			

Таблица № 1 – Сравнение на стойностите на плановите координати на подробни точки определени чрез права фотограметрична засечка в средата на Agisoft Metashape Professional и линейно-ъглови измервания.

В графичен вид разпределението на координатните разлики между двата вида измервания е показано на фиг. 5.



Фиг. 5. Разпределение на координатните разлики между стойностите получени чрез фотограметрични измервания и линейно-ъглови измервания.

Ако с достатъчна условност приемем, че стойностите координатите получени чрез линейно-ъгловите измервания за безгрешни, то показанире на фиг. 5 резултати от сравнението на двата метода позволяват да се направят следните два важни изводи относно възможностите на цифровата фотограметрия като технология ипрактика:

Първи извод: Цифровата фотограметрична технология и по специално нейната реализация чрез програмния продукт Agisoft Metashape Professiona осигурява възможност при обработка на аерофотоснимки получени с БЛА да се определят пространствените координати на точките от местността с точност съизмерима с тази при използването на класически линейно-ъглови измервания;

Втори извод: Точността на получаваните по фотограметричн път резултати с използване на метода „Права фотограметрична засечка“ е обвързана с показателя GSD на използваните снимки чрез съотношението:

$$m_{x,y} = \pm 3(4) * GSD \qquad (3)$$

ЗАКЛЮЧЕНИЕ

Разглеждайки приложимостта на метода „Права фотограметрична засечка“ чрез „ръчно“ измерване на образните координати върху стереодвойката снимки в средата на Agisoft Metashape Professiona, могат да се дефинират следните основни положения свързани с използването на БЛА и малко форматните метрични камери:

Първо. Изискуемата точност на крайния продукт – координати на обектите от местността следва да се разглежда като основен показател при определяне на параметрите на аерофотографиране и по специално показателя GSD на придобиваните снимкови избражения;

Второ. Успешното прилагането на този подход е от особена важност при осигуряването на артилерията с топогеодезически данни за единични обекти разположенни на огневите позиции или района на целите. Това е продиктувано от факта, че дешифровъчните показатели на суровите

аерофото снимки са значително по-добри от тези на формираните на изхода на фотограметричния софтуер георефериранн орторектифицирани изображения;

Трето. Практическото приложение на разгледания подход за определяне координатите на единични обекти от аероснимките позволява получаването на достатъчно точно резултати без използването на скъпо струващи и сложни за използване (особено на полеви условия) системи за стереоскопично наблюдение;

Четвърто. Не използването на заложения във всички софтуерни продукти автоматизиран подход за опознаване на идентични точки от стереодвойкарта снимки и възлагайки тази задача на оператора фотограметрист следва, че въпросите свързани с изучаването на дешифровъчните признаци на обектите и методиката за дешифриране на аерофотоснимките следва да намират своето подобаващо място в процеса на обучение на специалистите по фотограметрия и особено на тези от специалността АИР към НВУ „Васил Левски“ – Факултет по Артилерия ПВО и КИС – гр.Шумен.

References

1. Беджева М., Т. Игнатова, Analysis of the accuracy of geodesical maps prepared by the means of UAVs, Proceedings of university of Ruse – 2019, volume 58 (на български), ISSN 2603-4123 (online)

2. Господинова Веселина, Бегновска Милена, Петков Росен „Изследване възможностите на безпилотните летателни апарати при решаване на геодезически задачи“ Списание Геодезия Картография и Земеустройство – кн. 1-2 2017г. стр. 23.

3. Димитър Петров „ XXIV-ти Международен симпозиум „Съвременните технологии, образованието и професионалната практика в геодезията и свързаните с нея области“ София 06-07-Ноември 2014г.“

4. Филипов Атанас „Използване на безпилотни летателни системи (БЛС) като платформи за дистанционни изследвания“ Списание „Геомедия“
https://www.geomedia.bg/geodesia/izpolzvane-na-bezpilotni-letatelni-s-4/

INACCURACIES IN LINEAR OBJECTS TRANSFERRED FROM THE MAP OF THE RESTORED PROPERTY TO THE CADASTRAL MAP

Mirem E. Niyazi-Yusuf

Shumen's university "Bishop K. Preslavsky" m.niyazi@abv.bg

Abstract: *The cadastral map and cadastral registers are created under conditions of maximum use of the existing map of restored property (created under the Law on the Ownership and Use of Agricultural Lands, the Law on the Ownership of Forests and Lands from the Forest Fund) and the current cadastral plans of settlements, (approved in the order of the repealed Law on the Unified Cadastre and Law on Territorial and Settlement Planning).*

Key words: *interferometry, radar, interferogram, satellite image, monitoring, modeling*

НЕТОЧНОСТИ ПРИ ЛИНЕЙНИ ОБЕКТИ, ПРЕХВЪРЛЕНИ ОТ КАРТАТА НА ВЪЗСТАНОВЕНАТА СОБСТВЕНОСТ В КАДАСТРАЛНАТА КАРТА

Мирем Е. Ниязи-Юсуф

1. ВЪВЕДЕНИЕ

След премахването на социалистическия режим в България, XXXVI Народно събрание приема редица реституционни закони, с които се възстановява социалната справедливост по отношение на бившите собственици, нарушена от Народната власт след 9 септември 1944 г. Два от тези закона са Закон за собствеността и ползването на земеделските земи (ЗСПЗЗ) [3] и Закон за възстановяване на собствеността върху горите и земите от горския фонд (ЗВСГЗГФ).

В процедурите по възстановяване на собствеността на земеделските земи и на земите и горите от горския фонд са създадени за цялата извънселищна територия на страната планове за земеразделяне, карти на имотите в съществуващи или възстановими на терена стари реални граници и планове на горите и земите от горския фонд с регистри към тях. Плановете, картите и регистрите са създадени, ползвани и поддържани в цифров вид чрез специализиран софтуер. От съдържанието на тези планове и карти впоследствие е създаден в цифров вид единен графичен продукт, наречен карта на възстановената собственост (КВС) за земеделските и горските територии с регистри към нея.

През 2015 г. е приета Концепция за ускорено създаване на кадастрална карта и кадастрални регистри (КККР) и ускоряване на процеса по създаване на имотен регистър [4, 6, 8].

Целта на концепцията е ускоряване на процеса по създаване на КККР за територията на цялата страна, чрез изработване на КККР за неурбанизираната територия, ползвайки данните от картата на възстановената собственост КВС.

В практиката на АГКК - в процеса на създаване на КККР и поддържане на вече одобрените КККР в актуално състояние, се констатират несъответствия в неурбанизираната територия, които са прехвърлени в КККР от КВС.

При поддържане на КККР, несъответствията в неурбанизираната територия се констатират инцидентно – по повод на конкретни заявления от отделни заинтересувани лица. В голяма част от случаите, идентифицираните несъответствия са неточно отразени или липсващи топографски обекти с естествен или изкуствен произход – реки, дерета, пътища, техническа инфраструктура.

От случайно констатираните несъответствия не може да се направи обобщаващо заключение за качеството на КВС – както за едно землище, така и за всички землища на територията на страната, както и в каква степен КВС може да послужи за преобразуването й директно в КККР, без извършване на корекции.

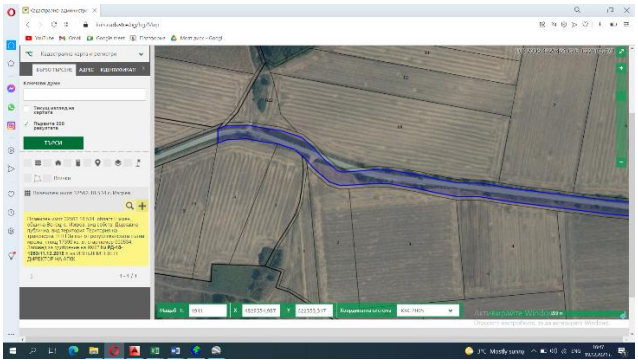
Създадените карти на възстановената собственост след 1990 г. съдържат множество грешки, които са прехвърлени от съществуващите до момента едромащабни топографски карти. За създаването на карти на възстановената собственост директно са използвани ЕТК, създадени през годините 1964 – 1968 г., без повторно аерофото заснемане и дешифриране на обектите [5].

2. РЕЗУЛТАТИТЕ ОТ ЕКСПЕРИМЕНТАЛНИ ИЗСЛЕДВАНИЯ ЗА НЕТОЧНОСТИ ПРИ ЛИНЕЙНИ ОБЕКТИ ПРЕХВЪРЛЕНИ ОТ КВС В КККР

Представени са два обекта на пътната инфраструктура и е направен анализ на точността на съществуваща карта на възстановената собственост съгласно Наредба РД 02-20-5 от 2016 г.

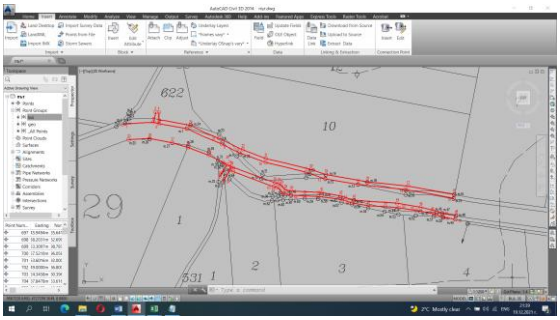
Първият обект е път от републиканска пътна мрежа с идентификатор 32562.18.534, намиращ се в землището на село Изгрев, община Венец, област Шумен.

В КАИС се визуализира пътя с основа аерофото изображение [10], [12].



Фиг. 1. Път от републиканската пътна мрежа

На фиг. 2 е показано положението на точките от обектите отразени в КК и на точките от същите обекти в резултат на геодезичните измервания, в участъка където разликите са най-големи. В черен цвят и номерация са показани обектите и тяхното отражение в КК, а в червен цвят тези от измерванията.



Фиг. 2. Координатите на всички точки са в координатна система БГС 2005.

При геодезичните измервания на пътя подробните точки предмет на замерване са точките по контура на асфалтовото покритие, банкетите, канавките и откосите.

Съгласно ал. 5 от чл. 18 на от Наредба № РД-02-20-5/15.12.2016г.[13] за неурбанизирани територии са определени и допустимите стойности на ΔS = 180 см, при случаите когато координатите на точките в кадастралната карта са определени от графичен план или карта.

Сравнените точки за извършване на анализа на обекта в землището на с. Изгрев са общо 64 бр. Данните са представени в таблица 1.

Таблица 1 Разлики в абсолютното положение на точките

№ на точката	Координати на точките от КК		Координати на точките от измервания		Разлики ΔS (cm)
	X (m)	У (m)	X (m)	У (m)	
1	4829636,313	622105,010	4829636,328	622105,045	3,808
2	4829633,305	622097,289	4829639,198	622142,929	4601,888
3	4829649,522	622112,259	4829651,534	622145,283	3308,523
4	4829646,829	622116,494	4829651,413	622149,454	3327,724
5	4829642,737	622112,609	4829641,302	622149,540	3695,887
6	4829637,498	622108,051	4829637,318	622149,574	4152,339
7	4829631,733	622183,453	4829631,502	622183,415	23,410
8	4829615,323	622227,099	4829613,396	622226,134	215,512
9	4829598,535	622244,537	4829603,202	622246,933	524,611
10	4829571,263	622275,005	4829591,140	622279,946	2048,191
11	4829572,911	622329,354	4829579,851	622329,347	694,000
12	4829572,059	622352,654	4829571,710	622352,572	35,850
13	4829565,303	622392,610	4829565,706	622392,604	40,304
14	4829553,378	622450,688	4829559,623	622450,393	625,196
15	4829549,078	622509,220	4829549,510	622509,075	45,569
16	4829553,897	622510,141	4829554,729	622509,978	84,782
17	4829558,538	622451,359	4829564,109	622453,757	606,518
18	4829568,092	622403,769	4829568,646	622404,079	63,484
19	4829576,956	622353,309	4829577,203	622353,668	43,576
20	4829577,777	622333,791	4829583,235	622335,038	559,864
21	4829576,299	622276,268	4829595,997	622280,106	2006,842
22	4829601,080	622248,948	4829606,715	622251,889	635,631
23	4829625,452	622222,892	4829620,296	622222,376	518,176
24	4829636,124	622187,925	4829635,592	622187,732	56,593
25	4829617,544	622112,733	4829617,565	622112,778	4,966
26	4829618,674	622138,408	4829619,129	622138,363	45,722
27	4829614,077	622165,792	4829614,287	622165,868	22,333
28	4829611,145	622185,409	4829608,753	622184,984	242,946
29	4829602,971	622210,589	4829599,647	622210,349	333,265
30	4829587,967	622227,002	4829591,229	622227,751	334,689

31	4829593,110	622221,629	4829588,089	622232,387	1187,203
32	4829567,181	622222,658	4829573,991	622224,182	697,844
33	4829566,505	622227,668	4829568,826	622228,896	262,584
34	4829577,631	622229,511	4829581,801	622236,245	792,058
35	4829588,851	622226,140	4829585,777	622238,348	1258,907
36	4829549,893	622288,604	4829566,800	622290,990	1707,453
37	4829550,468	622295,542	4829565,787	622296,098	1532,909
38	4829550,946	622299,675	4829563,438	622299,241	1249,954
39	4829550,908	622303,885	4829558,156	622304,177	725,388
40	4829551,458	622311,120	4829556,677	622311,475	523,106
41	4829552,221	622348,339	4829555,153	622348,420	293,312
42	4829548,709	622370,894	4829551,347	622371,478	270,187
43	4829545,916	622387,696	4829546,649	622387,703	73,303
44	4829535,091	622440,179	4829542,929	622440,602	784,941
45	4829533,149	622468,887	4829538,298	622469,180	515,733
46	4829531,904	622488,886	4829533,723	622488,906	181,911
47	4829531,022	622495,309	4829531,679	622495,308	65,700
48	4829528,267	622512,197	4829529,118	622512,380	87,045
49	4829523,910	622511,646	4829524,173	622511,639	26,309
50	4829525,931	622496,635	4829526,815	622496,750	89,145
51	4829527,564	622485,399	4829530,300	622485,627	274,548
52	4829528,225	622463,491	4829534,359	622464,033	615,790
53	4829529,565	622442,298	4829537,544	622442,572	798,370
54	4829532,673	622425,287	4829538,898	622426,050	627,159
55	4829536,881	622405,203	4829539,773	622405,458	290,322
56	4829541,256	622385,412	4829542,980	622385,668	174,290
57	4829543,371	622372,857	4829546,958	622373,301	361,437
58	4829547,368	622344,167	4829550,491	622344,507	314,145
59	4829547,709	622327,936	4829551,094	622327,689	339,400
60	4829546,469	622310,758	4829551,698	622310,872	523,024
61	4829545,619	622301,432	4829553,573	622301,616	795,613
62	4829545,330	622294,268	4829561,103	622294,013	1577,506
63	4829544,819	622287,945	4829561,969	622289,648	1723,435
64	4829570,525	622236,028	4829579,601	622240,737	1022,489

Всички стойности на ΔS по големи от 180 cm са показани в червен цвят и представляват 72 % от анализираните стойности.

В резултат от обработката на измерванията за оценка на точността на кадастралната карта се получават три статистически реда със стойности:

$$\Delta x_i = x_i - x_i^o$$

(1)

$$\Delta y_i = y_i - y_i^o$$

$$\partial S_i = \partial S_i - \partial S_i^o,$$

където означенията с горен индекс "о" са стойности от кадастралната карта, а означенията без горен индекс са получени в резултат на геодезични измервания и обработки.

Проверката на хипотезата за съгласуване на емпиричното разпределение с нормалното се осъществява чрез критерия на Пирсън (χ^2) и чрез изчисление на асиметрията, ексцеса и съответните им доверителни интервали [11] .

Проверка за съгласуваност чрез критерия на Пирсън (χ^2). Избрани са 5 интервала от -∞ до +∞. Изчислени са нормираните граници, вероятността за попадане и теоретичният и емпиричният брой грешки. Направено е изследване за груби и систематични грешки. Измервания, при които са налични груби грешки, са изключени при изследването.

Резултатите за реда ΔX са дадени в таблица 2.

Таблица 2. Резултати за реда ΔX

Действ.граници		Нормир. граници		Вероятн. за попадане		Брой грешки		Разл.	$\Delta N_j^2/N_j$
долна	горна	долна	горна	F(тд)	F(тг) - F(тд)	теорет.	емпир.	ΔN_j	χ^2_j
-∞	-2	0,000	-0,359	0,000	0,360	23,028	27,000	3,972	0,685
-2	0	-0,359	0,000	0,360	0,140	8,972	10,000	1,028	0,118
0	2	0,000	0,359	0,500	0,140	8,972	10,000	1,028	0,118
2	4	0,359	0,718	0,640	0,123	7,898	9,000	1,102	0,154
4	+∞	0,718	1,000	0,764	0,236	15,130	8,000	-7,130	3,360
			[ ]	1			64,000	χ^2=	3,74937

Общият брой на грешките в реда ΔX е 64.

Степента на свобода се определя с помощта на формулата

(4.3.) $$r = N - 3,$$

където N е броят на интервалите.

При стойност χ^2 =3,74937 и степен на свобода 2 е изчислена вероятността 0,1534. Изчислената вероятност е по-голяма от 0,1 и може да се твърди, че хипотезата за нормално разпределение на изследвания ред се потвърждава.

Резултатите за реда ΔУ са дадени в таблица 3.

Таблица 3. Резултати за реда ΔУ

Действ. граници		Нормир. граници		Вероятн. за попадане		Брой грешки		Разл.	$\Delta N_j^2/N_j$
долна	горна	долна	горна	F(тд)	F(тг) - F(тд)	теорет.	емпир.	ΔN_j	χ^2_j
-∞	-2	0,000	-2,828	0,000	0,002	0,122	0,000	-0,122	0,122
-2	0	-2,828	0,000	0,002	0,498	25,873	35,000	9,127	3,219
0	2	0,000	2,828	0,500	0,498	25,883	14,000	-11,883	5,456
2	4	2,828	5,656	0,998	0,002	0,122	3,000	2,878	67,976
4	+∞	5,656	1,000	1,000	0,000	0,000	0,000	0,000	0,000
			[ ]	1			52,000	χ^2=	76,6514

Поради наличието на груби грешки, от статистическия ред са изключени 12 на брой измервания. Общият брой на грешките в реда ΔУ е 52.

Резултатите за реда δS са дадени в таблица 4.

Таблица 4. Резултатите за реда δS

Действ.граници		Нормир. граници		Вероятн. за попадане		Брой грешки		Разл.	$\Delta N_j^2/N_j$
долна	горна	долна	горна	F(тд)	F(тг) - F(тд)	теорет.	емпир.	ΔN_j	χ^2_j
-∞	-2	0,000	-2,391	0,000	0,008	0,386	1,000	0,614	0,975
-2	0	-2,391	0,000	0,008	0,492	22,614	18,000	-4,614	0,941
0	2	0,000	2,391	0,500	0,492	22,614	27,000	4,386	0,851
2	4	2,391	4,782	0,992	0,008	0,386	0,000	-0,386	0,386
4	+∞	4,782	1,000	1,000	0,000	0,000	0,000	0,000	0,000
			[ ]	1			46,000	χ^2=	2,17845

Поради наличието на груби грешки, от статистическия ред са изключени 19 на брой измервания. Общият брой на грешките в реда δS е 46.

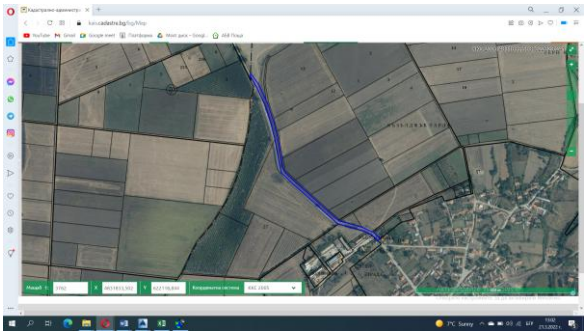
Съгласно Приложение № 6 към чл. 82, ал. 6 от Наредба № РД № 02-20-5/2016 г., когато над 5 % от стойностите на реда се изключват заради наличие на груби грешки, анализът на реда се прекратява.

За редовете ΔУ и δS наличието на грубите грешки надхвърля 5% и анализът за редовете ΔУ и δS се прекратява.

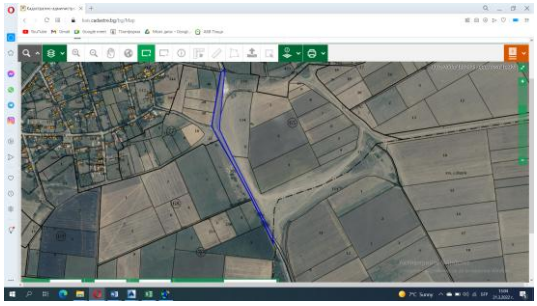
В заключение може да се каже, че редовете ΔУ и δS нямат нормално разпределение.

Вторият обект е местният път Наум – Климент с идентификатор 51158.1.112 и 37232.65.223, намиращ се в землището на село Наум и на село Климент, община Каолиново, област Шумен.

В КАИС се визуализира пътя с основа аерофото изображение.

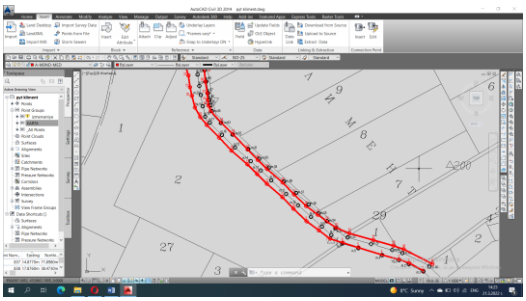


Фиг. 3. Местен път в землището на с. Наум в КАИС

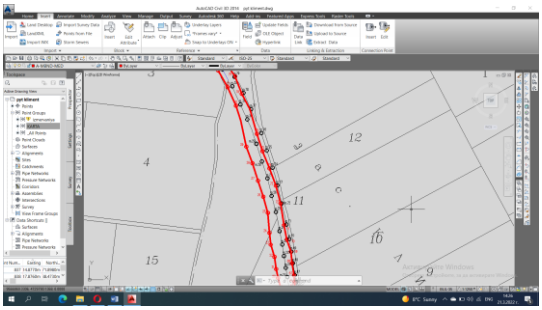


Фиг. 4. Местен път в землището на с. Климент в КАИС

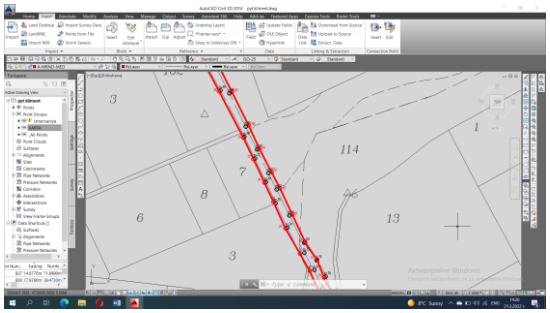
На фиг. 5, 6, 7 и 8 са показани положението на точките от обектите отразени в КК и на точките от същите обекти в резултат на геодезичните измервания, в участъка където разликите са най-големи. В черен цвят и номерация са показани обектите и тяхното отражение в КК, а в червен цвят са тези от измерванията.



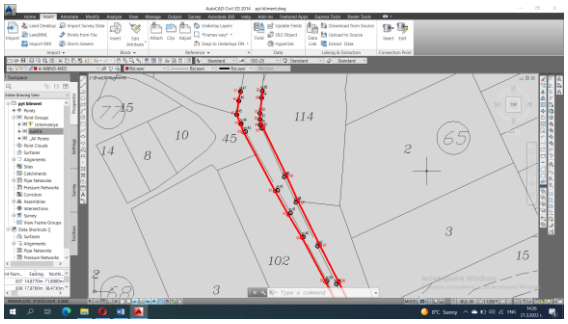
Фиг. 5



Фиг. 6



Фиг. 7



Фиг. 8

Координатите на всички точки са в координатна система БГС 2005.

Съгласно ал. 5 от чл. 18 на същата наредба за неурбанизирани територии са определени и допустимите стойности на ΔS = 180 см, при случаите когато координатите на точките в кадастралната карта са определени от графичен план или карта.

Сравнените точки за извършване на анализа на обекта в землището на с. Наум и на с. Климент са общо 95 бр. Данните са представени в таблица 5.

Таблица 5. Разлики в абсолютното положение на точките

№ на точката	**Координати на точките от КК**		**Координати на точките от измервания**		**Разлики ΔS cm**
	X	**У**	**X**	**У**	
1	4831626,108	622345,196	4831627,105	622344,994	101,726
2	4831635,452	622326,063	4831636,895	622326,747	159,690
3	4831640,753	622312,981	4831641,668	622313,399	100,596
4	4831646,958	622290,989	4831647,323	622291,287	47,120
5	4831655,840	622260,067	4831656,747	622260,182	91,426
6	4831661,847	622238,954	4831662,976	622239,620	131,080
7	4831672,978	622224,502	4831668,127	622223,076	505,625
8	4831683,784	622212,203	4831678,775	622208,381	630,062
9	4831696,562	622197,755	4831690,570	622192,101	823,843
10	4831711,399	622180,712	4831706,854	622174,772	747,935
11	4831726,110	622165,045	4831722,029	622160,199	633,548
12	4831743,915	622145,441	4831739,221	622139,835	731,169
13	4831756,580	622131,717	4831751,826	622127,100	662,701
14	4831768,700	622118,410	4831764,554	622114,239	588,103

15	4831786,392	622097,767	4831782,363	622093,152	612,626
16	4831802,739	622080,436	4831799,007	622076,866	516,456
17	4831818,548	622064,623	4831815,582	622060,644	496,282
18	4831826,410	622058,474	4831825,873	622051,968	652,812
19	4831839,988	622055,058	4831838,355	622044,743	1044,346
20	4831854,810	622052,457	4831853,652	622040,702	1181,190
21	4831866,476	622050,432	4831864,853	622038,295	1224,504
22	4831881,487	622047,965	4831880,268	622035,929	1209,757
23	4831896,037	622045,778	4831895,613	622031,113	1467,113
24	4831912,950	622042,195	4831910,618	622029,437	1296,938
25	4831937,098	622037,177	4831935,851	622027,164	1009,035
26	4831957,329	622031,628	4831956,262	622021,152	1053,020
27	4831979,549	622026,213	4831976,496	622014,268	1232,898
28	4832000,929	622019,017	4831998,521	622006,953	1230,197
29	4832023,222	622011,802	4832019,470	621999,116	1322,921
30	4832053,909	621999,988	4832052,441	621991,654	846,230
31	4832072,887	621991,151	4832071,237	621985,579	581,117
32	4832095,751	621980,641	4832094,536	621974,805	596,113
33	4832116,947	621967,945	4832115,577	621962,461	565,254
34	4832148,174	621946,203	4832147,332	621943,832	251,607
35	4832178,561	621931,366	4832180,264	621928,550	329,091
36	4832204,782	621919,015	4832204,346	621916,991	207,043
37	4832234,213	621905,011	4832233,632	621902,934	215,673
38	4832261,110	621891,565	4832260,388	621890,090	164,223
39	4832318,783	621861,076	4832317,957	621859,053	218,513
40	4832372,204	621831,717	4832371,672	621830,094	170,797
41	4832401,269	621815,916	4832399,365	621813,269	326,065
42	4832428,762	621800,278	4832427,763	621796,851	356,964
43	4832499,568	621760,593	4832498,869	621758,285	241,153
44	4832509,060	621755,259	4832508,651	621754,230	110,730
45	4832519,842	621749,429	4832519,902	621749,998	57,215
46	4832536,443	621752,287	4832536,838	621751,682	72,253
47	4832547,732	621754,231	4832548,128	621753,687	67,287
48	4831632,537	622352,850	4831636,222	622356,901	547,630
49	4831649,932	622317,601	4831655,161	622319,256	548,466
50	4831653,956	622304,308	4831659,626	622305,733	584,633
51	4831661,548	622276,607	4831666,757	622279,581	599,820
52	4831669,976	622246,009	4831675,391	622248,058	578,970
53	4831681,747	622229,853	4831682,267	622230,937	120,227
54	4831691,059	622219,028	4831690,713	622218,631	52,662
55	4831700,937	622207,865	4831699,436	622206,592	196,813
56	4831712,815	622194,505	4831710,482	622191,344	392,872

57	4831727,568	622178,124	4831725,543	622175,319	345,957
58	4831742,295	622162,046	4831741,102	622160,378	205,072
59	4831760,485	622142,173	4831758,458	622139,819	310,645
60	4831771,871	622129,518	4831770,506	622127,646	231,681
61	4831784,513	622115,162	4831783,790	622114,223	118,509
62	4831803,264	622094,449	4831803,628	622095,056	70,777
63	4831818,315	622078,970	4831818,635	622079,491	61,143
64	4831833,700	622067,253	4831833,752	622065,690	156,386
65	4831841,513	622065,457	4831841,065	622062,438	305,206
66	4831848,480	622063,778	4831848,131	622061,840	196,917
67	4831857,301	622062,082	4831857,182	622061,016	107,262
68	4831872,476	622059,537	4831872,266	622058,272	128,231
69	4831887,094	622057,364	4831887,077	622056,900	46,431
70	4831902,920	622054,647	4831902,436	622051,411	327,200
71	4831921,267	622050,852	4831920,812	622047,843	304,321
72	4831948,056	622044,624	4831947,799	622043,160	148,639
73	4831970,777	622038,927	4831970,379	622036,978	198,922
74	4831993,183	622032,565	4831992,230	622028,614	406,431
75	4832014,791	622025,137	4832013,897	622019,557	565,116
76	4832036,794	622018,015	4832035,839	622012,421	567,493
77	4832066,990	622004,699	4832066,831	622003,090	161,684
78	4832087,519	621995,028	4832086,357	621992,836	248,095
79	4832107,647	621983,495	4832108,279	621984,035	83,128
80	4832129,562	621967,724	4832130,162	621968,749	118,770
81	4832163,289	621948,833	4832164,655	621952,585	399,293
82	4832195,775	621932,574	4832197,226	621936,664	433,976
83	4832216,089	621922,135	4832217,465	621925,987	409,039
84	4832245,556	621907,681	4832246,751	621910,243	282,699
85	4832273,976	621893,166	4832275,568	621896,717	389,154
86	4832315,282	621872,223	4832317,226	621875,447	376,475
87	4832361,188	621849,054	4832362,537	621851,805	306,395
88	4832414,333	621822,322	4832415,856	621824,787	289,754
89	4832444,889	621807,875	4832446,444	621810,535	308,117
90	4832503,659	621780,136	4832504,308	621781,911	188,993
91	4832507,695	621778,234	4832507,945	621779,365	115,830
92	4832514,451	621777,898	4832514,449	621778,192	29,401
93	4832522,051	621777,671	4832522,020	621777,770	10,374
94	4832540,733	621779,439	4832540,674	621779,981	54,520
95	4832549,060	621780,277	4832549,066	621780,636	35,905

Всички стойности на ΔS по големи от 180 cm са показани в червен цвят и представляват 68 % от анализираните стойности.

В резултат от обработката на измерванията за оценка на точността на кадастралната карта се получават три статистически реда със стойности, изчислени по формулите (1).

Проверката на хипотезата за съгласуване на емпиричното разпределение с нормалното се осъществява чрез критерия на Пирсън (χ^2) и чрез изчисление на асиметрията, ексцеса и съответните им доверителни интервали.

Проверка за съгласуваност чрез критерия на Пирсън (χ^2). Избрани са 5 интервала от -∞ до +∞. Изчислени са нормираните граници, вероятността за попадане и теоретичният и емпиричният брой грешки. Направено е изследване за груби и систематични грешки. Измервания, при които са налични груби грешки, са изключени при изследването.

Резултатите за реда ΔX са дадени в таблица 6.

Таблица 6. Резултати за реда ΔX

Действ. граници		Нормир. граници		Вероятн. за попадане		Брой грешки		Разл.	$\Delta N_j^2/N_j$
долна	горна	долна	горна	F(тд)	F(tr) - F(тд)	теорет.	емпир.	ΔN_j	χ^2_j
-∞	-2	0,000	-0,921	0,000	0,178	16,952	10,000	-6,952	2,851
-2	0	-0,921	0,000	0,178	0,322	30,548	42,000	11,452	4,293
0	2	0,000	0,921	0,500	0,322	30,548	30,000	-0,548	0,010
2	4	0,921	1,843	0,822	0,146	13,846	7,000	-6,846	3,385
4	+∞	1,843	1,000	0,967	0,033	3,106	6,000	2,894	2,697
			[ ]	1			95,000	$\chi^2_=$	13,2367

Общият брой на грешките в реда ΔX е 95.

Степента на свобода се определя с помощта на формулата (4.3.).

При стойност χ^2 = 13,2367 и степен на свобода 2 е изчислена вероятността 0,0001. Изчислената вероятност е по-малка от 0,1 и може да се твърди, че хипотезата за нормално разпределение на изследвания ред не се потвърждава.

Резултатите за реда ΔУ са дадени в таблица 7.

Таблица 7. Резултати за реда ΔУ

Действ. граници		Нормир. граници		Вероятн. за попадане		Брой грешки		Разл.	$\Delta N_j^2/N_j$
долна	горна	долна	горна	F(тд)	F(tr) - F(тд)	теорет.	емпир.	ΔN_j	χ^2_j
-∞	-2	0,000	-0,460	0,000	0,323	30,662	34,000	3,338	0,363
-2	0	-0,460	0,000	0,323	0,177	16,838	24,000	7,162	3,046
0	2	0,000	0,460	0,500	0,177	16,838	13,000	-3,838	0,875
2	4	0,460	0,920	0,677	0,144	13,677	11,000	-2,677	0,524
4	+∞	0,920	1,000	0,821	0,179	16,985	13,000	-3,985	0,935
			[ ]	1			95,000	$\chi^2_=$	5,7434

Общият брой на грешките в реда ΔУ е 95.

При стойност $\chi^2 = 5{,}7434$ и степен на свобода 2 е изчислена вероятността 0,0566. Изчислената вероятност е по-малка от 0,1 и може да се твърди, че хипотезата за нормално разпределение на изследвания ред не се потвърждава.

Резултатите за реда δS са дадени в таблица 8.

Таблица 8. Резултати за реда δS

Действ. граници		Нормир. граници		Вероятн. за попадане		Брой грешки		Разл.	$\Delta N_j^2/N_j$
долна	горна	долна	горна	F(тд)	F(тг) - F(тд)	теорет.	емпир.	ΔN_j	χ^2_j
-∞	-2	0,000	-3,217	0,000	0,001	0,058	0,000	-0,058	0,058
-2	0	-3,217	0,000	0,001	0,499	44,440	47,000	2,560	0,147
0	2	0,000	3,217	0,500	0,499	44,444	42,000	-2,444	0,134
2	4	3,217	6,434	0,999	0,001	0,058	0,000	-0,058	0,058
4	+∞	6,434	1,000	1,000	0,000	0,000	0,000	0,000	0,000
			[ ]	1			89,000	χ^2=	0,3395

Поради наличието на груби грешки в реда δS, от статистическия ред са изключени 6 на брой измервания. Общият брой на грешките в реда δS е 89.

Определя се степента на свобода за реда δS с помощта на формула (4.3.).

При стойност $\chi^2 = 0{,}3395$ и степен на свобода 2 е изчислена вероятността 0,8439. Изчислената вероятност е по-голяма от 0,1 и може да се твърди, че хипотезата за нормално разпределение на изследвания ред се потвърждава.

Резултатите от трите таблици дават основание да се счита, че двата реда нямат разпределение, близко до нормалното, а само единият ред потвърждава хипотезата за нормално разпределение.

ЗАКЛЮЧЕНИЕ

Общото състояние на изработените и впоследствие поддържани от структурите на Министерство на земеделието и храните /МЗХ/ КВС по отношение на точността не е добро поради факта, че много рядко е прилагана разпоредбата на чл. 26 от ППЗСПЗЗ за поправка на същите. Това е наложило да се приемат разпоредби, които да позволят поправка на грешките от преобразуваните КВС и ПЗ в КККР.

References

1. Андреева П., Иванова И. Прилагане на системен подход при оценка ефективността на информационните системи за кадастъра. ШУ „Еп. К. Преславски" – МАТТЕХ 2016. ISSN: 1314-3921
2. Закон за кадастъра и имотния регистър, ДВ, бр. 34, 2000
3. Закон за собствеността и ползването на земеделските земи (ЗСПЗЗ), ДВ, бр.17, 1991
4. Иванова Ил., Андреева П. Актуални въпроси в областта на кадастъра. Proceedings of International Scientific Conference 2021, Faculty of Artillery, Air Defense and Communication and Information Systems - Shumen. 483- 491 p. ISSN 2367-7902

5. Иванова Ил., Андреева П. Поддържане и повишаване на професионалната квалификация по Закона за кадастър и имотен регистър. E- Journal VFU, Архитектура и строителство, бр.14, 2021. ВСУ „Черноризец Храбър". ISSN 1313-7514.
6. Иванова, Ил. Кадастърът в България. Замисъл и изпълнение
7. Иванова, Ил. Ръководство за упражнения по кадастър
8. Концепция за ускорено създаване на кадастрална карта и кадастрални регистри и за ускоряване процеса по създаване на имотен регистър, Януари 2015 г.
9. Наредба № РД-02-20-5 от 15 декември 2016 г. за съдържанието, създаването и поддържането на кадастралната карта и кадастралните регистри, ДВ, бр.4, 2017
10. Петрова П. Информационни системи за кадастър у нас и в чужбина. Трета международна конференция „Наука, образование, иновации" кн. II Шумен, 21-23 май 2014 г., стр. 196-204. ISBN: 978-954-577-969-5.
11. Andreeva P. Technology for applying a methodology for conducting empirical sociological surveys of the effectiveness of the cadaster information system. PROCEEDINGS OF UNIVERSITY OF RUSE - 2020, volume 59. Copyrights© 2020 ISSN 1311-3321 (print), ISSN 2535-1028 (CD-ROM), ISSN 2603-4123 (on-line). ISSN 2367-7902
12. https://kais.cadastre.bg – АГКК КАИС - портал за електронни услуги
13. http://www.cadastre.bg/ - Агенция по геодезия, картография и кадастър

RELATIONSHIP BETWEEN IMAGE COORDINATES OF CHARACTERISTIC POINTS OF A STEREO PAIR OF PHOTOGRAPHS

Monika B. Bedzheva

Department Artillery and Geodesy, Vasil Levski National Military University, Shumen, Bulgaria, monibedzh17@abv.bg

***Abstract**: In photogrammetry an important condition for building three-dimensional (3D) model is the complanarity of the eponymous projecting rays. This means that the photographs forming the stereo pairs should be mutual orientated. In this paper, taking into account the capabilities of unmanned aerial vehicles (UAVs), the relationship between image coordinates of characteristic points of a stereo pair of photographs is described and analyzed and the well-known fundamental condition for zero vertical (transverse) parallax of the eponymous projecting rays is derived and proved.*

***Keywords**: UAV, stereo pairs, image points, projecting rays, vertical parallax*

Introduction

Nowadays unmanned aerial vehicles (UAVs) find applications in many areas of life, including film and video-making, agriculture, rescue operations, sports, just to name a few. But they really revolutionazied one field of science – photogrammetry. Today, instead of using large and expensive aircrafts to photograph the land, UAVs are used and they do this task fast, cheap, easy and with high quality.

One of the prodults of the photogrammetric processing is a three-dimensional (3D) model of the shooted scene (land or vertical object) [1], [5], [6]. In order this 3D model to be made, the condition of complanarity of the eponymous projecting rays must be met. In the paper this condition is described and analyzed using vector equasions and solving them with Cramer's rule, known also as the rule of determinants. This approach is understandable and visual and is used to derive the well-known fundamental condition for zero vertical (transverse) parallax.

Mathematical model of the processing of information on a stereo pair of images obtained with a UAV

In a most general situation, a single photograph does not allow the creation of a three-dimensional model of the earth's surface. However, this is possible if the studied terrain is captured simultaneously with two photographs, which is commonly called a *stereo pair*.

Indeed, let the stereo pair of photos P_1, P_2, whose projection centers are S_1, S_2 (fig. 1), have the images m_1, m_2 of the point M of the studied terrain, respectively. If the position of the photos P_1, P_2, relative to some local coordinate system (CS) $OXYZ$ is known, then the coordinates of point M in this CS are calculated as follows [2], [3], [4].

From fig. 1 it is seen that since the vectors r_1 and $r_2$are collinear to the vectors R_1 and R_2 respectively, it is satisfied

$$R_1 = k_{m_1} r_1, \quad R_2 = k_{m_2} r_2. \tag{1}$$

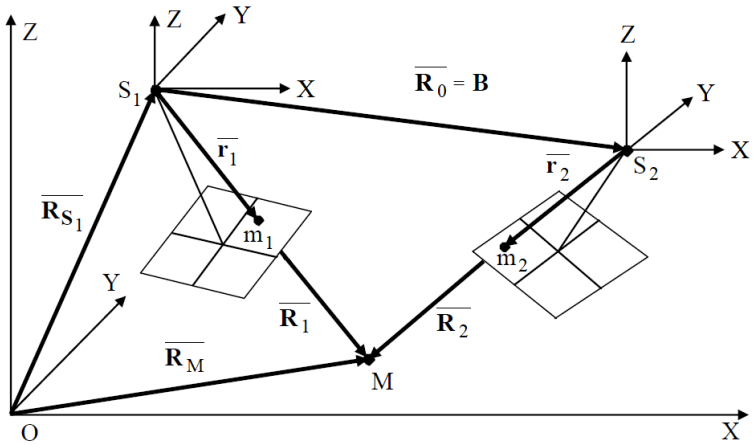


Figure 1: A geometric model of the formation of a stereo pair of photos using UAV

In (1) k_{m_1} and k_{m_2} are scalar multipliers. From fig. 1 also follows that

$$S_1S_2 = R_0 = R_1 - R_2. \tag{2}$$

Now let photogrammetric CS S_1XYZ and CS S_2XYZ are obtained after parallel translations of local CS $OXYZ$. Moreover, let B_X, B_Y, B_Z and $X'_{m_1}, Y'_{m_1}, Z'_{m_1}$ be the coordinates of the right projection center S_2 and of the point m_1 in CS S_1XYZ, and $X'_{m_2}, Y'_{m_2}, Z'_{m_2}$ are the coordinate points at point m_2 in CS S_2XYZ.

Under these assumptions and given (1), the vector relation (2) is equivalent to the following system of three equations:

$$\begin{aligned} k_{m_1}X'_{m_1} - k_{m_2}X'_{m_2} &= B_X \\ k_{m_1}Y'_{m_1} - k_{m_2}Y'_{m_2} &= B_Y \\ k_{m_1}Z'_{m_1} - k_{m_2}Z'_{m_2} &= B_Z \end{aligned} \tag{3}$$

The following circumstances should be specially noted here.

First, the coordinates $X_{S_1}, Y_{S_1}, Z_{S_1}$, $X_{S_2}, Y_{S_2}, Z_{S_2}$ of the projection centers S_1, S_2 respectively are determined by the UAV GNSS (Global Navigation Satellite System) receiver in some global geodetic system. As a result, the length of the base of photography

$$B = S_1S_2 = R_0 = \sqrt{X_{S_2} - X_{S_1}^{\ 2} + Y_{S_2} - Y_{S_1}^{\ 2} + Z_{S_2} - Z_{S_1}^{\ 2}} \tag{4}$$

is determined with centimeter accuracy.

It can be seen from (4) that if the CS $OXYZ$ (fig. 1) coincides with the global geodetic system used by the UAV, then:

$$B_X = X_{S_2} - X_{S_1}, \quad B_Y = Y_{S_2} - Y_{S_1}, \quad B_Z = Z_{S_2} - Z_{S_1}. \tag{5}$$

In addition, through the methods that will be analyzed in the next papers, the exact determination of B allows to calculate the coordinates B_X, B_Y, B_Z of the basis of photography in the so-called base and linear-angular CS, which find the greatest application in the creation of photogrammetric models of terrains photographed by UAV.

Second, at the beginning of this paper it was stated that the orientation of the photos P_1, P_2 relative to the selected local CS $OXYZ$ is known. This means that

$$X'_{m_1} = a'_1 x_{m_1} + a'_2 y_{m_1} - a'_3 f,$$
$$Y'_{m_1} = b'_1 x_{m_1} + b'_2 y_{m_1} - b'_3 f, \quad Z'_{m_1} = c'_1 x_{m_1} + c'_2 y_{m_1} - c'_3 f, \tag{6}$$

$$X'_{m_2} = a''_1 x_{m_2} + a''_2 y_{m_2} - a''_3 f,$$
$$Y'_{m_2} = b''_1 x_{m_2} + b''_2 y_{m_2} - b''_3 f, \quad Z'_{m_2} = c''_1 x_{m_2} + c''_2 y_{m_2} - c''_3 f. \tag{7}$$

In (6), (7) $x_{m_1}, y_{m_1}, -f$ and $x_{m_2}, y_{m_2}, -f$ are the coordinates of point m_1 and point m_2 in intermediate CS $S_1x_1y_1z_1$ and $S_2x_2y_2z_2$ of the photos P_1, P_2 respectively. Furthermore,

$$a'_1 = cos\alpha'_1 cos\chi'_1 - sin\alpha'_1 sin\omega'_1 sin\chi'_1,$$
$$a'_2 = -cos\alpha'_1 sin\chi'_1 - sin\alpha'_1 sin\omega'_1 cos\chi'_1,$$
$$a'_3 = -sin\alpha'_1 cos\omega'_1,$$
$$a''_1 = cos\alpha'_2 cos\chi'_2 - sin\alpha'_2 sin\omega'_2 sin\chi'_2,$$
$$a''_2 = -cos\alpha'_2 sin\chi'_2 - sin\alpha'_2 sin\omega'_2 cos\chi'_2,$$
$$a''_3 = -sin\alpha'_2 cos\omega'_2,$$

$$b'_1 = cos\omega'_1 sin\chi'_1, \quad b''_1 = cos\omega'_2 sin\chi'_2,$$
$$b'_2 = cos\omega'_1 cos\chi'_1, \quad b''_2 = cos\omega'_2 cos\chi'_2, \tag{8}$$
$$b'_3 = 0, \quad b''_3 = -sin\omega'_2,$$

$$c'_1 = sin\alpha'_1 cos\chi'_1 + cos\alpha'_1 sin\omega'_1 sin\chi'_1,$$
$$c'_2 = -sin\alpha'_1 sin\chi'_1 + cos\alpha'_1 sin\omega'_1 cos\chi'_1,$$
$$c'_3 = cos\alpha'_1 cos\omega'_1,$$
$$c''_1 = sin\alpha'_2 cos\chi'_2 + cos\alpha'_2 sin\omega'_2 sin\chi'_2,$$
$$c''_2 = -sin\alpha'_2 sin\chi'_2 + cos\alpha'_2 sin\omega'_2 cos\chi'_2,$$
$$c''_3 = cos\alpha'_2 cos\omega'_2,$$

are the so-called guiding cosines [2], [3], [4]. They are calculated on the basis of the known values $\alpha'_1, \omega'_1, \chi'_1$, $\alpha'_2, \omega'_2, \chi'_2$ of the angular elements of orientation of CS $S_1x_1y_1z_1$, $S_2x_2y_2z_2$ relative to photogrammetric CS S_1XYZ (fig. 1).

From the given arguments, it can be seen that in the conditions of modern UAVs, the system of three equations (3) has only two unknowns – k_{m_1}, k_{m_2}. Although the number of unknowns is less than the number of equations, ideally, when all the constants $X'_{m_1}, Y'_{m_1}, Z'_{m_1}$, $X'_{m_2}, Y'_{m_2}, Z'_{m_2}$, B_X, B_Y, B_Z are measured or calculated absolutely exactly, the system (3) is compatible and has a solution. This solution can be found analytically by dividing the system (3) into 3 systems of two equations with two unknowns, grouping the first and second equations, the first and third equations, and the second and third equations:

$$X'_{m_1} k_{m_1} - X'_{m_2} k_{m_2} = B_X$$
$$Y'_{m_1} k_{m_1} - Y'_{m_2} k_{m_2} = B_Y \tag{9}$$

$$X'_{m_1} k_{m_1} - X'_{m_2} k_{m_2} = B_X$$
$$Z'_{m_1} k_{m_1} - Z'_{m_2} k_{m_2} = B_Z \tag{10}$$

$$Y'_{m_1} k_{m_1} - Y'_{m_2} k_{m_2} = B_Y$$
$$Z'_{m_1} k_{m_1} - Z'_{m_2} k_{m_2} = B_Z \tag{11}$$

The result of solving the system (9) by the so-called Cramer's rule (rule of determinants) is:

$$k_{m_1} = \frac{\begin{matrix} B_X & -X'_{m_2} \\ B_Y & -Y'_{m_2} \end{matrix}}{\begin{matrix} X'_{m_1} & -X'_{m_2} \\ Y'_{m_1} & -Y'_{m_2} \end{matrix}} = \frac{-B_X Y'_{m_2} + B_Y X'_{m_2}}{-X'_{m_1} Y'_{m_2} + Y'_{m_1} X'_{m_2}},$$
$$k_{m_2} = \frac{\begin{matrix} X'_{m_1} & B_X \\ Y'_{m_1} & B_Y \end{matrix}}{\begin{matrix} X'_{m_1} & -X'_{m_2} \\ Y'_{m_1} & -Y'_{m_2} \end{matrix}} = \frac{B_Y X'_{m_1} - B_X Y'_{m_1}}{-X'_{m_1} Y'_{m_2} + Y'_{m_1} X'_{m_2}}. \quad (12)$$

The solutions of the systems (10) and (11) are found analogously:

$$k_{m_1} = \frac{\begin{matrix} B_X & -X'_{m_2} \\ B_Z & -Z'_{m_2} \end{matrix}}{\begin{matrix} X'_{m_1} & -X'_{m_2} \\ Z'_{m_1} & -Z'_{m_2} \end{matrix}} = \frac{-B_X Z'_{m_2} + B_Z X'_{m_2}}{-X'_{m_1} Z'_{m_2} + Z'_{m_1} X'_{m_2}},$$
$$k_{m_2} = \frac{\begin{matrix} X'_{m_1} & B_X \\ Z'_{m_1} & B_Z \end{matrix}}{\begin{matrix} X'_{m_1} & -X'_{m_2} \\ Z'_{m_1} & -Z'_{m_2} \end{matrix}} = \frac{B_Z X'_{m_1} - B_X Z'_{m_1}}{-X'_{m_1} Z'_{m_2} + Z'_{m_1} X'_{m_2}}, \quad (13)$$

$$k_{m_1} = \frac{\begin{matrix} B_Y & -Y'_{m_2} \\ B_Z & -Z'_{m_2} \end{matrix}}{\begin{matrix} Y'_{m_1} & -Y'_{m_2} \\ Z'_{m_1} & -Z'_{m_2} \end{matrix}} = \frac{-B_Y Z'_{m_2} + B_Z Y'_{m_2}}{-Y'_{m_1} Z'_{m_2} + Z'_{m_1} Y'_{m_2}},$$
$$k_{m_2} = \frac{\begin{matrix} Y'_{m_1} & B_Y \\ Z'_{m_1} & B_Z \end{matrix}}{\begin{matrix} Y'_{m_1} & -Y'_{m_2} \\ Z'_{m_1} & -Z'_{m_2} \end{matrix}} = \frac{B_Z Y'_{m_1} - B_Y Z'_{m_1}}{-Y'_{m_1} Z'_{m_2} + Z'_{m_1} Y'_{m_2}}. \quad (14)$$

As noted above, with sufficient accuracy of determination of the constants in the system (3), it is compatible (i.e. has a solution). Therefore, the solutions (12), (13) and (14) must coincide:

$$\frac{-B_X Y'_{m_2} + B_Y X'_{m_2}}{-X'_{m_1} Y'_{m_2} + Y'_{m_1} X'_{m_2}} = \frac{-B_X Z'_{m_2} + B_Z X'_{m_2}}{-X'_{m_1} Z'_{m_2} + Z'_{m_1} X'_{m_2}} = \frac{-B_Y Z'_{m_2} + B_Z Y'_{m_2}}{-Y'_{m_1} Z'_{m_2} + Z'_{m_1} Y'_{m_2}},$$
$$\frac{B_Y X'_{m_1} - B_X Y'_{m_1}}{-X'_{m_1} Y'_{m_2} + Y'_{m_1} X'_{m_2}} = \frac{B_Z X'_{m_1} - B_X Z'_{m_1}}{-X'_{m_1} Z'_{m_2} + Z'_{m_1} X'_{m_2}} = \frac{B_Z Y'_{m_1} - B_Y Z'_{m_1}}{-Y'_{m_1} Z'_{m_2} + Z'_{m_1} Y'_{m_2}}. \quad (15)$$

Now it should be noted that:

$$R_M = R_{S_1} + R_1 = R_{S_1} + R_0 + R_2 \quad (16)$$

The vector ratio (16) is equivalent to the following system of three equalities:

$$\begin{aligned} X_M &= X'_{S_1} + k_{m_1} X'_{m_1} = X'_{S_1} + B_X + k_{m_2} X'_{m_2} \\ Y_M &= Y'_{S_1} + k_{m_1} Y'_{m_1} = Y'_{S_1} + B_Y + k_{m_2} Y'_{m_2} \\ Z_M &= Z'_{S_1} + k_{m_1} Z'_{m_1} = Z'_{S_1} + B_Z + k_{m_2} Z'_{m_2} \end{aligned} \quad (17)$$

In (17) $X'_{S_1}, Y'_{S_1}, Z'_{S_1}$ and $X'_{S_2} = X'_{S_1} + B_X, Y'_{S_2} = Y'_{S_1} + B_Y, Z'_{S_2} = Z'_{S_1} + B_Z$ are the coordinates of the projection centers S_1, S_2 of the photos P_1, P_2 respectively, and X_M, Y_M, Z_M are the sought coordinates of point M from the studied terrain in the local CS $OXYZ$ of the geometric model in fig. 1.

Formulas (16) and (17) are invariant relative to the used local CS, and as such, any CS that simplifies the process of processing photo information can be used. The only mandatory requirement is that the orientation of the intermediate CS $S_1 x_1 y_1 z_1$, $S_2 x_2 y_2 z_2$ (of the photos P_1, P_2) relative to the local CS $OXYZ$ (fig. 1) be known.

The following facts should be specially noted here.

First, in photogrammetry the problem analyzed in this paper is commonly called *a straight photogrammetric resection*.

Second, from (17) the following system of equalities is obtained:

$$\begin{aligned} k_{m_1}X'_{m_1} - k_{m_2}X'_{m_2} &= B_X \\ k_{m_1}Y'_{m_1} - k_{m_2}Y'_{m_2} &= B_Y \\ k_{m_1}Z'_{m_1} - k_{m_2}Z'_{m_2} &= B_Z \end{aligned} \tag{18}$$

Now let the orientation of the photos P_1, P_2 relatively the selected local CS $OXYZ$ and the coordinates $x_{m_1}, y_{m_1}, -f$ of point m_1 in the intermediate CS $S_1x_1y_1z_1$ of the photo P_1 be known, and the coordinates $x_{m_2}, y_{m_2}, -f$ of point m_2 in intermediate CS $S_2x_2y_2z_2$ in photo P_2 are unknown. Then, taking x_{m_2} as a parameter, from (6), (7) and (18) we obtain the following system of three equations with three unknowns ($k_{m_1}, k_{m_2}, y_{m_2}$) and one parameter ($x_{m_2}$):

$$\begin{aligned} X'_{m_1}k_{m_1} - \ a''_1x_{m_2} - a''_3f\ \ k_{m_2} + a''_2\ \ k_{m_2}y_{m_2} \ &= B_X \\ Y'_{m_1}k_{m_1} - \ b''_1x_{m_2} - b''_3f\ \ k_{m_2} + b''_2\ \ k_{m_2}y_{m_2} \ &= B_Y \\ Z'_{m_1}k_{m_1} - \ c''_1x_{m_2} - c''_3f\ \ k_{m_2} + c''_2\ \ k_{m_2}y_{m_2} \ &= B_Z \end{aligned} \tag{19}$$

Using Cramer's rule (the rule of determinants) it is found that the solution of (19) is:

$$k_{m_1} = \frac{\begin{matrix} B_X & - a''_1x_{m_2} - a''_3f & a''_2 \\ B_Y & - b''_1x_{m_2} - b''_3f & b''_2 \\ B_Z & - c''_1x_{m_2} - c''_3f & c''_2 \end{matrix}}{\begin{matrix} X'_{m_1} & - a''_1x_{m_2} - a''_3f & a''_2 \\ Y'_{m_1} & - b''_1x_{m_2} - b''_3f & b''_2 \\ Z'_{m_1} & - c''_1x_{m_2} - c''_3f & c''_2 \end{matrix}},$$

$$k_{m_2} = \frac{\begin{matrix} X'_{m_1} & B_X & a''_2 \\ Y'_{m_1} & B_Y & b''_2 \\ Z'_{m_1} & B_Z & c''_2 \end{matrix}}{\begin{matrix} X'_{m_1} & - a''_1x_{m_2} - a''_3f & a''_2 \\ Y'_{m_1} & - b''_1x_{m_2} - b''_3f & b''_2 \\ Z'_{m_1} & - c''_1x_{m_2} - c''_3f & c''_2 \end{matrix}}, \tag{20}$$

$$k_{m_2}y_{m_2} = \frac{\begin{matrix} X'_{m_1} & - a''_1x_{m_2} - a''_3f & B_X \\ Y'_{m_1} & - b''_1x_{m_2} - b''_3f & B_Y \\ Z'_{m_1} & - c''_1x_{m_2} - c''_3f & B_Z \end{matrix}}{\begin{matrix} X'_{m_1} & - a''_1x_{m_2} - a''_3f & a''_2 \\ Y'_{m_1} & - b''_1x_{m_2} - b''_3f & b''_2 \\ Z'_{m_1} & - c''_1x_{m_2} - c''_3f & c''_2 \end{matrix}}.$$

Therefore

$$y_{m_2} = \frac{k_{m_2}y_{m_2}}{k_{m_2}} = \frac{\begin{matrix} X'_{m_1} & - a''_1x_{m_2} - a''_3f & B_X \\ Y'_{m_1} & - b''_1x_{m_2} - b''_3f & B_Y \\ Z'_{m_1} & - c''_1x_{m_2} - c''_3f & B_Z \end{matrix}}{\begin{matrix} X'_{m_1} & B_X & a''_2 \\ Y'_{m_1} & B_Y & b''_2 \\ Z'_{m_1} & B_Z & c''_2 \end{matrix}}. \tag{21}$$

The practical significance of (21) arises from the following circumstances.

First, in the most general situation, the process of calculating the spatial coordinates of the points of the photographed area starts by grouping into pairs the images of the points on the pictures P_1 and P_2. Since each photo has $N_{pa} \times N_{pb}$ pixels, the amount of N_{ch} checks to form the pairs is

$$N_{ch} = N_{pa}^2 N_{pb}^2. \tag{22}$$

Since y_{m_2} is determined by x_{m_1}, y_{m_1} and x_{m_2} according to (21), the amount of checks N_{ch} reduces to

$$N_{ch} = N_{pa}^2 N_{pb}. \tag{23}$$

In the ideal shooting case, when the stereo pair of photos P_1, P_2 are strictly parallel to the surface of the ellipsoid, and the base of photography is also parallel to the surface of the ellipsoid and coincides with the direction "West – East" (i.e. $B_Y = B_Z = 0$), then (19) simplifies to the form

$$\begin{gathered} x_{m_1} k_{m_1} - x_{m_2} k_{m_2} = B_X \\ y_{m_1} k_{m_1} - k_{m_2} y_{m_2} = 0 \\ -f k_{m_1} + f k_{m_2} = 0 \end{gathered} \tag{24}$$

Therefore $k_{m_1} = k_{m_2}$ and

$$y_{m_2} = y_{m_1}, \tag{25}$$

which is the known condition for zero vertical (transverse) parallax.

Conclusion

In the paper the mathematical model of the processing of information on a stereo pair of images obtained with a UAV is described and the relationship between image coordinates of characteristic points of a stereo pair of photographs is analized. Using vector equasions and solving them with Cramer's rule the known condition for zero vertical (transverse) parallax is derived and proved.

Acknowledgments

This paper is written thanks to project BG05M2OP001-2.016-0003 "Modernization of Vasil Levski National Military University – Veliko Tarnovo and Sofia University "St. Kliment Ohridski" – Sofia in professional direction 5.3 Computer and communication technology", financed by the operational program "Science and education for intelligent growth".

References

1. Andreev A., Andreeva P. (2009) Creating a digital terrain model of the database for subsequent topographic maps in GIS environment. *Artillery review magazine, book 3*, pp. 17- 31, ISBN 1314-0388.
2. Krasnopevtsev, B. (2008). *Photogrammetry.* Moscow: Moscow National University of Geodesy and Cartography
3. Lobanov, A. (1984). *Photogrammetry.* Moscow: Nedra
4. Nazarov, A. (2006). *Photogrammetry.* Moscow: Tetra Systems
5. Niyazi-Yusuf, M. (2021) Assessment of the actuality of the content and accuracy of the current cadastral plans, *Annual of FTS*, Vol. XI E, Shumen, Bishop Konstantin Preslavsky University press, pp. 59-62, ISSN: 1311-834X
6. Prokopov, Y., (2021). Capabilities of terrestrial laser scanning – a basis for geodetic modeling, *International Scientific Conference -Defense Technologies, DefTech*, 06-08.10.2021, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, pp. 467-473, ISSN 2367-7902.

METHODOLOGY FOR BUILDING A SINGLE PHOTOGRAMMETRIC MODEL

Monika B. Bedzheva

Department Artillery and Geodesy, Vasil Levski National Military University, Shumen, Bulgaria, monibedzh17@abv.bg

***Abstract**: The purpose of photogrammetric processing of photos is to obtain spatial informaion about objects situated on earth's suface and the surface itself. For this reason a series of overlapping images is taken with UAV (unmanned aerial vehicle) camera, which are called stereo pairs. From these stereo pairs a three-dimensional (3D) model of the surface is build and the spatial coordinates of each point can be extracted. Such 3D model made from single stereo pair without georeferencing is called single photogrammetric model and the means of obtainig it are discussed in this paper.*

***Keywords**: Single photogrammetric model, basic coordinate system, linear-angular coordinate system, characteristic points, tie points*

Introduction

One of the main geodetic tasks is to obtain spatial information about earth's surface and the objects situated on it. This task can be done either using geodetic means like classical or GNSS (Global Navigation Satellite System) measurements, or using photogrammetric means like building 3D model from stereo pairs of photos [1], [6], [7]. These models are two types. In the first model ground control points (GCPs) are used to orientate the model in the global geodetic system, like WGS84. Such model is called *georeferenced model* and is used to extract real spatial coordinates.

The second model can be made in arbitrary coordinate system (CS) and in arbitrary scale. Such model, obtained from one stereo pair and without GCPs is called *photogrammetric model*. Its location in space is shifted from its real one, so real spatial coordinates cannot be obtained. However, if its scale is 1:1 the relative location of the points can be determined and a general evaluation of the captured scene – terrain or vertical object – can be made.

1. Conditions for building a single photogrammetric model

It is known from the general theory of photogrammetry that under fairly general conditions it is possible to determine the surface formed by the set of points where the corresponding (eponymous) projecting rays intersect [3], [4], [5]. This result is demonstrated in fig. 1.

In the following, this surface will be called the *photogrammetric model* of the photographed object (terrain), since its coordinate system (CS) is photogrammetric. This means that its particular selection provides the simplest view of the dependencies between the model points and the captured object (terrain).

In principle, the task of creating a photogrammetric model of a photographed object (terrain) can be solved with instrumental or analytical methods.

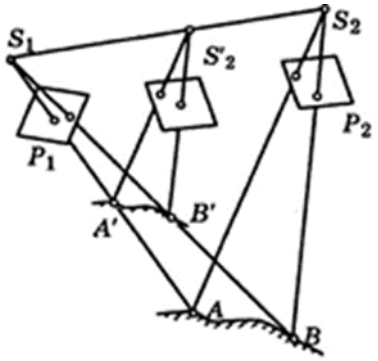


Figure 1: Determination of the surface, defined by the intersections of the projecting rays of photos P_1 and P_2

The instrumental method is based on the use of optical-mechanical, mechanical and/or optical instruments for analog modeling of the operations for internal and mutual orientation of the photographs, as well as for determining the position of the points of the photographed objects (terrain). Here it should be specially noted that the instrumental method is actually applicable in view of the following facts.

First, the photogrammetric model of the captured object can be built at any scale. Indeed, if the real photography basis $S_1S_2 = B$ is replaced by the shorter basis $S_1S_2' = B'$ (fig. 1), then the scale of the photogrammetric model will be:

$$\frac{1}{k_m} = \frac{B'}{B}. \quad (1)$$

Second, the photogrammetric terrain model is not destroyed if the two bundle links are turned or tilted in any direction at the same time without changing their relative position.

The following conclusions arise from these facts.

The photogrammetric model of the object can be built in:

- arbitrary scale allowing the fabrication of the optical-mechanical, mechanical and/or optical instruments for analog modeling with dimensions that are acceptable from a technical point of view;
- an arbitrary CS, after which it can be converted into a CS fully tailored to the specific practical goals, using ground control points (GCPs) or other data; the last operation is called *external (geodetic) orientation*.

In connection with the first conclusion, it should be noted that the construction of a photogrammetric model of a photographed object does not depend on the specific coordinates of the projection centers S_1, S_2. This circumstance allows the creation of three-dimensional (3D) digital models of buildings, bridges, monuments, etc., which are simply photographed with a digital camera without using GNSS (Global Navigation Satellite System) receivers. This fact is explained in fig. 2.

The analytical method is based on mathematical modeling of the processes in building a photogrammetric model according to the strict dependencies discussed in the next paper. It can be performed in basic, linear-angular or arbitrary CS [3], [4], [5].

The analytical method is used in the analytical photogrammetric instruments and in the digital photogrammetric systems.

What is presented in [4], [5] makes it possible to justify the following detailed methodology for building a photogrammetric model of terrain photographed with a UAV according to the analytical method, which in the specialized literature is accepted to be called *a single photogrammetric model*.

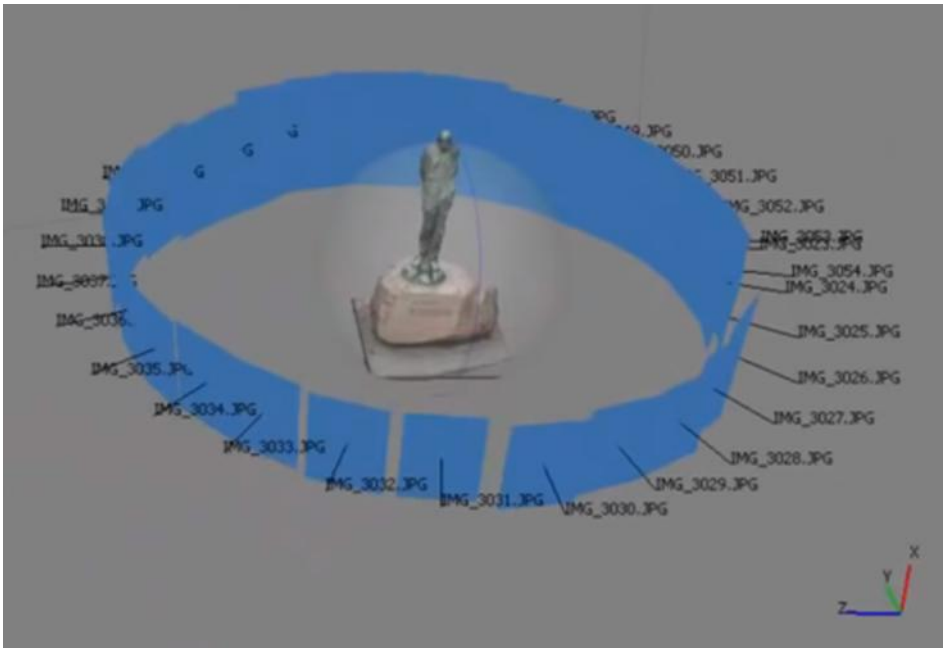


Figure 2: 3D digital model of monument
(research conducted under the supervision of the author of the paper)

2. Methodology for building a single photogrammetric model

Step 1) Determination of all points on the captured section of the stereo pair whose images on the left and right photos have similar brightness and spectral characteristics. In digital photogrammetry systems, this operation is performed automatically by a special program module using computer vision, called a *correlator*.

These points form the set of characteristic points (CP, points of interest).

Step 2) Selection of tie points (TP) $\{D_{P_1 i}, D_{P_2 i}\}, i = 1, 2, \dots, N_{tp}$, $5 \le N_{tp} \le 18$, which are a subset of the full set of CP. It should be noted here that the use of more than $N_{tp} = 18$ TPs is impractical, since the load on the computer system in processing the photo information increases significantly, while the improvement in the accuracy of mutual orientation of the two photos is small.

Step 3) Determination of the coordinates $x_{m_{1k}}, y_{m_{1k}}$, $x_{m_{2k}}, y_{m_{2k}}$ $k = 1, 2, \dots, N_{tp}, N_{tp} \ge 5$ of all TPs in the image CS $o_1 x_1 y_1$ and $o_2 x_2 y_2$ of the left and right pictures, respectively.

Step 4) Determination of the external orientation elements $\alpha'_1, \alpha'_2, \omega'_2, \chi'_1, \chi'_2$, $\tau', \nu', \Delta\alpha, \Delta\omega, \Delta\chi$ of the two pictures in the basic or linear-angular CS respectively, using the image coordinates $x_{m_{1k}}, y_{m_{1k}}$, $x_{m_{2k}}, y_{m_{2k}}$ $k = 1, 2, \dots, N_{tp}, N_{tp} \ge 5$ of all TPs.

Step 5) Completion of the image coordinates measured at Step 3 $x_{m_{1k}}, y_{m_{1k}}$, $x_{m_{2k}}, y_{m_{2k}}$ to coordinates from the intermediate CS $x_{m_{1k}}, y_{m_{1k}}, -f$, $x_{m_{2k}}, y_{m_{2k}}, -f$ of all CPs and their transformation into coordinates $X'_{m_{1k}}, Y'_{m_{1k}}, Z'_{m_{1k}}$, $X'_{m_{2k}}, Y'_{m_{2k}}, Z'_{m_{2k}}$ from the photogrammetric CS of the photogrammetric model.

In this step, the guide cosines are first calculated for the left and right pictures respectively:

$$T' = \begin{matrix} a'_1 & a'_2 & a'_3 \\ b'_1 & b'_2 & b'_3 \\ c'_1 & c'_2 & c'_3 \end{matrix}, \quad T'' = \begin{matrix} a''_1 & a''_2 & a''_3 \\ b''_1 & b''_2 & b''_3 \\ c''_1 & c''_2 & c''_3 \end{matrix}, \tag{2}$$

depending on whether the basic or linear-angular CS was selected at Step 4 for the CS of the single photogrammetric model.

Then the coordinates $x_{m_{1k}}, y_{m_{1k}}, -f$, $x_{m_{2k}}, y_{m_{2k}}, -f$ of all CPs are transformed into coordinates $X'_{m_{1k}}, Y'_{m_{1k}}, Z'_{m_{1k}}$, $X'_{m_{2k}}, Y'_{m_{2k}}, Z'_{m_{2k}}$ in the CS of the single photogrammetric model.

Step 6) Calculation of the coordinates of all CPs in the CS of the single photogrammetric model. Moreover, if the basic CS was used in Step 4, then the photographing base S_1S_2 lies in the plane $S_1X'Z'$, where for each CP the geometric relations presented in fig. 3 are fullfiled.

The comparison of fig. 1 [2] and fig. 3, shows that the coordinates $X_{M_k}, Y_{M_k}, Z_{M_k}$ of an arbitrary point M_k from the set of CPs in the basic CS are determined by the ratios:

$$\begin{aligned} X_{M_k} &= X'_{S_1} + k_{m_{1k}} X'_{m_{1k}} = \frac{B_X Z'_{m_{2k}}}{X'_{m_{1k}} Z'_{m_{2k}} - Z'_{m_{1k}} X'_{m_{2k}}} X'_{m_{1k}} \\ Y_{M_k} &= Y'_{S_1} + k_{m_{1k}} Y'_{m_{1k}} = \frac{B_X Z'_{m_{2k}}}{X'_{m_{1k}} Z'_{m_{2k}} - Z'_{m_{1k}} X'_{m_{2k}}} Y'_{m_{1k}} \\ Z_{M_k} &= Z'_{S_1} + k_{m_{1k}} Z'_{m_{1k}} = \frac{B_X Z'_{m_{2k}}}{X'_{m_{1k}} Z'_{m_{2k}} - Z'_{m_{1k}} X'_{m_{2k}}} Z'_{m_{1k}} \end{aligned} \tag{3}$$

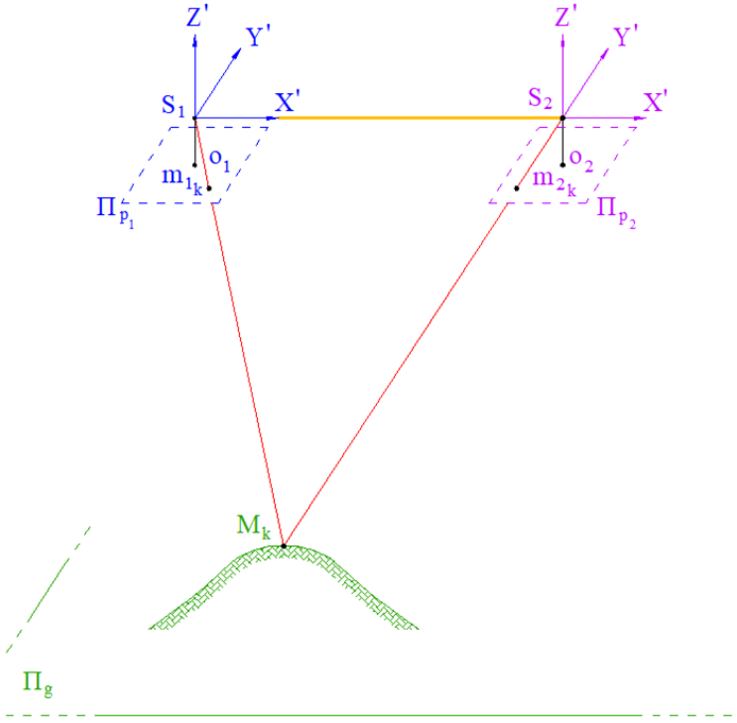


Figure 3: Single photogrammetric model after mutual orientation of the images from the stereo pair in the basic CS

The ratios (3) are obtained after substitution by

$$\begin{aligned} B_X = B = \sqrt{\left(X_{S_2} - X_{S_1}\right)^2 + \left(Y_{S_2} - Y_{S_1}\right)^2 + \left(Z_{S_2} - Z_{S_1}\right)^2}, \\ B_Y = B_Z = 0, \quad X'_{S_1} = Y'_{S_1} = Z'_{S_1} = 0. \end{aligned} \tag{4}$$

If at Step 4 the linear-angular CS was used, then for each CP the geometric ratios presented in fig. 4 are fullfiled. It is not difficult to notice that the geometrical ratios of fig. 4 and fig. 1 [2], are completely analogous.

Therefore, the coordinates $X_{M_k}, Y_{M_k}, Z_{M_k}$ of an arbitrary point M_k from the set of CPs in the linear-angular CS are determined by the relations:

$$X_{M_k} = x'_{S_1} + k_{m_{1k}} x'_{m_{1k}} = \frac{B_X Z'_{m_{2k}} - B_Z X'_{m_{2k}}}{X'_{m_{1k}} Z'_{m_{2k}} - Z'_{m_{1k}} X'_{m_{2k}}} x'_{m_{1k}}$$
$$Y_{M_k} = y'_{S_1} + k_{m_{1k}} y'_{m_{1k}} = \frac{B_X Z'_{m_{2k}} - B_Z X'_{m_{2k}}}{X'_{m_{1k}} Z'_{m_{2k}} - Z'_{m_{1k}} X'_{m_{2k}}} y'_{m_{1k}} \quad (5)$$
$$Z_{M_k} = z'_{S_1} + k_{m_{1k}} z'_{m_{1k}} = \frac{B_X Z'_{m_{2k}} - B_Z X'_{m_{2k}}}{X'_{m_{1k}} z'_{m_{2k}} - Z'_{m_{1k}} X'_{m_{2k}}} z'_{m_{1k}}$$

The ratios (5) are obtained after substitution by

$$B = \sqrt{X_{S_2} - X_{S_1}{}^2 + Y_{S_2} - Y_{S_1}{}^2 + Z_{S_2} - Z_{S_1}{}^2}, \quad (6)$$
$$B_X = B\cos\tau'\cos\nu',\ B_Y = B\sin\tau'\cos\nu',\ B_Z = B\sin\nu',\ x'_{S_1} = y'_{S_1} = z'_{S_1} = 0.$$

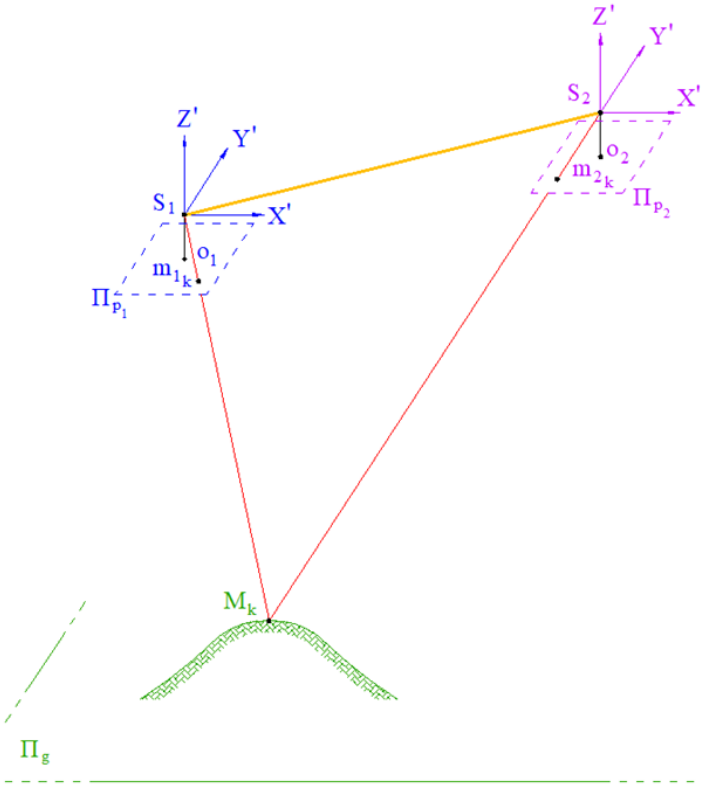


Figure 4: Single photogrammetric model after mutual orientation of the images from the stereo pair in the linear-angular CS

The following circumstances should be specially noted here.

First, the single photogrammetric models constructed with the above-presented methodology are free, in the sense that their basic or linear-angular CS may be oriented arbitrarily relative to the geodetic system used by the UAV's GNSS receiver.

Second, modern UAVs with a single take-off can fly around and take a series of consecutive photos of large terrains, the area of which is on the order of tens or even hundreds of acres. This results in a series of stereo pair photos.

Applying the above-described methodology to the series of stereo-pair images during a single UAV flight allows a free photogrammetric model of the entire captured terrain to be obtained, using only tie points.

Conclusion

In this paper a methodology for building a single photogrammetric model using basic and linear-angular CS is discussed and analized. It is shown that a free photogrammetric model can be obtained using only tie points and that such a model, although not georeferenced, can still be used for points relative location determination and general evaluation of a captured scene.

Acknowledgments

This paper is written thanks to project BG05M2OP001-2.016-0003 "Modernization of Vasil Levski National Military University – Veliko Tarnovo and Sofia University "St. Kliment Ohridski" – Sofia in professional direction 5.3 Computer and communication technology", financed by the operational program "Science and education for intelligent growth".

References

1. Andreev A., Andreeva P. (2009) Creating a digital terrain model of the database for subsequent topographic maps in GIS environment. *Artillery review magazine, book 3,* pp. 17- 31, ISBN 1314-0388.
2. Bedzheva, M. (2022) Relationship between image coordinates of characteristic points of a stereo pair of photographs, *Proceedings of International Scientific Conference "Defense Technologies"* DefTech 2022, Faculty of Artillery, Air Defense and Communication and Information Systems (in print)
3. Krasnopevtsev, B. (2008). *Photogrammetry.* Moscow: Moscow National University of Geodesy and Cartography
4. Lobanov, A. (1984). *Photogrammetry.* Moscow: Nedra
5. Nazarov, A. (2006). *Photogrammetry.* Moscow: Tetra Systems
6. Niyazi-Yusuf, M. (2021) Assessment of the actuality of the content and accuracy of the current cadastral plans, *Annual of FTS*, Vol. XI E, Shumen, Bishop Konstantin Preslavsky University press, pp. 59-62, ISSN: 1311-834X
7. Prokopov, Y., (2021). Capabilities of terrestrial laser scanning – a basis for geodetic modeling, *International Scientific Conference -Defense Technologies, DefTech*, 06-08.10.2021, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, pp. 467-473, ISSN 2367-7902.

A METHOD FOR BUILDING A PHOTOGRAMMETRIC MODEL OF AN AREA PHOTOGRAPHED WITH AN UAV

Monika B. Bedzheva

Department Artillery and Geodesy, Vasil Levski National Military University, Shumen, Bulgaria, monibedzh17@abv.bg

***Abstract**: One of the photogrammetric processing products is a three-dimensional (3D) model of a captured scene. From such a model an orthophotomosaic is obtained that is free from distortion and can be used for map production. In order to do that the 3D model must be georeferenced. Usually ground control points (GCPs) are used, but this means more time spend on terrain. Today modern unmanned aerial vehicles (UAVs) allow a 3D model to be made using directly the information from their GNSS (Global Navigation Satellite System) receiver. This spends time both on terrain and in processing. Bearing this fact in mind a method for building a photogrammetric model of an area photographed with an UAV is presented in the paper.*

***Keywords**: UAV, stereo pairs, tie points, photogrammetric model.*

Introduction

Today three-dimensional (3D) models find applications in many different fields – gaming, film making, archelogy, geodesy [1], [7], [8]. Especially in geodesy it is crutial the model to be georeferenced, i.e. orientated in a global geodetic system like WGS84. Usually ground control points (GCPs) are used for this purpose, but this means more time spend on terrain and carrying more instruments with oneself. To avoid this inconvenience 3D models can be made directly in the coordinate system (CS) of the unanned aerial vehichle's (UAV) GNSS (Global Navigation Satellite System) receiver. Bearing this fact in mind a method for building a photogrammetric model of an area photographed with an UAV is described below.

Method of semi-dependent models

Applying the methodology described in [3] to the series of stereo pair images during a single UAV flight allows a free photogrammetric model of the entire captured terrain to be obtained, using only tie points. This fact will be explained using the so-called method of *semi-dependent models* – fig. 1.

More specifically, let P_{i-1}, P_i, P_{i+1} be the $i-1st$, ith, and $i+1st$ pictures taken consecutively by the UAV camera while flying over some terrain (object). Then, after applying the methodology from [3] to the stereo pair P_{i-1}, P_i, using the linear-angular coordinate system (CS) will result in a photogrammetric model in which the axes of the CS $S_i x_i' y_i' z_i'$ of the photo P_i are parallel to the axes of CS $S_{i-1} x_{i-1}' y_{i-1}' z_{i-1}'$ in the photo P_{i-1}. Therefore, the stereo image pair P_{i-1}, P_i in fig. 1 fully corresponds to the stereo pair of photos P_1, P_2 in fig. 4 from [3]. Moreover, considering Step 5, the transformed image coordinates of an arbitrary point m_{ik} from the picture P_i are:

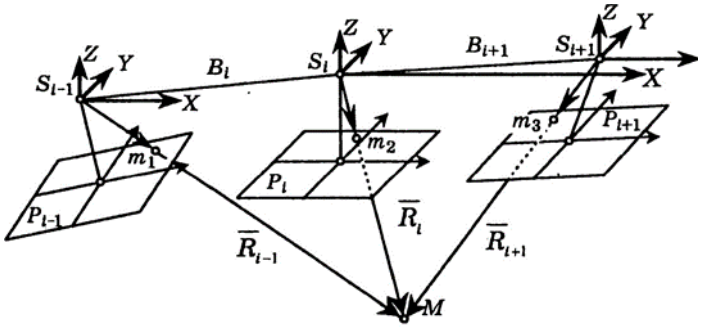


Figure 1: Two consecutive stereo pairs,
formed by three consecutive pictures

$$\begin{matrix} x'_{m_{ik}} \\ y'_{m_{ik}} \\ z'_{m_{ik}} \end{matrix} = T''_{i-1} \begin{matrix} x_{m_{ik}} \\ y_{m_{ik}} \\ -f \end{matrix}, \; T''_{i-1} = \begin{matrix} a''_{1,i-1} & a''_{2,i-1} & a''_{3,i-1} \\ b''_{1,i-1} & b''_{2,i-1} & b''_{3,i-1} \\ c''_{1,i-1} & c''_{2,i-1} & c''_{3,i-1} \end{matrix}. \quad (1)$$

In (1) $x_{m_{ik}}, y_{m_{ik}}, -f$ are the "initial" image coordinates of an arbitrary point m_{ik} from the picture P_i, $x'_{m_{ik}}, y'_{m_{ik}}, z'_{m_{ik}}$ are its coordinates transformed into the CS $S_i x_i' y_i' z_i'$ whose axes are parallel to the axes of the CS $S_{i-1} x_{i-1}' y_{i-1}' z_{i-1}'$ in the photo P_{i-1}. In addition, the guiding cosines (the elements of the transformation matrix T''_{i-1}) are calculated using the already determined angular elements of mutual orientation $\tau'_{i-1}, \nu'_{i-1}, \Delta\alpha_{i-1}, \Delta\omega_{i-1}, \Delta\chi_{i-1}$ of the stereo image pair P_{i-1}, P_i.

Therefore, given (5) and (6) from [3] the coordinates $X_{M_{i-1k}}, Y_{M_{i-1k}}, Z_{M_{i-1k}}$ of an arbitrary point M_{i-1k} from the set of characteristic points (CPs) of the stereo pair of pictures P_i, P_{i+1} in the linear-angular CS of the picture P_{i-1} are determined by the ratios:

$$\begin{aligned} X_{M_{i-1k}} &= x'_{S_{i-1}} + k_{m_{i-1k}} x'_{m_{i-1k}} = \frac{B_{Xi-1} Z'_{m_{ik}} - B_{Zi-1} X'_{m_{ik}}}{X'_{m_{i-1k}} Z'_{m_{ik}} - Z'_{m_{i-1k}} X'_{m_{ik}}} x'_{m_{i-1k}} \\ Y_{M_{i-1k}} &= y'_{S_{i-1}} + k_{m_{i-1k}} y'_{m_{i-1k}} = \frac{B_{Xi-1} Z'_{m_{ik}} - B_{Zi-1} X'_{m_{ik}}}{X'_{m_{i-1k}} Z'_{m_{ik}} - Z'_{m_{i-1k}} X'_{m_{ik}}} y'_{m_{i-1k}} \\ Z_{M_{i-1k}} &= z'_{S_{i-1}} + k_{m_{i-1l}} z'_{m_{i-1k}} = \frac{B_{Xi-1} Z'_{m_{ik}} - B_{Zi-1} X'_{m_{ik}}}{X'_{m_{i-1k}} Z'_{m_{ik}} - Z'_{m_{i-1k}} X'_{m_{ik}}} z'_{m_{i-1k}} \end{aligned} \quad (2)$$

The following equalities are also used in (2):

$$\begin{gathered} B_{i-1} = \sqrt{X_{S_i} - X_{S_{i-1}}{}^2 + Y_{S_i} - Y_{S_{i-1}}{}^2 + Z_{S_i} - Z_{S_{i-1}}{}^2}, \\ B_{Xi-1} = B_{i-1} cos\tau'_{i-1} cos\nu'_{i-1}, \quad B_{Y_{i-1}} = B_{i-1} sin\tau'_{i-1} cos\nu'_{i-1}, \\ B_{Z_{i-1}} = B_{i-1} sin\nu'_{i-1}, \quad x'_{S_{i-1}} = y'_{S_{i-1}} = z'_{S_{i-1}} = 0. \end{gathered} \quad (3)$$

The calculation of the photographing base B_{i-1} is possible because the coordinates of the projection centers S_{i-1}, S_i were measured by the GNSS (Global Navigation Satellite System) receiver of the UAV, and the angles τ'_{i-1}, ν'_{i-1} are determined at Step 4 of the methodology for building a single photogrammetric model based on the stereo pair of photos P_{i-1}, P_i.

Now it should be noted that the stereo pair of photos P_i, P_{i+1} in fig. 1 also fully corresponds to the stereo pair of photos P_1, P_2 in fig. 4 [3]. Therefore, applying the methodology for building a single photogrammetric model to the stereo pair of photos P_i, P_{i+1} the angular elements of mutual orientation $\tau'_i, \nu'_i, \Delta\alpha_i, \Delta\omega_i, \Delta\chi_i$ of the stereo pair can be calculated in CS $S_i x_i' y_i' z_i'$ whose axes are parallel to the

axes of CS $S_{i-1}x_{i-1}'y_{i-1}'z_{i-1}'$ in the photo P_{i-1}. More specifically, the image coordinates of the points of the photo P_{i+1} are transformed analogously to (1):

$$\begin{matrix} x'_{m_{i+1k}} \\ y'_{m_{i+1k}} \\ z'_{m_{i+1k}} \end{matrix} = T_i'' \begin{matrix} x_{m_{i+1k}} \\ y_{m_{i+1k}} \\ -f \end{matrix}, \; T_i'' = \begin{matrix} a''_{1,i} & a''_{2,i} & a''_{3,i} \\ b''_{1.i} & b''_{2,i} & b''_{3,i} \\ c''_{1,i} & c''_{2,i} & c''_{3,i} \end{matrix}. \tag{4}$$

In (4) $x_{m_{i+1k}}, y_{m_{i+1k}}, -f$ are the "initial" coordinates of an arbitrary point m_{i+1k} from the photo P_{i+1}, and $x'_{m_{i+1k}}, y'_{m_{i+1k}}, z'_{m_{i+1k}}$ are its coordinates transformed by the matrix T_i''. In this case, the elements of the matrix T_i'' are calculated by using the already defined angular elements of mutual orientation $\tau_i', \nu_i', \Delta\alpha_i, \Delta\omega_i, \Delta\chi_i$ of the stereo pair of photos P_i, P_{i+1} in CS $S_i x_i' \, y_i' z_i'$.

As a result of the listed operations, a second single photogrammetric model is obtained, whose CS is CS $S_{i-1}x_{i-1}'y_{i-1}'z_{i-1}'$ of the photo P_{i-1}. Therefore, given (5) and (6) from [3] the coordinates $X_{M_{ik}}, Y_{M_{ik}}, Z_{M_{ik}}$ of an arbitrary point M_{ik} from the set of CPs of the stereo pair of photos P_i, P_{i+1} in linear-angular CS of the picture P_{i-1} are determined by the ratios:

$$\begin{aligned} X_{M_{ik}} &= x'_{S_i} + k_{m_{ik}} x'_{m_{ik}} = B_{Xi-1} + \frac{B_{Xi}Z'_{m_{i+1k}} - B_{Zi}X'_{m_{i+1k}}}{X'_{m_{ik}}Z'_{m_{i+1k}} - Z'_{m_{ik}}X'_{m_{i+1k}}} x'_{m_{ik}} \\ Y_{M_{ik}} &= y'_{S_i} + k_{m_{ik}} y'_{m_{ik}} = B_{Yi-1} + \frac{B_{Xi}Z'_{m_{i+1k}} - B_{Zi}X'_{m_{i+1k}}}{X'_{m_{ik}}Z'_{m_{i+1k}} - Z'_{m_{ik}}X'_{m_{i+1k}}} y'_{m_{ik}} \\ Z_{M_{ik}} &= z'_{S_i} + k_{m_{ik}} z'_{m_{ik}} = B_{Zi-1} + \frac{B_{Xi}Z'_{m_{i+1k}} - B_{Zi}X'_{m_{i+1k}}}{X'_{m_{ik}}Z'_{m_{i+1k}} - Z'_{m_{ik}}X'_{m_{i+1k}}} z'_{m_{ik}} \end{aligned} \tag{5}$$

The following equalities are also used in (5):

$$\begin{gathered} B_i = \sqrt{\left(X_{S_{i+1}} - X_{S_i}\right)^2 + \left(Y_{S_{i+1}} - Y_{S_i}\right)^2 + \left(Z_{S_{i+1}} - Z_{S_i}\right)^2}, \\ B_{Xi} = B_i cos\tau_i' cos\nu_i', \quad B_{Y_i} = B_i sin\tau_i' cos\nu_i', \\ B_{Z_i} = B_i sin\nu_i', \quad X'_{S_i} = B_{Xi-1}, \quad y'_{S_i} = B_{Yi-1}, \quad z'_{S_i} = B_{Zi-1}. \end{gathered} \tag{6}$$

As above, the calculation of the photographing base B_i is possible because the coordinates of the projection centers S_i, S_{i+1} are measured by the GNSS receiver of the UAV, and the angles τ_i', ν_i' are determined at Step 4 of the methodology for building a single photogrammetric model based on the stereo pair of photos P_i, P_{i+1}.

Obviously, the application of the described method to the consecutive stereo pairs of photos P_1, P_2; P_2, P_3; P_3, P_4, etc. allows to obtain a unified photogrammetric model whose CS is CS $S_1x_1y_1z_1$ of the photo P_1.

Here it should be noted that in many modern software products, bundle adjustment (BA) is applied simultaneously to whole groups of consecutive pictures. This approach can be explained with fig. 2, where point M is a tie point for both the stereo pair of photos P_{i-1}, P_i and the stereo pair of photos P_i, P_{i+1}. Therefore, the projection beam lengths S_iM calculated for each of the single photogrammetric models based on the stereo image pairs P_{i-1}, P_i and P_i, P_{i+1} respectively must match. This fact allows the construction of more complex systems of normal equations, in the solution of which BA is achieved simultaneously for a whole group of consecutive photos.

Here it should be specially noted that the equipment of modern UAVs allows the CS of the photogrammetric model of the photographed terrain to be the geodetic CS $O_\Gamma X_\Gamma Y_\Gamma Z_\Gamma$. Indeed, let the correlator of the photogrammetric image processing program has detected six or more TPs ($N_{tp} \geq 6$) on an arbitrary stereo pair of images P_{i-1}, P_i. Then the mutual orientation of the photos P_{i-1}, P_i can be done directly in the CS used by the GNSS receiver of the UAV. Indeed, let point M_k be the kth TP, $1 \leq k \leq N_{tp}$, and point m_{i-1k} and point m_{ik} be its images on the photos P_{i-1}, P_i respectively (fig. 2).

In this situation in the CS of the GNSS receiver of the UAV, the fact that the vectors R_{0i-1}, R_{i-1}, R_i are collinear is expressed by the zero determinant [5, 6]:

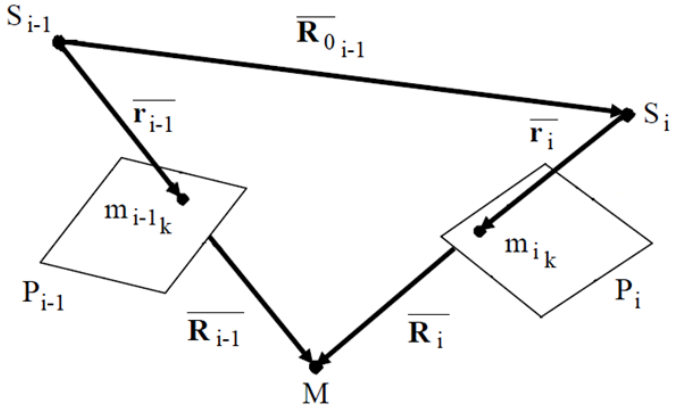


Figure 2: Tie point (M_k) on the imaged earth surface and its images (m_{i-1k}, m_{ik}) on the pictures from the stereo pair P_{i-1}, P_i

$$\begin{vmatrix} B_{X_{i-1}} & B_{Y_{i-1}} & B_{Z_{i-1}} \\ x'_{m_{i-1k}} & y'_{m_{i-1k}} & z'_{m_{i-1k}} \\ x'_{m_{ik}} & y'_{m_{ik}} & z'_{m_{ik}} \end{vmatrix} = B_{X_{i-1}}\ y'_{m_{i-1k}} z'_{m_{ik}} - y'_{m_{ik}} z'_{m_{i-1k}}\ - \\ -B_{Y_{i-1}}\ x'_{m_{i-1k}} z'_{m_{ik}} - x'_{m_{ik}} z'_{m_{i-1k}}\ + B_{Z_{i-1}}\ x'_{m_{i-1k}} y'_{m_{ik}} - x'_{m_{ik}} y'_{m_{i-1k}}\ = 0. \tag{7}$$

In (7) in view of [2], [4], [5], [6] the following relations are valid:

$$x'_{m_{i-1k}} = a'_1 x_{m_{i-1k}} + a'_2 y_{m_{i-1k}} - a'_3 f,$$
$$y'_{m_{i-1k}} = b'_1 x_{m_{i-1k}} + b'_2 y_{m_{i-1k}} - b'_3 f,\ \ z'_{m_{i-1k}} = c'_1 x_{m_{i-1k}} + c'_2 y_{m_{i-1k}} - c'_3 f, \tag{8}$$

$$x'_{m_{ik}} = a''_1 x_{m_{ik}} + a''_2 y_{m_{ik}} - a''_3 f,$$
$$y'_{m_{ik}} = b''_1 x_{m_{ik}} + b''_2 y_{m_{ik}} - b''_3 f,\ \ z'_{m_{ik}} = c''_1 x_{m_{ik}} + c''_2 y_{m_{ik}} - c''_3 f. \tag{9}$$

In (8), (9) $x_{m_{i-1k}}, y_{m_{i-1k}}, -f$ and $x_{m_ik}, y_{m_{ik}}, -f$ are the coordinates of point m_{i-1k} and point m_{ik} in the intermediate CS $S_i x_{i-1} y_{i-1} z_{i-1}$, $S_i x_i y_i z_i$ of the photos P_{i-1}, P_i respectively. Furthermore,

$$a'_1 = cos\alpha'_{i-1} cos\chi'_{i-1} - sin\alpha'_{i-1} sin\omega'_{i-1} sin\chi'_{i-1},$$
$$a''_1 = cos\alpha'_i cos\chi'_i - sin\alpha'_i sin\omega'_i sin\chi'_i,$$
$$a'_2 = -cos\alpha'_{i-1} sin\chi'_{i-1} - sin\alpha'_{i-1} sin\omega'_{i-1} cos\chi'_{i-1},$$
$$a''_2 = -cos\alpha'_i sin\chi'_i - sin\alpha'_i sin\omega'_i cos\chi'_i,$$
$$a'_3 = -sin\alpha'_{i-1} cos\omega'_{i-1}, a''_3 = -sin\alpha'_i cos\omega'_i,$$
$$b'_1 = cos\omega'_{i-1} sin\chi'_{i-1}, b''_1 = cos\omega'_i sin\chi'_i,$$
$$b'_2 = cos\omega'_{i-1} cos\chi'_{i-1}, b''_2 = cos\omega'_i cos\chi'_i, \tag{10}$$
$$b'_3 = -sin\omega'_{i-1}, b''_3 = -sin\omega'_i,$$
$$c'_1 = sin\alpha'_{i-1} cos\chi'_{i-1} + cos\alpha'_{i-1} sin\omega'_{i-1} sin\chi'_{i-1},$$
$$c''_1 = sn\alpha'_i cos\chi'_i + cos\alpha'_i sin\omega'_i sin\chi'_i,$$
$$c'_2 = -sin\alpha'_{i-1} sin\chi'_{i-1} + cos\alpha'_1 sin\omega'_{i-1} cos\chi'_{i-1},$$
$$c''_2 = -sin\alpha'_i sin\chi'_i + cos\alpha'_i sin\omega'_i cos\chi'_i,$$
$$c'_3 = cos\alpha'_{i-1} cos\omega'_{i-1}, c''_3 = cos\alpha'_i cos\omega'_i,$$

are the guiding cosines, which are functions of the angular elements of orientation $\alpha'_{i-1}, \omega'_{i-1}, \chi'_{i-1}$, $\alpha'_i, \omega'_i, \chi'_i$ of the intermediate CS $S_i x_{i-1} y_{i-1} z_{i-1}$, $S_i x_i y_i z_i$ of the photos P_{i-1}, P_i relative to the CS of the GNSS receiver of the UAV [5], [6].

Also, in (7) the coordinates of the photographing base are determined as follows

$$B_{X_{i-1}} = X_{S_i} - X_{S_{i-1}}, \quad B_{Y_{i-1}} = Y_{S_i} - Y_{S_{i-1}}, \quad B_{Z_{i-1}} = Z_{S_i} - Z_{S_{i-1}}, \tag{11}$$

based on the coordinates $X_{S_{i-1}}, Y_{S_{i-1}}, Z_{S_{i-1}}$, $X_{S_i}, Y_{S_i}, Z_{S_i}$ of the projection centers S_{i-1}, S_i registered by the GNSS receiver of the UAV.

Condition (7) is easily reduced to linear form if all angles $\alpha'_{i-1}, \alpha'_i, \omega'_{i-1}, \omega'_i, \chi'_{i-1}, \chi'_i$ in absolute value are smaller than 3°. In such situation it is fulfilled:

$$sin\varepsilon = \frac{\varepsilon}{1!} - \frac{\varepsilon^3}{3!} + \frac{\varepsilon^5}{5!} - \frac{\varepsilon^7}{7!} + \cdots \approx \varepsilon, \quad cos\varepsilon = 1 - \frac{\varepsilon^2}{1!} + \frac{\varepsilon^4}{4!} - \frac{\varepsilon^6}{6!} + \cdots \approx 1, \tag{12}$$

where ε, $\varepsilon \leq 3°$ can be any of the small angles $\alpha'_{i-1}, \alpha'_i, \omega'_{i-1}, \omega'_i, \chi'_{i-1}, \chi'_i$.

After taking into account (12) in (10) the result is

$$\begin{gathered} a'_1 \approx 1, \quad a''_1 \approx 1, \\ a'_2 \approx -\chi'_{i-1}, \quad a''_2 \approx -\chi'_i, \\ a'_3 \approx -\alpha'_{i-1}, \quad a''_3 \approx -\alpha'_i, \\ b'_1 \approx \chi'_{i-1}, \quad b''_1 \approx \chi'_i, \\ b'_2 \approx 1, \quad b''_2 \approx 1, \\ b'_3 \approx -\omega'_{i-1}, \quad b''_3 \approx -\omega'_i, \\ c'_1 \approx \alpha'_{i-1}, \quad c''_1 \approx \alpha'_i, \\ c'_2 \approx \omega'_{i-1}, \quad c''_2 \approx \omega'_i, \\ c'_3 \approx 1, \quad c''_3 \approx 1. \end{gathered} \tag{13}$$

Putting the approximations (13) into (8) and (9) allows $x'_{m_{i-1k}}, y'_{m_{i-1k}}, z'_{m_{i-1k}}, x'_{m_{ik}}, y'_{m_{ik}}, z'_{m_{ik}}$ be represented as linear functions of the mutual orientation elements $\alpha'_{i-1}, \alpha'_i, \omega'_{i-1}, \omega'_i, \chi'_{i-1}, \chi'_i$:

$$\begin{gathered} x'_{m_{i-1k}} = x_{m_{i-1k}} - y_{m_{i-1k}}\chi'_{i-1} + f\alpha'_{i-1}, \\ y'_{m_{i-1k}} = x_{m_{i-1k}}\chi'_{i-1} + y_{m_{i-1k}} + f\omega'_{i-1}, \\ z'_{m_{i-1k}} = x_{m_{i-1k}}\alpha'_{i-1} + y_{m_{i-1k}}\omega'_{i-1} - f, \end{gathered} \tag{14}$$

$$\begin{gathered} x'_{m_{ik}} = x_{m_{ik}} - y_{m_{ik}}\chi'_i + f\alpha'_i, \\ y'_{m_{ik}} = x_{m_{ik}}\chi'_i + y_{m_{ik}} + f\omega'_i, \\ z'_{m_{ik}} = x_{m_{ik}}\alpha'_i + y_{m_{ik}}\omega'_i - f. \end{gathered} \tag{15}$$

From (14) and (15), and after keeping only the terms with first-order significance (i.e. assuming that $\alpha'_i\chi'_{i-1} \approx 0, \omega'_i\chi'_{i-1} \approx 0, \alpha'_{i-1}\chi'_i \approx 0, \alpha'_{i-1}\omega'_i \approx 0$) it is established that:

$$\begin{gathered} B_{X_{i-1}}\ y'_{m_{i-1k}}z'_{m_{ik}} - y'_{m_{ik}}z'_{m_{i-1k}} = B_{X_{i-1}}\ -x_{m_{i-1k}}f\chi'_{i-1} + \\ +x_{m_{ik}}y_{m_{i-1k}}\alpha'_i + y_{m_{i-1k}}y_{m_{ik}}\omega'_i - y_{m_{i-1k}}f - f^2\omega'_{i-1} + \\ +x_{m_{ik}}f\chi'_i - x_{m_{i-1k}}y_{m_{ik}}\alpha'_{i-1} - y_{m_{i-1k}}y_{m_{ik}}\omega'_{i-1} + y_{m_{ik}}f + f^2\omega'_i\ , \end{gathered} \tag{16}$$

$$\begin{gathered} -B_{Y_{i-1}}\ x'_{m_{i-1k}}z'_{m_{ik}} - x'_{m_{ik}}z'_{m_{i-1k}} = -B_{Y_{i-1}}\ x_{m_{i-1k}}x_{m_{ik}}\alpha'_i + \\ +x_{m_{i-1k}}y_{m_{ik}}\omega'_i - x_{m_{i-1k}}f + y_{m_{i-1k}}f\chi'_{i-1} - f^2\alpha'_{i-1} - \\ -x_{m_{i-1k}}x_{m_{ik}}\alpha'_{i-1} - x_{m_{ik}}y_{m_{i-1k}}\omega'_{i-1} + x_{m_{ik}}f - y_{m_{ik}}f\chi'_i + f^2\alpha'_i\ , \end{gathered} \tag{17}$$

$$\begin{aligned} B_{Z_{i-1}}\ x'_{m_{i-1k}}y'_{m_{ik}} - x'_{m_{ik}}y'_{m_{i-1k}}\ &= B_{Z_{i-1}}\ x_{m_{i-1k}}x_{m_{ik}}\chi'_i + \\ +x_{m_{i-1k}}y_{m_{ik}} + x_{m_{i-1k}}f\omega'_i - y_{m_{i-1k}}y_{m_{ik}}\chi'_{i-1} + y_{m_{ik}}f\alpha'_{i-1} - \\ -x_{m_{i-1k}}x_{m_{ik}}\chi'_{i-1} - x_{m_{ik}}y_{m_{i-1k}} - x_{m_{ik}}f\omega'_{i-1} + y_{m_{i-1k}}y_{m_{ik}}\chi'_i - y_{m_{i-1k}}f\alpha'_i\ . \end{aligned} \tag{18}$$

Now, after substituting (16), (17) and (18) into (7) and removing the parentheses, the following linear equation with 6 unknowns is obtained:

$$a_k\alpha'_{i-1} + b_k\alpha'_i + c_k\omega'_{i-1} + d_k\omega'_i + e_k\chi'_{i-1} + f_k\chi'_i + q_k = 0. \tag{19}$$

In (19) the following notations are used:

$$\begin{aligned} d_{1k} &= -B_{X_{i-1}}x_{m_{i-1k}}y_{m_{ik}} + B_{Y_{i-1}}f^2 + B_{Y_{i-1}}x_{m_{i-1k}}x_{m_{ik}} + B_{Z_{i-1}}y_{m_{ik}}f, \\ d_{2k} &= B_{X_{i-1}}x_{m_{ik}}y_{m_{i-1k}} - B_{Y_{i-1}}f^2 - B_{Y_{i-1}}x_{m_{i-1k}}x_{m_{ik}} - B_{Z_{i-1}}y_{m_{i-1k}}f, \\ d_{3k} &= -B_{X_{i-1}}y_{m_{i-1k}}y_{m_{ik}} - B_{X_{i-1}}f^2 + B_{Y_{i-1}}x_{m_{ik}}y_{m_{i-1k}} - B_{Z_{i-1}}z_{m_{ik}}f, \\ d_{4k} &= B_{X_{i-1}}y_{m_{i-1k}}y_{m_{ik}} + B_{X_{i-1}}f^2 - B_{Y_{i-1}}x_{m_{i-1k}}y_{m_{ik}} + B_{Z_{i-1}}z_{m_{i-1k}}f, \\ d_{5k} &= -B_{X_{i-1}}x_{m_{i-1k}}f - B_{Y_{i-1}}y_{m_{i-1k}}f - B_{Z_{i-1}}x_{m_{i-1k}}x_{m_{ik}} - B_{Z_{i-1}}y_{m_{i-1k}}y_{m_{ik}}, \\ d_{6k} &= B_{X_{i-1}}x_{m_{ik}}f + B_{Y_{i-1}}y_{m_{ik}}f + B_{Z_{i-1}}x_{m_{i-1k}}x_{m_{ik}} + B_{Z_{i-1}}y_{m_{i-1k}}y_{m_{ik}}, \\ q_k &= B_{X_{i-1}}\ -y_{m_{i-1k}} + y_{m_{ik}}\ f + B_{Y_{i-1}}\ x_{m_{i-1k}} - x_{m_{ik}}\ f + \\ &\quad +B_{Z_{i-1}}\ x_{m_{i-1k}}y_{m_{ik}} - x_{m_{ik}}y_{m_{i-1k}}\ . \end{aligned} \tag{20}$$

Here it should be recalled the assumption made above that the correlator of the program for photogrammetric processing of the photos has detected at least six TPs ($N_{tp} \geq 6$). Let their coordinates in the intermediate CS $S_{i-1}x_{i-1}y_{i-1}z_{i-1}, S_ix_iy_iz_i$ of the two photos P_{i-1}, P_i be

$$x_{m_{i-1k}}, y_{m_{i-1k}}\ ,\quad x_{m_{ik}}, y_{m_{ik}}\ ,\quad k = 1,2,3,4,5,6 \tag{21}$$

respectively. Therefore, when the index k passes through all possible values $k = 1, 2, \dots, N_{tp}, N_{tp} \geq 6$, from (19), (20) and (21) the following system of 6 linear equations with 6 unknowns is obtained:

$$\begin{matrix} d_{11} & d_{12} & d_{13} & d_{14} & d_{15} & d_{16} \\ d_{21} & d_{22} & d_{23} & d_{24} & d_{25} & d_{26} \\ d_{31} & d_{32} & d_{33} & d_{34} & d_{35} & d_{36} \\ d_{41} & d_{42} & d_{43} & d_{44} & d_{45} & d_{46} \\ d_{51} & d_{52} & d_{53} & d_{54} & d_{55} & d_{56} \\ d_{61} & d_{62} & d_{63} & d_{64} & d_{65} & d_{66} \end{matrix} \begin{matrix} \alpha'_{i-1} \\ \alpha'_i \\ \omega'_{i-1} \\ \omega'_i \\ \chi'_{i-1} \\ \chi'_i \end{matrix} = \begin{matrix} q_1 \\ q_2 \\ q_3 \\ q_4 \\ q_5 \\ q_6 \end{matrix}\ . \tag{22}$$

The system of linear equations (22) can easily be solved by the method of Gauss or by the method of determinants (Cramer's method). Its solution

$$\alpha'_{i-1} = \alpha'_{i-10},\quad \alpha'_i = \alpha'_{i0},\quad \omega'_{i-1} = \omega'_{i-10},\quad \omega'_i = \omega'_{i0},\quad \chi'_{i-1} = \chi'_{i-10},\quad \chi'_i = \chi'_{i0} \tag{23}$$

allows to mutually orient the two pictures P_{i-1}, P_i and create a single photogrammetric model based on this stereo pair, whose CS coincides with the geodetic CS $O_\Gamma X_\Gamma Y_\Gamma Z_\Gamma$.

If any of the angles $\alpha'_{i-1}, \alpha'_i, \omega'_{i-1}, \omega'_i, \chi'_{i-1}, \chi'_i$ in absolute value is greater than 3°, then the condition (7) is reduced to a linear form by expanding in Taylor series and considering only the elements of the first order of significance:

$$\begin{gathered} B_{X_{i-1}}\ y'_{m_{i-1k}}z'_{m_{ik}} - y'_{m_{ik}}z'_{m_{i-1k}}\ - B_{Y_{i-1}}\ x'_{m_{i-1k}}z'_{m_{ik}} - x'_{m_{ik}}z'_{m_{i-1k}}\ + \\ +B_{Z_{i-1}}\ x'_{m_{i-1k}}y'_{m_{ik}} - x'_{m_{ik}}y'_{m_{i-1k}}\ = \\ = \psi_k\ \alpha'_{i-1}, \alpha'_i, \omega'_{i-1}, \omega'_i, \chi'_{i-1}, \chi'_i, x_{m_{i-1k}}, y_{m_{i-1k}}, x_{m_{ik}}, y_{m_{ik}}\ = \\ = a_k\delta\alpha'_{i-1} + b_k\delta\alpha'_i + c_k\delta\omega'_{i-1} + d_k\delta\omega'_i + e_k\delta\chi'_{i-1} + f_k\delta\chi'_i + l_k - v_k = 0. \end{gathered} \tag{24}$$

In (24) the following notations are used:

$$\begin{gathered} a_k = \frac{\partial\psi_k}{\partial\alpha'_{i-1}}\ U_{0k}, \quad b_k = \frac{\partial\psi_k}{\partial\alpha'_i}\ U_{0k}, \quad c_k = \frac{\partial\psi_k}{\partial\omega'_{i-1}}\ U_{0k}, \\ d_k = \frac{\partial\psi_k}{\partial\omega'_i}\ U_{0k}, \quad e_k = \frac{\partial\psi_k}{\partial\chi'_{i-1}}\ U_{0k}, \quad f_k = \frac{\partial\psi_k}{\partial\chi'_i}\ U_{0k}, \quad l_k = \psi_k\ U_{0k}. \end{gathered} \tag{25}$$

In (25), the symbol U_{0k} means that the first partial derivatives of the function (24) with respect to the (unknown) arguments $\alpha'_{i-1}, \alpha'_i, \omega'_{i-1}, \omega'_i, \chi'_{i-1}, \chi'_i$ and the free term l_k are "valued", putting in them the approximate values of the arguments (the unknowns) (23), as well as the image coordinates $x_{m_{i-1k}}, y_{m_{i-1k}}$, $x_{m_{ik}}, y_{m_{ik}}$ of the kth TP, $k = 1, 2, \dots, N_{tp}, N_{tp} \geq 6$. Put another way, in each of the first partial derivatives $\frac{\partial\psi_k}{\partial\alpha'_{i-1}}, \frac{\partial\psi_k}{\partial\alpha'_i}, \frac{\partial\psi_k}{\partial\omega'_{i-1}}, \frac{\partial\psi_k}{\partial\omega'_i}, \frac{\partial\psi_k}{\partial\chi'_{i-1}}, \frac{\partial\psi_k}{\partial\chi'_i}$ and in the free member l_k, the known approximate values of the angular elements of mutual orientation in the CS of the GNSS receiver of the UAV and the image coordinates of the point m_{i-1k} and point m_{ik} are applied, i.e. $U_{0k} = \ \alpha'_{i-1} = \alpha'_{i-10}, \alpha'_i = \alpha'_{i0}, \omega'_{i-1} = \omega'_{i-10}, \omega'_i = \omega'_{i0}, \chi'_{i-1} = \chi'_{i-10}, \chi'_i = \chi'_{i0}, x_{m_{i-1k}}, y_{m_{i-1k}}, x_{m_{ik}}, y_{m_{ik}}$.

Moreover, in (24) $\delta\alpha'_{i-1}, \delta\alpha'_i, \delta\omega'_{i-1}, \delta\omega'_i, \delta\chi'_{i-1}, \delta\chi'_i$ are the corrections to the approximate values of the arguments (the unknowns), and v_k is the correction to the result of the kth measurement. Here it should be noted that v_k is the correction to the transverse parallax $q_k = y_{m_{i-1k}} - y_{m_{ik}}$ of the image coordinates of the kth TP.

When in (24) the index k passes through all possible values $k = 1, 2, \dots, N_{tp}, N_{tp} \geq 6$, a system of N_{tp} equations, 6 unknowns and N_{tp} parameters is obtained, which is solved by *least squares method*. The thus determined angular orientation elements $\alpha'_{i-1}, \omega'_{i-1}, \chi'_{i-1}$, $\alpha'_i, \omega'_i, \chi'_i$ allow to transform the coordinates of all CPs of the stereo pair P_{i-1}, P_i from CS $S_{i-1}x_{i-1}y_{i-1}z_{i-1}$ and $S_ix_iy_iz_i$ to the CS of the GNSS receiver of the UAV. Then, using the photo P_{i-1} as the initial photo for the stereo pairs $P_{i-1}, P_{i-2};\ P_{i-2}, P_{i-3}; \dots;\ P_2, P_1,$ and P_i as the initial photo for the stereo pairs $P_i, P_{i+1};\ P_{i+1}, P_{i+2};\ P_{i+2}, P_{i+3}$; ... by the method of semi-dependent models it is possible to create a unified photogrammetric model whose CS is the CS of the UAV's GNSS receiver. However, the position of this CS relative to the geodesic CS $O_\Gamma X_\Gamma Y_\Gamma Z_\Gamma$ s precisely known.

Conclusion

In this paper a method for building a photogrammetric model of an area in the CS of the UAV GNSS receiver is discussed and analized. Such model can be obtained using only tie points and without using ground control points. This fact is very important, because it saves a lot of time on terrain and reduces the time for photogrammetric processing.

Acknowledgments

This paper is written thanks to project BG05M2OP001-2.016-0003 "Modernization of Vasil Levski National Military University – Veliko Tarnovo and Sofia University "St. Kliment Ohridski" – Sofia in professional direction 5.3 Computer and communication technology", financed by the operational program "Science and education for intelligent growth".

References

1. Andreev A., Andreeva P. (2009) Creating a digital terrain model of the database for subsequent topographic maps in GIS environment. *Artillery review magazine, book 3*, pp. 17- 31, ISBN 1314-0388.
2. Bedzheva, M. (2022) *Relationship between image coordinates of characteristic points of a stereo pair of photographs*, Proceedings of International Scientific Conference "Defense Technologies" DefTech 2022, Faculty of Artillery, Air Defense and Communication and Information Systems (in print)
3. Bedzheva, M. (2022) *Methodology for building a single photogrammetric model*, Proceedings of International Scientific Conference "Defense Technologies" DefTech 2022, Faculty of Artillery, Air Defense and Communication and Information Systems (in print)
4. Krasnopevtsev, B. (2008). *Photogrammetry.* Moscow: Moscow National University of Geodesy and Cartography
5. Lobanov, A. (1984). *Photogrammetry.* Moscow: Nedra
6. Nazarov, A. (2006). *Photogrammetry.* Moscow: Tetra Systems
7. Niyazi-Yusuf, M. (2021) Assessment of the actuality of the content and accuracy of the current cadastral plans, *Annual of FTS*, Vol. XI E, Shumen, Bishop Konstantin Preslavsky University press, pp. 59-62, ISSN: 1311-834X
8. Prokopov, Y., (2021). Capabilities of terrestrial laser scanning – a basis for geodetic modeling, *International Scientific Conference -Defense Technologies, DefTech*, 06-08.10.2021, Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, pp. 467-473, ISSN 2367-7902.

CREATING AN ORTHOPHOTO MAP AND ELEVATION MODEL OF AN URBANIZED AREA WITH A UAV

Nikolay H. Kopanov, Ivan Y. Radev

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

***Abstract**: In recent years, unmanned aerial vehicles have demonstrated significant capabilities with the potential for applications in many fields. One of their recent applications is in the field of photogrammetry such as aerial orthophoto-surveying and map and elevation model creation. This material aims to show the application of UAVs in the performance of various tasks.*

***Keywords**: Photogrammetry; Map; Geographic data; UAV; GNSS.*

СЪЗДАВАНЕ НА ОРТОФОТО КАРТА И ВИСОЧИНЕН МОДЕЛ НА УРБАНИЗИРАН РАЙОН С БЛА

Николай Х. Копанов, Иван Й. Радев

1. Въведение

В геодезическата практика през последните години масово навлизат съвременни методи базирани на използването на професионални БЛА. Тези летателни системи притежават сензорите за заснемане и разнообразни решения за поддържане на полета както „фиксирано", така и с „ротиращо" крило. БЛА са способни да изпълняват функции по придобиване на фотограметрични данни чрез монтираните на тях компактни високоточни цифрови фотоапарати със сменяема оптика или огледални-рефлексни цифрови фотоапарати в напълно автоматичен режим на полет. [4]

Една от основните разлики между дистанционно управляемите летателни апарати и безпилотните летателни системи е наличието на навигационна апаратура, позволяваща следването на определен летателен курс и оценка на позицията на летателния апарат в момента на включване на камерата. Така практически може да позволи директно георефериране на заснетите от борда на летателния апарат изображения. За по-голяма прецизност се прилага корекционен пакет, включващ параметрите на ориентация, записани от интегрираните на борда GPS/INS сензори. За някои приложения, където не се изисква висока точност на позициониране, например за приложения, свързани с бързото картографиране, точността на позициониране получено от GPS/INS сензорите, може да бъде достатъчна. В останалите случаи пространственото ориентиране на ортофото мозайките, генерирани от заснетите изображения, се реализира чрез предварително изграждане на мрежа от достатъчен брой наземни контролни точки. [5]

Използването на БЛА като инструмент за генериране на прецизен модел на повърхността се базира на алгоритъм и включва фотограметричен процес, който може да бъде разделен на няколко стъпки. Заснемат сеа частично припокриващи се изображения под формата на надлъжно и напречно застъпване (до 80%). Придобиването на изображения се извършва от БЛА в автоматичен режим на полет. За заснемане на относително малки територии (до 1 km^2) се препоръчва използването на летателни апарати с „ротиращо крило, а при заснемане на по-големи територии –

използване на летателни апарати с „фиксирано крило“. БЛА са оборудвани с автопилот за следване на плана за летене, включване на фотокамерата в определените позиции, както и двупосочна радиовръзка. Това позволява проследяването на полета и получаването на телеметрична информация за параметрите на полета в реално време. В същото време данните от полета се записват и впоследствие се използват за уточняване на позицията на летателния апарат и на камерата в момента на заснемане. [3]

При съвременните БЛА точността която се получава е не достатъчно точна за създаване на карта и височинен модел на земната повърхност, но с помощта напоследваща софтуерна обработка на данните и използване на ГНСС приемници, тази грешка се свежда до такава че получените данни след обработка да отговарят на изискванията за заснемане в кратък срок на не големи по площ обекти, като населено място, квартал или имот, земеделски и горски площи. [2]

Използването и поддържането на БЛА е много по-евтино сравнение с класическите фотограметрични способи и има по-голямата гъвкавост при приложението им в зони с висок риск, където живота на пилота и оператора биха били застрашени. [6]

2. Създаване на ортофото карта и височинен модел

В избраният район за заснемане с БЛА, се създават контролни точки, като техните координати се снемат с помоща ГНСС приемници в режим RTK, с точност ±2. Точките на терена (GCP) се отбелязват със специални марки, който при заснемането ще са лесно различими на терена. [1]

Следващата стъпка е подготвяне на План за летене. Това се извършва с помощта на специализиран софтуер върху височиния модел на територията за заснимане. Такива софтуери които се използват свободно са DroneDeploye, Pix4Dcapture, DJI GO 4 и др . След като плана за летене е готов следва заснемането на терена от БЛА.

Фиг. 1. Ортофото карта

Данните от ГНСС приемика и БЛА се въвеждат в специализирани софтуери за обработка, като AGISOFT, Pix4D, 3DSurvey и др. След обработката се създава височинна карта и ортофотокарта.

3. Анализ на данните след обработка от софтуера

Number of images: 182, Flying altitude: 71.8 m, Ground resolution: 1.72 cm/pix, Coverage area: 1.37e+05 sq m, Camera stations: 181, Tie points: 189,354, Projections: 656,708, Reprojection error:

1.02 pix, Camera Model FC6310S (8.8 mm), Resolution 4864 x 3648, Focal Length 8.8 mm, Pixel Size 2.61 x 2.61 um, Precalibrated No. Camera locations and error estimates average camera location error.

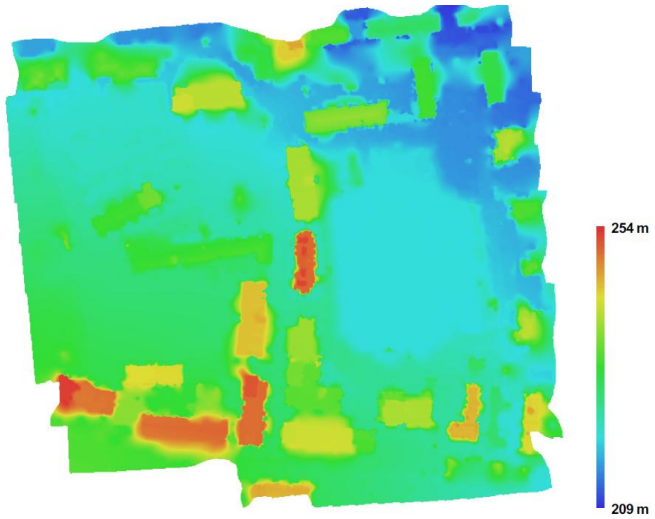
Таблица 1. Точност на изходните данни

X error (m)	**Y error (m)**	**XY error (m)**	**Z error (m)**	**Total error (m)**
1.67285	0.36564	1.71235	18.3585	18.4382

Таблица 2. Където се вижда разликата с точността на координатите.

Label	**XY error (m)**	**Z error (m)**	**Error (m)**	**Projections**	**Error (pix)**
1	0.024651	0.0156537	0.0292012	11	0.242
2	0.0295698	-0.0109004	0.031515	8	0.338
3	0.0206263	-0.00827763	0.0222253	12	0.177
4	0.0250059	0.0102182	0.0270131	9	0.451
5	0.0247412	-0.0123501	0.0276523	12	0.164
Total	**0.0250795**	**0.0117415**	**0.027692**	**-**	**0.280**

Създаване на височинен модел на терена (фиг. 2.)



Фиг. 2. Височинен модел (DTM)

Processing Parameters

General	
Cameras	182
Aligned cameras	181
Markers	5
Coordinate system	WGS 84 (EPSG::4326)
Point Cloud	
Points	189,354 of 206,520
RMS reprojection error	0.151854 (1.02049 pix)
Max reprojection error	0.749224 (25.1655 pix)

Mean key point size	6.30974 pix
Effective overlap	3.59965
Alignment parameters	
Accuracy	Medium
Pair preselection	Generic
Key point limit	40,000
Tie point limit	4,000
Constrain features by mask	No
Matching time	8 minutes 4 seconds
Alignment time	1 minutes 44 seconds
Optimization parameters	
Parameters	fx, fy, cx, cy, skew, k1-k3, p1, p2
Optimization time	6 seconds
Model	
Faces	26,776
Vertices	13,745
Texture	4,096 x 4,096, uint8
Reconstruction parameters	
Surface type	Height field
Source data	Sparse
Interpolation	Enabled
Geometry type	Point cloud
Face count	30,000
Processing time	3 seconds
Texturing parameters	
Mapping mode	Adaptive orthophoto
Blending mode	Max intensity
Texture size	4,096 x 4,096
UV mapping time	3 seconds
Blending time	28 seconds
DEM	
Size	837 x 930
Coordinate system	WGS 84 (EPSG::4326)
Orthomosaic	
Size	23,202 x 21,207
Coordinate system	WGS 84 (EPSG::4326)
Blending mode	Mosaic

4. Заключение

След направените анализи за точността, се вижда че контролните точки спомагат за значително повишаване на точността на ортофотокартата и височинния модел на терена. Получената географска информация намира широко приложение за решаване на различни задачи в областта на геодезията, управлението на териториите и др. Данните се придобиват бързо, лесно и сравнително икономично в сравнение със стандартните методи на фотограметрията Достъпът до този източник на геоинформация е лесен и безопасен за хората и околната среда.

References

1. Андреева П., Димова Г., Андреев А. Приложение на ГИС и ГНСС в навигацията. Proceedings of International Scientific Conference 2021, Faculty of Artillery, Air Defense and Communication and Information Systems - Shumen. 511 - 517 p. ISSN 2367-7902

2. Андреева П., Андреев А. Върху проблемите на геоинформационните технологии у нас. Proceedings of International Scientific Conference 2021, Faculty of Artillery, Air Defense and Communication and Information Systems - Shumen. 492- 502 p. ISSN 2367-7902

3. Беджева М., Т. Игнатова, Analysis of the accuracy of geodesical maps prepared by the means of UAVs, Proceedings of university of Ruse – 2019, volume 58 (на български), ISSN 2603-4123 (on-line)

4. Господинова Веселина, Бегновска Милена, Петков Росен „Изследване възможностите на безпилотните летателни апарати при решаване на геодезически задачи“ Списание Геодезия Картография и Земеустройство – кн. 1-2 2017г. стр. 23.

5. Димитър Петров „ XXIV-ти Международен симпозиум „Съвременните технологии, образованието и професионалната практика в геодезията и свързаните с нея области“ София 06-07-Ноември 2014 г.“

6. Филипов Атанас „Използване на безпилотни летателни системи (БЛС) като платформи за дистанционни изследвания“ Списание „Геомедия“

https://www.geomedia.bg/geodesia/izpolzvane-na-bezpilotni-letatelni-s-4/

---

[i] *Закон за административно-териториалното устройство, изм. ДВ. бр.36 от 1 май 2021г.*

[ii] *Army_Field_Manual__AFM__A5_Master_ADP_Interactive_Gov_Web*

[iii] *Енев Е, Когнитивни процеси при управление на информацията в операции за урбанизирани територии, Монография, 2021г, ISBN 978-619-239-533-9*

[iv] *FM 3-06.Urban operations, Washington, D.C.: Headquarters, Department of theArmy.*

[v] *ATP 3-06 Urban operations Headquarters, Department of the Army - december 2017*

[vi] *Хинов И., Влияние на боеспособността на тактическите формирования върху вземането на решение, дисертация; Рег. №RB 217308-083-06/СИ-29-51/24.02.2022 г.*

[vii] ATP_2-01.3_Intelligence_Preparation_of_the_Battlefield

[viii] Army_Field_Manual__AFM__A5_Master_ADP_Interactive_Gov_Web(1)

[ix] World Urbanization Prospects The 2018 Revision - Methodology

[x] FM 3-06.Urban operations, Washington, D.C.: Headquarters, Department of theArmy.