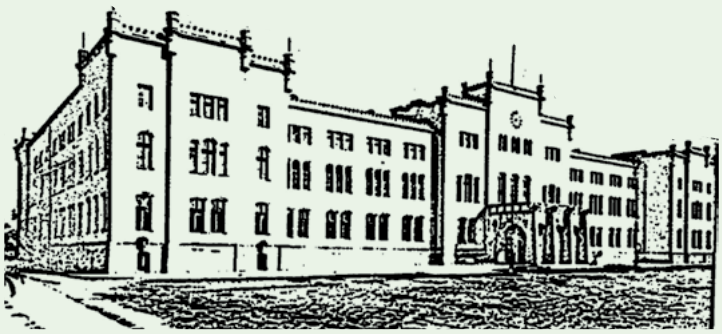
ГОДИШНИК

НА ВОЕННА АКАДЕМИЯ „ГЕОРГИ СТОЙКОВ РАКОВСКИ“



ANNUAL PROCEEDINGS

of Rakovski National Defence College

ТОМ 2 / VOLUME 2
СОФИЯ, 2026 Г. / SOFIA, 2026

ГОДИШНИК
НА ВОЕННА АКАДЕМИЯ „ГЕОРГИ СТОЙКОВ РАКОВСКИ“

РЕДАКЦИОННА КОЛЕГИЯ

Председател:

Полковник доц. д.н. **Петър МАРИНОВ**

Членове:

Полковник доц. д-р **Живко ЖЕЛЕВ**
Полковник проф. д-р **Емил ЕНЕВ**
Полковник доц. д-р **Живо ПЕТРОВ**
Полковник доц. д.н. **Петко ДИМОВ**

Всички публикувани статии са преминали успешно през процедура на двойно „сляпо“ рецензиране и проверка за подобие със специализиран софтуер.

ANNUAL PROCEEDINGS
OF RAKOVSKI NATIONAL DEFENCE COLLEGE

EDITORIAL BOARD

Chairman:

Colonel Assoc. Prof. **Petar MARINOV**, DSc.

Members:

Colonel Dr. **Zhivko ZHELEV**, Assoc. Prof.
Colonel Prof. Dr. **Emil ENEV**
Colonel Dr. **Zhivo PETROV**, Assoc. Prof.
Colonel Assoc. Prof. **Petko DIMOV**, DSc.

All articles published have successfully passed through a double "blind" peer-review procedure and a similarity check with specialized software.

Собственик и издател на Годишник на Военна академия „Георги Стойков Раковски“ е Военна академия „Г. С. Раковски“

ISSN 3033-2672

ВОЕННА АКАДЕМИЯ „ГЕОРГИ СТОЙКОВ РАКОВСКИ“



ОТБРАНА И СИГУРНОСТ
В ЕПОХА НА ДРАМАТИЧНИ ПРОМЕНИ

ГОДИШНА КОНФЕРЕНЦИЯ ● СОФИЯ ● 05 – 06 НОЕМВРИ 2026

СЪДЪРЖАНИЕ / CONTENTS

13 Iron Hand, Velvet Glove: toward Building a Permanent Regulatory Framework for Artificial Intelligence / *Adelina Zhiyanski*

26 Нов модел на организация и управление на авиационната сигурност на летище „Васил Левски“ – София: от традиция към иновация / *Албена Попова*
A New Model for Aviation Security Organisation and Management at Vasil Levski Sofia Airport: from Tradition to Innovation / *Albena Popova*

36 Мениджмънт на системите за симулиране и моделиране в българската военнообразователна система / *Анатоли Палев*
Management of Modeling and Simulation Systems in the Bulgarian Military Education System / *Anatoli Palev*

49 Продължителни грижи за пострадали на бойното поле: приложение на предварителен донорски резерв за осигуряване на цяла кръв / *Антония Пушкарова*
Prolonged Casualty Care on the Battlefield: Application of a Walking Blood Bank for Whole Blood Transfusion / *Antonia Pushkarova*

62 Индикаторен подход за количествен анализ и оценка на резултатите от обучението във висшето военно образование / *Боти Видолов*
Indicator-Based Approach to Quantitative Analysis and Assessment of Learning Outcomes in Higher Military Education / *Boti Vidolov*

72 Проблеми на предвидимостта на системните състояния при неустойчиви условия на средата / *Валентин Василев*
Predictability Problems of System States under Unstable Environmental Conditions / *Valentin Vasilev*

81 Факторът „сили“ в многомерното пространство / *Валентин Василев*
Forces as a Factor of Multidomain Environment / *Valentin Vasilev*

91 Нова концепция и ново решение на проблема FPV дрон и дронова защита на критична, военна и гражданска инфраструктура / *Валентин Каравълчев*
New Concept and New Solution to the FPV Drone Problem and Drone Protection of Critical, Military, and Civilian Infrastructure / *Valentin Karavalchev*

102 AI-Driven Deep Strikes via UAVs in the War in Ukraine: New Capabilities and Operational Art / *Valentin Peychev*

112 Микросъюзите – военно-икономическата симбиоза в средата за сигурност / *Валери Тодоров*
Micro-Alliances – Military-Economic Symbiosis in the Security Environment / *Valeri Todorov*

128 Историческо развитие на концепцията за мисийното командване / *Веселин Георгиев*
Historical Development of the Mission Command Concept / *Veselin Georgiev*

139 Геополитически измерения на структурните предизвикателства пред сигурността на Европейския съюз / *Виктория Вутова*
Geopolitical Dimensions of the Structural Challenges to the Security of the European Union / *Viktoriya Vutova*

152 Влияние на изкуствения интелект върху икономиката и отбраната / *Владислав Василев*
Impact of Artificial Intelligence on the Economy and Defence / *Vladislav Vasilev*

163 From Competitive Intelligence to Risk Intelligence: Reframing Intelligence for Decision Advantage under Uncertainty / *Georgi Dimitrov*

171 Operational-Level Decision Making: Uncertainty Decreasing Tools / *Daniel Roman, Claudiu-Valer Nistorescu*

189 Стратегическо предвиждане за кризисна готовност по източния фланг на НАТО: измерения на национална устойчивост на България в рискова среда за сигурност / *Деница Хинкова*
Strategic Foresight for Crisis Preparedness and Deterrence on NATO's Eastern Flank: Comparative Models and Dimensions of Bulgaria's National Resilience / *Denitsa Hinkova*

207 Гражданската устойчивост в контекста на когнитивните въздействия върху общественото съзнание на българите от Западните Балкани / *Деница Китанова*
Civic Resilience in the Context of Cognitive Impacts on the Public Consciousness of Bulgarians in the Western Balkans / *Denitsa Kitanova*

217 Изкуственият интелект в системата за поддръжка на вземането на решения в системата за сигурност и отбрана / *Деян Иванов*
Artificial Intelligence in the Decision-Making Support System Within the Security and Defence System / *Deyan Ivanov*

229 Съвременни проекции на Арменско-Азербайджанските отношения и европейската сигурност / *Димитър Дринков*
Contemporary Dimensions of Armenian-Azerbaijani Relations and European Security / *Dimitar Drinkov*

238 Ролята на изкуствения интелект в киберсигурността / *Димитър Малкочев*
Interaction Between Cybersecurity and Modern Trends in the Development of Artificial Intelligence / *Dimitar Malkochev*

247 Three-Dimensionally Printed Firearms as an Emerging Security Challenge: Accessibility, Detection and Investigative Responses with Implications for Bulgaria and South-Eastern Europe / *Dimitar Rangelov, Chavdar Georgiev*

260 Нанасянето на далекобойни удари като средство за постигане на дългосрочни оперативно-стратегически цели във войната в Украйна / *Димо Савов, Пламен Дяков*
Long-Range Strikes as a Means of Achieving Long-Term Operational-Strategic Objectives in the Ukraine War / *Dimo Savov, Plamen Dyakov*

278 Възможности за въвеждане на изкуствен интелект в системите за обработка на багаж на летищата / *Елена Стоянова*
Opportunities for the Introduction of Artificial Intelligence in Airport Baggage Handling Systems / *Elena Stoyanova*

288 Приватизацията на войната: частните военни компании като фактор за отбраната и сигурността в променящия се свят / *Запрян Вълков*
The Privatization of War: Private Military Companies as a Factor for Defense and Security in a Changing World / *Zapryan Valkov*

295 From Satsuma Samurai to Meiji Japan: a Scientific Investigation of the Participation and Contributions of Seigo Yamazawa in the Liberation of Bulgaria / *Ivan Botev, Atanas Vladikov*

303 Алтернативи за управление на военния риск за търговското корабоплаване в зони на конфликт / *Иван Вълков*
Alternatives for Managing War Risk to Merchant Shipping in Conflict Zones / *Ivan Valkov*

319 Условия за успешна реализация на еволюиращи системи за командване, управление, комуникации, компютри, киберпространство, разузнаване, наблюдение и войсково разузнаване (C5ISR) с отворена архитектура / *Иван Иванов, Антон Манчев, Иван Чакъров*
Conditions for the Successful Realization of Evolving C5ISR Systems with Open Architecture / *Ivan Ivanov, Anton Manchev, Ivan Chakarov*

334 Локални безжични мрежи, базирани на технологии за клетъчни системи от шесто поколение (6G LAN): особености, архитектура и перспективи / *Иван Иванов, Александър Колев, Иван Чакъров*
Local Wireless Networks Based on Technologies of Sixth-Generation Cellular Systems (6G LAN): Features, Architecture and Prospects / *Ivan Ivanov, Alexander Kolev, Ivan Chakarov*

347 Публично-частно партньорство при защитата на критичната инфраструктура: сравнителен анализ и предложения за нормативно регулиране в Република България / *Иван Кутелов*
Public-Private Partnership in Critical Infrastructure Protection: a Comparative Analysis and Proposals for Bulgaria / *Ivan Kutelov*

363 Дигиталните измерения на крайнодесния екстремизъм: онлайн радикализация, дезинформация и рискове за вътрешната сигурност на България / *Ивелина Дундакова*
The Digital Dimensions of Far-Right Extremism: Online Radicalization, Disinformation, and Risks to Bulgaria’s Internal Security / *Ivelina Dundakova*

377 Автоматизирани решения и системи с изкуствен интелект в управлението на корпоративния риск / *Илина Козарова-Арменчева, Мирослава Младенова*
Automated Solutions and Artificial Intelligence Systems in Corporate Risk Management / *Ilina Kozarova-Armencheva, Miroslava Mladenova*

390 Теоретични аспекти на стратегическата стабилност през призмата на съвременната среда на сигурност / *Йорданка Савова*
Theoretical Aspects of Strategic Stability Through the Prism of the Contemporary Security Environment / *Yordanka Savova*

402 Устойчивостта като форма за намаляване на риска и несигурността във военното дело / *Калин Градев*
Resilience as a Form of Reducing Risk and Uncertainty in the Military Sphere / *Kalin Gradev*

413 Адаптацията на системите за отбрана в Българската армия и предизвикателствата пред сухопътните войски / *Калин Градев*
The Adaptation of Defense Systems in the Bulgarian Army and the Challenges Facing the Land Forces / *Kalin Gradev*

422 Влияние на макроикономическата среда върху сигурността и отбраната / *Катя Пейчева*
Impact of the Macroeconomic Environment on Security and Defence / *Katya Peycheva*

435 Оперативна среда и противоминен капацитет в Черно море: регионални казуси, дефицити и доктринални реалности / *Красимир Ангелов*
Operational Environment and Mine Countermeasures Capacity in the Black Sea: Regional Case Studies, Deficits and Doctrinal Realities / *Krasimir Angelov*

444 Мрежово-центричен модел на система от системи в противоминната борба / *Красимир Ангелов*
Network-Centric System of Systems Model in Mine Countermeasures / *Krasimir Angelov*

454 Комуникационни модели на влиянието на медийната информация върху спорта като елемент на националната устойчивост / *Кубрат Пулев*
Communication Models of the Influence of Media Information on Sport as an Element of National Resilience / *Kubrat Pulev*

464 Системен подход за противодействие на безпилотни летателни апарати / *Любосвет Стоев, Живо Петров*
Systems Approach to C-UAS Operations / *Lyubosvet Stoev, Zhivo Petrov*

480 Скрининг на рисковите профили на държавната граница на Република България като инструмент за превенция на заплахи за националната сигурност / *Мохамед Насри*
Screening of Risk Profiles at the State Border of the Republic of Bulgaria as an Instrument for Preventing Threats to National Security / *Mohamed Nasri*

493 Периферия или стратегически кръстопът: променя ли се ролята на Югоизточна Европа в европейската сигурност / *Невена Алексиева*
Periphery or Strategic Crossroads: is the Role of Southeastern Europe in European Security Changing / *Nevena Aleksieva*

506 Използване на виртуалната реалност в тактическото изграждане на отбраната и сигурността / *Невяна Петкова*
The Use of Virtual Reality in the Tactical Development of Defense and Security / *Neviana Petkova*

516 Влияние на пространствено-времевите фактори, хидрометеорологичната среда и логистичния дефицит върху оперативните способности при далечни полярни плавания / *Николай Данаилов*
Influence of Spatial-Temporal Factors, the Hydrometeorological Environment, and Logistical Deficits on Operational Capabilities during Long-Distance Polar Sailings / *Nikolay Danailov*

529 Причинен принос и граници на причинния извод при изследването на реализирани загуби в областта на националната сигурност / *Николай Илиев*
Causal Contribution and the Limits of Causal Inference in the Study of Realized Losses in the Field of National Security / *Nikolay Iliev*

538 Конфигурации от реализирани загуби и контрол срещу двойно отчитане в областта на националната сигурност / *Николай Илиев*
Configurations of Realized Losses and Double-Counting Control in the Field of National Security / *Nikolay Iliev*

549 Управляемост в ерата на изкуствения интелект: кибернетичен прочит на рисковете / *Николай Николов*
Governability in the Age of Artificial Intelligence: A Cybernetic Reading of the Risks / *Nikolay Nikolov*

558 Динамика на резилентността на българското общество срещу информационно въздействие и дезинформация: сравнителен анализ 2023 – 2025 г. / *Петко Димов*
Dynamics of the Resilience of Bulgarian Society Against Information Influence and Disinformation: A Comparative Analysis 2023 – 2025 / *Petko Dimov*

573 Геополитическите измерения на военноисторическата компаративистика: методологически и приложни аспекти / *Радослав Бонев*
The Geopolitical Dimensions of Military-Historical Comparativistics: Methodological and Applied Aspects / *Radoslav Bonev*

581 Преподаването на философия във Военната академия: дидактически предизвикателства и перспективи / *Радослав Бонев*
Teaching Philosophy at the Military Academy: Didactic Challenges and Perspectives / *Radoslav Bonev*

591 Програмно и апаратно осигуряване на автономни безпилотни летателни системи / *Севдалин Стойков, Венелин Рашков, Александър Колев, Иван Иванов*
Software and Hardware Provision for Autonomous Unmanned Aerial Systems / *Sevdalin Stoykov, Venelin Rashkov, Alexander Kolev, Ivan Ivanov*

602 От състояние към отношение: стратегизацията на икономическата сигурност при стратегическа взаимозависимост / *Станимир Станев*
From State to Relation: The Strategization of Economic Security under Strategic Interdependence / *Stanimir Stanev*

617 Лидерство и организационни подходи в управлението на образователния процес в ерата на изкуствения интелект / *Стоян Червеняков*
Leadership and Organizational Approaches to the Management of the Educational Process in the Era of Artificial Intelligence / *Stoyan Chervenyakov*

631 Разсекретяване на разузнавателна информация като инструмент на стратегическите комуникации / *Теменуга Хасекиева*
Declassification of Intelligence Information as an Instrument of Strategic Communications / *Temenuga Hasekieva*

644 Сигурност, бедност, климат: защо хората мигрират / *Христо Маруков*
Security, Poverty, Climate: Why People Migrate / *Hristo Marukov*

655 Трудовата миграция – нищо тревожно, погледнато и от двете страни / *Христо Маруков*
Labor Migration – Nothing to Worry About, Viewed from Both Sides / *Hristo Marukov*

669 Предизвикателството U-space за изпълнение на държавни полети с безпилотни въздухоплавателни средства / *Христо Станев*
The U-space Challenge to Perform State Flights with Unmanned Aircraft / *Hristo Stanev*

683 Шенген като геополитически риск-мултипликатор: разпространението на адитивно произведени огнестрелни оръжия в контекста на войната в Украйна и сигурността на Източния фланг на ЕС/НАТО / *Чавдар Георгиев, Димитър Рангелов*
Schengen as a Geopolitical Risk-Multiplier: The Proliferation of Additively Manufactured Firearms in the Context of the War in Ukraine and the Security of NATO's Eastern Flank / *Chavdar Georgiev, Dimitar Rangelov*

701 Military History as a Potential Mechanism of Civic Identity Formation: Public Perceptions of Patriotic Education in Kazakhstan and the Bulgarian Experience / *Yelvira Ibadullayeva*

https://doi.org/10. 66334/annu26_ironvelvet

IRON HAND, VELVET GLOVE: TOWARD BUILDING A PERMANENT REGULATORY FRAMEWORK FOR ARTIFICIAL INTELLIGENCE

Adelina Zhiyanski
Rakovski National Defence College (Bulgaria)

Abstract. Artificial intelligence is reshaping the strategic, military, defence and decision-making landscape faster than existing regulatory frameworks can follow. This paper introduces the "Iron Hand, Velvet Glove" concept as a governance framework designed to balance firm institutional control with the flexibility required to foster technological innovation. Moving beyond static, legislation-driven models, the paper proposes a shift toward permanent, adaptive oversight capacity – one that enables countries and security institutions to continuously monitor, anticipate, assess and respond to emerging AI risks across military, cyber, informational as well as economic domains. The central contribution is the reconceptualization of AI governance as a strategic capability rather than a purely administrative function, requiring institutional coordination, adaptive risk management and mechanisms for timely intervention. The framework offers a novel approach to maintaining effective oversight throughout the full cycle of AI development and deployment, which ensures that regulatory capacity evolves alongside the technology it seeks to govern.

Keywords: adaptive regulation; artificial intelligence; human decision-making; national security; strategic governance

I. Introduction

Artificial intelligence (AI) is no longer a technology of the future. It is a present and accelerating force that is reshaping the conditions under which countries encounter and manage conflicts. AI has indeed embedded itself across the full spectrum of national security- from autonomous weapons systems to algorithmic decision-making intelligence, from cyber operations to economic forecasting tools used by individuals and governments. For a significant amount of time the question was whether AI will transform the world we live in. Now that it is doing so, the most important question that stands is whether governments can keep pace with the development of AI.

The challenge itself can be considered mainly structural, as most of the existing regulatory frameworks were initially designed for a world in which technology evolved at human-institutional speed. In that world, legislatures could observe a problem, deliberate, draft a response and implement it before the technology had changed beyond recognition. With AI, this is temporally impossible as its capabilities evolve throughout rapid deployment and learning as well as an extremely fast diffusion across sectors and borders. By the time a regulatory response is enacted toward one generation of AI, the next generation has already rendered it obsolete (Dafoe 2018).

This paper argues that the response to this complex challenge cannot be another static regulatory instrument, as what is required is a fundamentally different approach toward this new world we are and will be living in- a new conception of governance which is adaptive and institutionally embedded. The metaphor proposed in this paper is “Iron Hand, Velvet Glove” concept, which is used to illustrate the dual nature of this challenge and the need to conceptualize the balance between firm control – the clear mechanisms for accountability, monitoring, risk assessment, and regulatory flexibility as the need for innovation and technological development stands in the center of each country’s national security success.

II. Materials and Methods

This study adopts a conceptual and qualitative analytical approach to develop the Iron Hand, Velvet Glove framework for adaptive AI governance. Rather than testing a predefined regulatory model empirically, the study synthesizes established concepts from governance and regulatory theory with contemporary approaches to AI governance in order to identify the institutional capacities required for effective and adaptive oversight of rapidly evolving AI technologies.

The conceptual analysis draws on three main bodies of literature: adaptive governance, risk-based regulation, and AI-specific governance. Adaptive governance provides the theoretical basis for continuous monitoring, institutional learning and feedback mechanisms in conditions of uncertainty and rapid change. Risk-based regulatory theory provides the rationale for differentiating the intensity of regulatory intervention according to the nature and magnitude of potential risks. AI governance literature and existing regulatory initiatives provide the technological and institutional context within which these principles are examined.

The analytical process was structured in three stages. First, the characteristics of AI deployment across military, cyber, informational, economic and strategic decision-making domains were examined to identify governance challenges associated with technological speed, opacity, cross-sectoral diffusion and potential high-impact consequences. Second, these characteristics were considered in relation to the limitations of conventional regulatory approaches, with particular attention to three structural challenges identified in the analysis: the temporal mismatch between technological development and regulatory response, jurisdictional fragmentation, and the limited transparency and predictability of advanced AI systems. Existing risk-based regulation, voluntary ethical frameworks and international governance principles were considered as reference points for assessing how current approaches address these challenges.

Third, the identified governance challenges were translated into institutional requirements. This analytical mapping resulted in four interconnected functional pillars: (1) horizon scanning and continuous monitoring; (2) adaptive risk classification; (3) institutional coordination and international cooperation; and (4) enforceable authority and accountability. These pillars form the operational architecture of the Iron Hand, Velvet Glove framework. The "iron hand" represents the non-negotiable component of governance- legal authority, accountability and the capacity for regulatory intervention – whereas the "velvet glove" represents adaptability, proportionality, institutional learning and mechanisms that allow regulation to evolve in response to technological development.

The resulting framework is therefore not proposed as a replacement for existing risk-based regulatory systems. Instead, it is developed as a complementary institutional layer intended to provide continuous regulatory adaptation between formal legislative interventions. The analysis is conceptual and exploratory; consequently, the framework should be understood as a basis for further empirical testing, institutional comparison and operational development rather than as a validated regulatory model.

III. The Diffusion of AI across Security-Relevant Domains

In order to understand why AI governance requires a completely new approach, it is necessary to understand the scale and character of AI's penetration into all domains that are of strategic importance. Important to note is that this diffusion does not follow a linear pattern. It proceeds across multiple axes simultaneously. By doing so, it generates governance challenges that are qualitatively different from those posed by previous dual-use technologies.

3.1. Military & Operational Domains

Looking back at the mid-2010's, the integration of AI into the military sector and its systems has accelerated substantially and examples of this are the semi-autonomous weapons systems, AI-assisted targeting, logistical optimization and battlefield awareness tools. All those listed above are no longer experimental, rather they are completely deployed and/or in advanced development by multiple country actors (Scharre 2018). AI-enabled systems can now operate at speeds that preclude meaningful human decision-making in the loop, simply by compressing time between threat detection and response. The threshold for initiating conflict may now be lowered by the reduced cost of military action. This clearly suggests that the implications for international security are profound.

At the same time, AI introduces new forms of strategic vulnerability as systems trained on historical data can perform poorly, sometimes catastrophically in novel operational environments and threats. By stating this, there is another important component which are exactly the adversarial manipulations of AI inputs – the so-called "adversarial AI attacks". Machine tricks and manipulated inputs which cause systems to misclassify targets or generate false intelligence assessments, leading to disastrous outcomes (Brundage et al. 2018). The current opacity of the majority of AI systems, especially those based on deep learning architectures creates accountability gaps that the existing military doctrine and the international laws are poorly equipped and not ready to address.

3.2. Cyber and Informational Domains

AI has also fundamentally changed the character of cyber operations and information warfare. On the offensive side, AI enables the automation of discovering vulnerability, the generation of personalized phishing attacks and synthetic media. All this at a scale and speed that deceives human judgment and most of all- overwhelms traditional detection capabilities (Chesney, Citron 2019). On the other side, there is a significant protection aspect as the current AI-powered

anomaly detection and threat intelligence systems offer new capabilities for protecting critical infrastructure and communications networks.

Analyzing AI on both those sides can also be interpreted in the informational domain, where there are particularly acute governance challenges being presented. The same AI capabilities that enable targeted advertising can also be weaponized for influence operations where it shifts public opinions, undermines electoral processes and erodes the epistemic foundations of democratic deliberation (Floridi et al. 2018). It is now increasingly evident that the threats around AI do not respect sandboxes or any form of restrictions. Borders and limits mean little when AI operates at a tempo that leaves regulatory response purely reactive.

3.3. Economic & Decision-Making Domains

Beyond the security sector, AI is highly impacting the economic domain. Currently there are thousands of algorithmic trading systems, AI-assisted sanction enforcement, supply chain analysis, predictive economic modelling as well as the human factor- those systems being used by humans. Switching back to countries, the above mentioned are increasingly central to how countries exercise economic power and manage strategic competition. Furthermore, the concentration of advanced AI capabilities in a small number of private companies, mainly in the USA and China, creates asymmetries that smaller countries must navigate with extreme caution (Kissinger, Schmidt, Huttenlocher 2021).

Perhaps the most consequential is the fact that AI is entering the domain of strategic decision-making. This domain was mainly human-led and navigated, whereas now AI tools aggregate and analyze a vast quantity of intelligence data and information, generate policy options and are used at senior and overall higher levels of government. This raises the fundamental questions about accountability. To what extent is the delegation of strategic assessment to algorithmic systems reliable, and under what conditions must human judgment remain sovereign?

IV. The Concept: Iron Hand, Velvet Glove

The central conceptual contribution of this paper is the intertwined character of AI- the Iron Hand, Velvet Glove concept. This section develops the main concept in detail by explaining the theoretical foundations and by distinguishing it from the existing approaches to technology regulation, decision-making and accountability.

4.1. Origin & Meaning

The phrase “iron hand in a velvet glove” has a long history in political thought, most commonly attributed to a single figure. Napoleon Bonaparte, who is

said to have used it to describe the relationship between authority, tact and diplomacy in governance. This metaphor captures a fundamental tension in the exercise of power- the necessity of firm, non-negotiable authority and the equally necessary quality of flexibility, adaptability and restraint in its applications. An iron hand without a velvet glove is pure tyranny- rigid, brittle and ultimately self-defeating. On the contrary, a velvet glove without an iron hand is ineffectual- warm to the touch but completely incapable of exerting meaningful force when required.

Applied to AI governance, this metaphor takes the idea on a new level and has a precise institutional meaning. The "iron hand" represents the hard core of regulatory authority without which there is pure chaos and inability to react properly. With it, there are clear legal mandates, enforceable accountability requirements and most of all- the institutional capacity to intervene when AI systems cause or threaten harm. This is non-negotiable. Without it, governance is merely advisory and the history of self-regulation in the technological sector provides ample evidence of its inadequacy (Calo 2017).

The second important aspect of the concept is the "velvet glove" which represents flexibility, adaptiveness and proportionality of the architecture of regulations. It entails a whole system unit of regulatory sandboxes that allow controlled experimentation, tiered compliance requirements calibrated to the level of risk, updating mechanisms that allow frameworks to evolve without full legislative cycles and collaborative governance structures that incorporate technical expertise, together with democratic accountability. In no case can it be concluded that the velvet glove is a softening of regulatory authority. On the contrary, it is the means by which that authority remains effective, as well as legitimate and most of all – capable of governing a technology which has no days off and is no longer predictable.

4.2. Theoretical Foundation

The "Iron Hand, Velvet Glove" concept draws on three pillars of governance theory that, taken together, provide its intellectual foundation.

First, it draws on the adaptive governance literature- the study of institutional arrangements designed to manage complex, rapidly evolving systems characterized by uncertainty (Folke et al. 2005). The scholarship on adaptive governance emphasizes on the importance of monitoring, mechanisms for feedback, institutional learning as those are the core functions of an effective governance, rather than treating legislation as a one-time intervention.

Second, the concept draws on risk-based regulatory theory, which holds that the intensity and character of regulatory intervention should be proportion-

ate to the level of risk posed by the regulated activity (Baldwin, Cave, Lodge 2012). Applied to AI, this suggests that governance frameworks should differentiate sharply between high-risk applications (e.g. autonomous weapons, critical infrastructure control, judicial decision-making) and lower-risk applications, applying corresponding different levels of oversight, accountability and intervention authority.

Third, the concept engages with the currently emerging literature on AI-specific governance, which has increasingly converged on the view that AI requires purpose-built institutional arrangements rather than the extension of existing regulatory categories (Dafoe 2018; Russell 2019; Harari 2024). The Iron Hand, Velvet Glove concept builds on this insight by specifying what those arrangements must be capable of doing. Not simply regulating AI as it exists now but governing it as it continues to develop and change.

4.3. The Existing Approaches and The New Concept

It is of key importance to distinguish the concept of the "Iron Hand, Velvet Glove" from the two existing approaches that are in the field of AI governance.

The first is the European Union's AI Act, which is the most comprehensive attempt up to this date to regulate AI through risk-based classification.[1] It is a significant advance, however it remains in its core idea a legislative instrument. The AI Act establishes categories and requirements at a point in time and depends on conventional amendment processes to update them. On the other side, the concept in this paper proposes something different and most importantly- more adaptive. In the core of the idea stands a permanent institutional capacity that can update its own parameters in response to the fast technological change without waiting for legislative revisions.

The second existing approach comprises voluntary frameworks and ethical guidelines for AI, including the OECD Recommendation on Artificial Intelligence[2] and the UNESCO Recommendation on the ethics of Artificial Intelligence[3], as well as numerous national AI strategies that have emerged since 2016. These frameworks articulate important principles and normative commitments but generally rely on limited or indirect enforcement mechanisms. In terms of the proposed concept, they therefore represent the "velvet glove" without a sufficiently developed "iron hand." However, the Iron Hand, Velvet Glove framework should not be understood as an alternative to risk-based regulation, including the approach established at EU level. Rather, it complements such regulation by adding a permanent institutional layer of continuous monitoring, regulatory adaptation and responsive intervention,

allowing governance mechanisms to evolve alongside technological developments.

V. The Structural Failures of the Current Regulatory Approaches

Now that the conceptual foundation has been established, this section focuses on the record of AI regulation up to this date. In this section the structural patterns of failure will be identified, where the Iron Hand, Velvet Glove can actually be a long-term solution, if properly structured and applied throughout the evolution of technology.

5.1. The Timing Mismatch

Time is the most valuable asset. By not approaching it in this manner, there is a significant chance of falling behind considering the fast development of AI. The legislative and regulatory processes operate on a timescale which spans from years to decades. Yet, this timeframe is extremely wide, considering AI's capability to squeeze this timeframe in months to years. This significant timing mismatch puts a considerably bigger challenge in front of technology governing bodies. They become incapable of governing the current generation, as it is already several steps ahead (Calo 2017).

The history of AI regulation illustrates this vividly. The EU AI Act was first proposed in April 2021, before generative AI tools such as ChatGPT reached the public in late 2022. By the time the Act entered into force in 2024, the AI landscape had already changed dramatically by the new generative AI systems. The Act needed an urgent change and guidance to address this new reality of AI, a change that itself risks becoming unusable the moment it takes effect.

5.2. The Gap in Jurisdiction

As previously mentioned, the AI development is rapid and does not respect borders. Its updated versions become global at a single click, yet regulatory authorities remain national and regional. This creates a competitive dynamic which tips the scales in favour of AI and puts different regions and countries at a risky situation (Kissinger, Schmidt, Huttenlocher 2021). At the same time, the concentration of frontier AI development in the already mentioned small number of private actors means that the regulatory jurisdiction in smaller democracies in Europe has the least direct leverage over the entities whose decisions shape AI's development. This raises the question of whether AI's development is part of the modern hybrid conflict. If it is, how can smaller democracies defend their interests against actors with such leverage? Such aspects of AI's development show

that it is a strategic instrument for power, which if not used correctly and without the necessary legislative framework, could lead to large scale conflicts.

5.3. Opacity

Effectiveness in regulation requires a good understanding of what is, in reality, being regulated. Many of the current AI systems that are advanced, especially those based on large neural networks, are not fully transparent even to their developers. The internal processes and failure modes of these exact systems cannot be fully specified in advance or with a reliable prediction. At first glance this looks like a small technical inconvenience when in fact it is a fundamental challenge to the idea of regulation-by-specification that underlies most existing approaches (Russell 2019).

As the whole AI idea is based on a what-if- then scenario and concept, then it can be concluded that: If nothing can be specified in advance and if there is no guarantee, then compliance-based regulation is structurally impossible. Instead, what is required is a monitoring and intervention capacity that can detect harmful behavior as it emerges and respond timely. This is precisely what permanent institutional oversight can provide and periodic legislative regulation cannot.

VI. Toward a Permanent Regulatory Framework

There is an evident need for a permanent AI regulatory framework whose institutional architecture is consistent with the Iron Hand, Velvet Glove concept. The framework in this section is organized around four functional pillars, which together address the structural failures identified in Section V.

6.1. ONE: Horizon Scanning & Continuous Monitoring

The timing mismatch stands as the main issue in terms of establishing a permanent capacity for continuous monitoring of AI development and deployment. This is not a one-time regulatory assessment but an ongoing institutional function, as an example similar to the continuous market surveillance conducted by financial regulators. This continuous monitoring has three distinct activities. First is the technical horizon scanning. Tracking AI's capability developments, assessing the potential security implications are crucial moments before deployment. Second comes the incident monitoring. A systematic approach is needed so that reports of AI system failures are collected and analyzed so that an evidence base for adaptive regulatory response is made. Last, deployment monitoring, which is tracking the penetration of AI systems into critical sectors and decision-making processes, as well as identifying concentrations of AI-mediated power that may require regulatory attention.

The main point is still that a separate institutional home should be created, which is independent of both the AI industry and the political executives. There are many useful templates of independent depots such as the Financial Stability Board in monitoring risk (Baldwin, Cave, Lodge 2012).

6.2. TWO: Adaptive Risk Classification

The opacity problem is situated exactly here, as moving from specification-based to performance-based risk classification is easier said than done. An adaptive risk classification can help in updating risk assessments based on observed behaviours, incident data sheets and evolving technical understanding. This, of course, requires a tiered system with clear criteria for upward and downward reclassification, administered again by the independent monitoring body established under pillar one (6.1). The high-risk classifications trigger mandatory transparency requirements, audit rights, reporting obligations as well as pre-deployment assessments; the lower-risk ones permit lighter-touch oversight. The key innovation is that these classifications are not fixed at a moment of legislation but are continuously being updated as the evidence base evolves. By stating this, an important aspect are the Principles of Responsible Use set out in NATO's Artificial Intelligence Strategy.[4] The concept in this paper bases itself on exactly this- to operationalize those principles through binding institution mechanisms rather than voluntary commitments.

6.3. THREE: Coordination & Cooperation

The jurisdictional gap. By establishing structured coordination mechanisms between the national regulatory bodies and between countries, however again this does require something more than the current landscape of parallel, uncoordinated initiatives. At a national level, effective AI governance requires coordination across multiple stakeholders such as defence, interior, finance, justice, that currently operate with limited information sharing and no common framework in terms of AI risk assessment. A permanent AI governance body must have a cross- governmental mandate and the authority to coordinate regulatory activities across these silos. On an international level- a development of minimum common standards for AI safety and security. Just as the Basel Accords in banking regulation, this will establish a floor below which no country would permit AI deployment in defined high-risk applications. Those standards can be developed throughout the existing OECD, G7, NATO and can be binding on member countries through their national implementation (Dafoe 2018).

6.4. FOUR: Authority & Accountability

The fourth pillar is the iron hand itself. The real, enforceable authority to intervene when AI systems cause or threaten harm. Without this, the preceding three pillars are intelligence without power. Intervention authority must include the power to require modification or suspension of AI systems that pose risks and in extreme cases can prohibit the deployment of specific AI applications entirely. Such powers must be subject to procedural safeguards, including judicial review. Accountability mechanisms must ensure that the legal and ethical responsibility for AI-caused harm can be traced to specific individuals and/or institutional actors. This is both a matter of justice and a one of governance, as such an accountability creates space for responsible development and deployment that voluntary frameworks cannot replicate (Floridi et al. 2018).

VII. Conclusion

This paper has discussed that the governance of artificial intelligence requires a fundamental change. AI is not new, however its recent development shows a global security threat, as acknowledged by OpenAI CEO Sam Altman before the UN Security Council.[5] As of September 2026, Anthropic and OpenAI have publicly committed to voluntarily slowing the pace of frontier AI development.[6] This is further evidence that, in the absence of regulation, even the developers of a technology are calling for restraint. Or maybe such a viral message is a bidding game on the back end for the bigger players and actors as such a voluntary pacing may simply consolidate the advantage of the largest players (NPR 2026). In this sense, the iron hand is a machine, and the velvet glove is the human factor. One without the other is terror- together, they are development and success.

As AI is a transformative key, it is already changing the domains of military power, cyber operations and information warfare- all aspects that the current frameworks are incapable of governing properly and adequately. The Iron Hand, Velvet Glove concept proposed offers a coherent response to this challenge. It insists that there need to be accountability mechanisms that can monitor the ongoing development of AI in real time, where the iron hand is exactly those mechanisms and the velvet glove- where adaptability is the core aspect of the institutional architecture.

This concept is based upon an adaptive governance theory, risk-based regulations and the emerging literature on AI-specific governance. The central argument is that AI governance must be understood as a strategic capability, not a legislative exercise performed once and then left to age, but a permanent insti-

tutional function which is central to national security and therefore military readiness. The countries that develop this capability are likely to emerge as leading strategic forces due to their effective sovereignty and an adequate regulation of AI. Artificial intelligence will not decide who leads the century, but the countries that learn to govern it- will.

NOTES

1. EC, 2021. *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*. COM (2021) 206 final. Brussels: European Commission.

2. OECD, 2019. Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. *OECD Legal Instruments* [online] [last viewed 28.09.2026]. Available from: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

3. UNESCO, 2021. Recommendation on the Ethics of Artificial Intelligence. *UNESCO Digital Library* [online] [last viewed 28.09.2026]. Available from: https://unesdoc.unesco.org/ark:/48223/pf0000381137.

4. NATO, 2021. Summary of the NATO Artificial Intelligence Strategy. *NATO* [online] [last viewed 28.09.2026]. Available from: https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

5. ALTMAN, S., 2026. Sam Altman's Remarks at the United Nations Security Council. *OpenAI* [online], 2026 [last viewed 28.09.2026]. Available from: https://openai.com/index/sam-altman-un-security-council-remarks.

6. AMODEI, D., 2026. We Must Pace the Frontier. *DarioAmodei* [online] [last viewed 28.09.2026]. Available from: https://darioamodei.com/post/we-must-pace-the-frontier; HA, A., 2026. Anthropic CEO Outlines Plan to Slow AI Development. *TechCrunch* [online] [last viewed 28.09.2026]. Available from: https://techcrunch.com/2026/09/12/anthropic-ceo-outlines-plan-to-pace-the-frontier.

REFERENCES

BALDWIN, R.; CAVE, M.; LODGE, M., 2012. *Understanding Regulation: Theory, Strategy and Practice.* 2nd ed. Oxford: Oxford University Press. ISBN 9780199576081.

BRUNDAGE, M. et al., 2018. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. *Arxiv* [online]. Available from: https://doi.org/10.48550/arXiv.1802.07228h [28.09.2026].

CALO, R., 2017. Artificial Intelligence Policy: A Primer and Roadmap. *UC Davis Law Review,* vol. 51, no. 2, pp. 399-435.

CHESNEY, R.; CITRON, D., 2019. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review,* vol. 107, no. 6, pp. 1753 - 1820.

DAFOE, A., 2018. AI Governance: A Research Agenda. *Oxford: Centre for the Governance of AI, Future of Humanity Institute, University of Oxford* [online]. Available from: https://cdn.governance.ai/GovAI-Research-Agenda.pdf [28.09.2026].

FLORIDI, L. et al., 2018. An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines,* vol. 28, no. 4, pp. 689 – 707.

FOLKE, C. et al., 2005. Adaptive Governance of Social-Ecological Systems. *Annual Review of Environment and Resources,* vol. 30, pp. 441 – 473.

HARARI, Y.N., 2024. Nexus: A Brief History of Information Networks from the Stone Age to AI. London: Vintage Publishing. ISBN 9781529923506.

KISSINGER, H.; SCHMIDT, E.; HUTTENLOCHER, D., 2021. *The Age of AI: And Our Human Future.* New York: Little, Brown and Company. ISBN 9780316273800.

RUSSELL, S., 2019. *Human Compatible: Artificial Intelligence and the Problem of Control.* New York: Viking. ISBN 9780525558613.

SCHARRE, P., 2018. *Army of None: Autonomous Weapons and the Future of War.* New York: W. W. Norton & Company. ISBN 9780393356588.

Adelina Zhiyanski
National Security and Defence Faculty
Rakovski National Defence College
Sofia, Bulgaria
E-mail: adeline.zhiyanski@gmail.com

https://doi.org/10. 66334/annu26_newavia

НОВ МОДЕЛ НА ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ НА АВИАЦИОННАТА СИГУРНОСТ НА ЛЕТИЩЕ „ВАСИЛ ЛЕВСКИ“ – СОФИЯ: ОТ ТРАДИЦИЯ КЪМ ИНОВАЦИЯ

д-р Албена Попова
„СОФ Кънект“ ЕАД

Абстракт. Дейност от стратегическо значение и ключова отговорност на летищния оператор „СОФ Кънект“ е гарантирането на сигурността и защитата на пътниците, екипажите, персонала, обществеността, въздухоплавателните средства и инфраструктурата от актове на незаконна намеса. За поддържане на устойчиво високо ниво на сигурност, качество на изпълнение и непрекъсваемост на операциите висшето ръководство на компанията инициира иновативен подход за трансформация в организацията и управлението на сигурността, насочен към повишаване на ефективността, развитие на човешкия ресурс и култура на сигурност. Трансформацията е реализирана чрез преминаване от традиционен модел на управление към модел, основан на екипност, отговорност и постигане на измерими резултати. Новият подход в управлението на сигурността е проектиран и осъществен като неразделна част от цялостната оперативна, културна и дигитална трансформация на компанията, с фокус върху пътническото преживяване,

повишаване на ефективността и превръщане на летище „Васил Левски“ – София в модерен 5-звезден регионален център.

Ключови думи: летище; трансформация; авиационна сигурност; иновативен подход; ефективност; култура на сигурност

I. Въведение

„СОФ Кънект“ ЕАД е лицензираният летищен оператор на най-голямото международно летище в Република България. Фирмата е собственост на френския инфраструктурен фонд Meridiam и поема управлението на летище „Васил Левски“ – София през 2021 г. с ясно изразена стратегическа цел за развитие и модернизация чрез прилагане на най-добрите практики и високи стандарти в услугите и обслужването. За нейното постигане висшето ръководство на компанията разработва план-програма с поставени цели за цялостна оперативна, културна и дигитална трансформация с фокус върху пътническото преживяване и с очаквани крайни резултати за повишаване на ефективността и превръщане на летището в модерен 5-звезден регионален авиационен център.

Наред със стремежа за постигане на висока удовлетвореност сред пътниците, партньорите и обществеността, неотменна и ключова отговорност на компанията е предоставянето на висококачествено авиационно и търговско обслужване с фокус върху осигуряването и поддържането на безопасността и сигурността на полетите, оперираци от и до летище „Васил Левски“ – София. В тази връзка една от най-важните и критични дейности, произтичащи от поетите ангажименти на компанията, е гарантирането на сигурността и защитата на пътниците, екипажите, персонала, обществеността, въздухоплавателните средства и критичната инфраструктура на летището от актове на незаконна намеса.

II. От традиция към иновация

2.1. *Предпоставки*

В началото на своята работа „СОФ Кънект“ наследява структура на управление, в която дирекция „Сигурност“ е най-голямата организационна единица, функционираща в среда на ниска ефективност, силно повлияна от кризата, породена от COVID-19 и критични констатации след про-

верка от Европейската комисия. Тази комбинация от фактори с негативно въздействие провокира вземането на неотложни мерки, базирани на задълбочен анализ и категорично дефинирана необходимост от устойчива промяна, насочена към повишаване на качеството на изпълнение, компетентността на служителите, културата на сигурност и организационната ефективност, т.е. – необходима е трансформация, а не промяна. На фигура 1 е илюстрирана разликата между трансформацията и промяната, както и техните ключови характеристики, представени от Хуан Рамон Матас Себастия, главен оперативен директор на „СОФ Кънект“, в рамките на среща с дирекция „Сигурност“ през февруари 2024 г.



Фигура 1. Трансформация с/у промяна

Идентифицираните слабости в съществуващия традиционен модел на управление показват, че дирекция „Сигурност“ не може да продължава да функционира ефективно в новата реалност:

– липсва взаимозаменяемост на функциите между отделите, извършващи проверки по сигурността, което е показател за ограничена гъвкавост;

– част от функциите с критично значение за ефективното изпълнение на операциите по сигурността, като разработване на политики, процеси и процедури, както и планирането на ресурсите, са разпръснати между отделите и това води до слаба координация, ниска оперативна гъвкавост и слабости при прилагането на *системния подход* в управлението на сигурността.

Принцип на системния подход не е оптимизирането на отделни елементи, а изграждането на интегрирано цяло чрез еднопосочност на действията и обединяване на усилията в организацията, което води до повишаване на общия резултат. Целта е отделните, но взаимносвързани звена да се структурират и организират по начин, който да осигури обща ефективност, която е по-голяма от сумата от тези на отделните звена, т.е. организацията да се отличава с висока степен на синергия. (Panov & Panova 2005). На фигура 2 е показан традиционният модел на управление на дирекция „Сигурност“ преди трансформацията.



Фигура 2. Традиционен модел на управление на дирекция „Сигурност“

На базата на извършен анализ и идентифициране на първопричините, висшият мениджмънт на компанията инициира фундаментална трансформация с прилагане на иновативен подход за организация и управление на сигурността, насочен към повишаване на ефективността, подобряване на координацията между дейности и отговорности, засилване на взаимодействието между отделните структурни звена, развитие на човешкия ресурс и утвърждаване на висока култура на сигурност.

Новият подход е насочен към цялостна трансформация и устойчиви резултати в условия на *нова реалност*. Това се постига чрез прилагане на *системен подход* за преминаване от традиционния модел на управление към модел, основан на екипност, отговорност и постигане на измерими резултати чрез установяване на ключови показатели за ефективност.

2.2. *Реализация на проекта*

Висшият мениджмънт на „СОФ Кънект“ съвместно с екипи на дирекции „Човешки ресурси“, „Сигурност“ и водещи международни експерти разработва проект за трансформация с обща продължителност от 24 месеца. Основният фокус е върху елиминирането на слабости в системата на сигурността посредством работа по няколко ключови аспекта:

– развитие, обучение, непрекъснато усъвършенстване и надграждане на компетенциите на служителите по сигурността;

– оптимизация на организационната структура на дирекция „Сигурност“, въвеждане на нови структурни звена, роли и отговорности;

– лидерство, мотивация и подкрепа; повишаване на културата на сигурност посредством продължаващо обучение и комуникация.

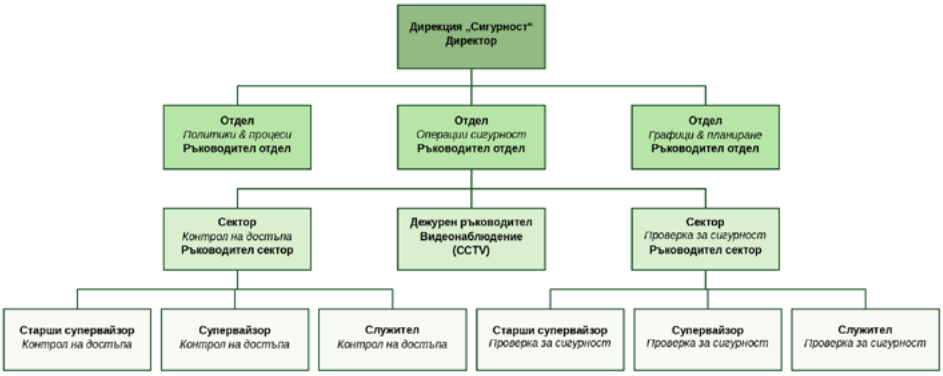
2.2.1. *Развитие, обучение, непрекъснато усъвършенстване и надграждане компетенциите на служителите по сигурността*

Ключов елемент във всяка ефективно работеща система е човешкият ресурс и неговото ниво на компетентност. Всяко отклонение от изискуемите нива на знания и умения води до слаби звена в системата и потенциална възможност за грешки при изпълнение на задачите.

Като се вземат предвид констатираните слабости от проведения външен мониторинг и негативното въздействие от пандемията COVID-19, ръководството на „СОФ Кънект“ предприема мерки за недопускане на задълбочаване на проблема с човешкия фактор. Извършва се организация за провеждане на фокусирано специализирано обучение на всички служители от дирекция „Сигурност“, работещи с рентгеново оборудване за проверка на лица и багажи. Целта е опресняване и надграждане на знанията и уменията на служителите и гарантиране на тяхното устойчиво поддържане. Установяват се ключови показатели за ефективност и целеви нива, които всеки служител следва да постигне, като изпълнението им се оценява чрез тестване на индивидуалните способности. Напредъкът се наблюдава и контролира чрез система за измерване на резултатите. В продължение на 12 месеца екипи от международни консултанти инвестират средно 144 учебни часа в обучение и тестване на всеки служител по сигурността, работещ с рентгеново оборудване. Крайните резултати показват достигнато ниво на компетентност на служителите, съответстващо на изискванията, доказано с мониторингов доклад на Европейската комисия.

2.2.2. *Оптимизация на организационната структура на дирекция „Сигурност“, въвеждане на нови структурни звена, роли и отговорности*

Действията в този етап на проекта за трансформация се планират след задълбочен анализ и на базата на сериозен международен опит. Компанията предприема фундаментален редизайн на структурата, ролите и отговорностите в дирекция „Сигурност“. Новата структура е с по-малък брой йерархични нива и позволява лесно движение в и между тях (фигура 3).



Фигура 3. Оптимизирана структура и роли в дирекция „Сигурност“

От съществуващите в старата структура седем отдела се обособява един оперативен отдел с две направления – контрол на достъпа и проверка за сигурност. Иновативен е подходът за създаването в оперативната част на роли, които могат да бъдат изпълнявани за определен период (*дежурен ръководител, старши супервайзор).* Заемането им пряко зависи от представянето и мотивацията на служителя.

Нов подход спрямо традиционната структура е създаването на направления „Политики и процеси“ и „Графици и планиране“. Те са позиционирани извън оперативната дейност и в тях работят служители с експертиза в разработването и поддържането на програми, процедури, оценки на риска, планиране на служители, работни графици, проследяване на наличие и валидност на обучения и сертификати за компетентност на оперативните служители.

По този начин се постига централизиране на ролите и отговорностите при изпълнение на задачи, които са изцяло експертни, но с ключово значение за ефективността на операциите по сигурността. Този нов подход гарантира, че служителите по сигурността остават изцяло фокусирани върху своите оперативни задължения и нивото на тяхното изпълнение, без

да инвестират време и внимание в задачи, които са извън обхвата на отговорностите им.

Постигнатият ефект от цялостния нов модел на роли и отговорности е максимална оперативна гъвкавост и взаимозаменяемост, основана на придобити нови компетенции, способност за изпълнение на различни задачи и възможности за развитие.

2.2.3. *Лидерство, мотивация, подкрепа и повишаване културата на сигурност*

Процесите, свързани с новия подход в организацията и управлението на сигурността, могат да функционират ефективно единствено при изградена и установена култура на сигурност. Тя се определя от ценностите, нагласите и поведението, които всеки служител демонстрира по отношение на целите по сигурността, определени от политиката за сигурност на компанията. Възможността за повишаване на компетентностите на персонала посредством обучения, образование, комуникация и обмен на информация, води до среда на споделени разбирания и поведение, съответстващо на целите на организацията, при изпълнение на задачите по сигурността[1].

Като се основава на принципите за позитивна култура на сигурност, „СОФ Кънект“ организира за периода на проекта провеждането от международни експерти на поредица от сесии за лидерство, мотивация и култура на сигурност с продължителност и обхват, съответстващи на ролите и отговорностите, които всяка целева група изпълнява. Практически всички служители в дирекция „Сигурност“, от ръководител до оперативен служител, преминават комплекс от обучения, състоящи се от практически занимания, дискусии и ситуационни ролеви игри.

2.3. *Внедряване на новия модел*

Подготовка за внедряване. Този етап изисква изготвяне на съвместен план за действие с участието на всички заинтересовани страни. Специално създадени екипи от ръководители от дирекция „Сигурност“ и експерти от „Човешки ресурси“ преминават обучение относно предстоящата комуникационна кампания със служителите. Основната задача на всеки от екипите е да обясни по достъпен начин промените и предимствата на новата организационна структура и да получи обратна връзка, която да послужи за подобрение.

Комуникационна кампания. От ключово значение за успеха на проекта е провеждането на нарочна среща с цялата дирекция „Сигурност“

за представяне на новата организационна структура, роли и отговорности. Като следваща необходима стъпка екипите провеждат последователни индивидуални срещи с всеки служител, за да гарантират задълбочено разбиране на промените, да отговорят на възникналите въпроси и да насърчат активното участие в процеса на трансформация.

Финален етап. Проектът за трансформация завършва с въвеждане в пълна оперативна функционалност на новия модел на организация и управление на дирекция „Сигурност“ от 01.03.2025 г.

III. Бизнес и организационна ефективност на проекта

Проектът за трансформация на дирекция „Сигурност“ се отличава със своята уникалност и иновативност поради няколко фактора – създава условия за прилагане на *системен подход* към управлението на сигурността, като осигурява *структуриран процес* на управление, *интегриран* в общата система за управление и представляващ *неразделна част от бизнес процесите* на организацията. Чрез *холистичния подход* се постига координиране на дейности, отговорности, процеси, процедури и ресурси в условия на развита култура на сигурност.

Ефектът е видим и измерим:

– *изграден капацитет* – постигане на съответствие с регулаторните изисквания при изпълнението на задачите по сигурността и доказано чрез външен мониторинг високо ниво на успеваемост;

– проектът се реализира при *непрекъсваемост на операциите, прозрачност, комуникация и адаптиране* с цел постигане на развитие и модернизация чрез прилагане на най-добрите практики и високи стандарти в услугите и обслужването;

– *повишена ефективност* – през 2025 г. успешно са обслужени над 1 милион повече пътници спрямо началния период на концесията;

– проектът е *част от цялостната трансформация на летището* за постигане на всеобхватна оперативна, културна и дигитална трансформация;

– висшият мениджмънт, дирекция „Сигурност“ и дирекция „Човешки ресурси“ са стратегически партньори в разработването и прилагането на *холистичен подход за изграждането на високоефективна екипна култур*а;

– консолидираните длъжности и новите роли в рамките на една и съща длъжност позволяват *развитие на хората по иновативен начин*;

– участието на международни експерти позволява *надграждане на знанията и експертизата и споделяне на добри практики.*

IV. Заключение

Проектът се отличава като знакова трансформация в Република България, а постигнатите резултати са признати чрез присъждането на престижни национални и международни награди на Летище „Васил Левски“ – София. „СОФ Кънект“ – операторът на летище София е големият победител в категорията „Най-добър HR проект на голяма компания“ на Годишните HR награди на Българската асоциация за управление на хора за 2025 г. Отличието бе връчено на официална церемония на 16 април 2026 г. в София.

Летище „Васил Левски“ – София е отличено с наградата HR Excellence Award 2026 на специална церемония по време на годишния конгрес на Европейския съвет на летищата ACI EUROPE в Прага на 24 юни 2026 г. Това е едно от най-престижните отличия в европейската авиационна индустрия и се присъжда на летища, които демонстрират изключителни постижения в развитието на човешкия капитал, организационната култура и подготовката на екипите за предизвикателствата на бъдещето.

Тези награди потвърждават успеха на трансформацията и предоставят признание за стратегическата визия на „СОФ Кънект“ и иновативния подход към управлението.

Благодарности. Тази статия включва елементи от описанието на кандидатурата на „СОФ Кънект“ за Годишните HR награди на Българската асоциация за управление на хора за 2025 г.

Представянето на статията на Годишната научна конференция на Военна академия „Г. С. Раковски“ през 2026 г. се реализира с подкрепата на г-н Хуан Рамон Матас Себастия, главен оперативен директор, и г-жа Анелия Димова, главен директор „Човешки ресурси“ в „СОФ Кънект“ ЕАД.

БЕЛЕЖКИ

1. ICAO, 2013. *Safety Management Manual (SMM). Doc 9859*, Chapter 5, Third Edition.

ЛИТЕРАТУРА

ПАНОВ, Т.; М. ПАНОВА, 2005. *Теория на организацията.* София. ISBN 954-90993-6-9.

REFERENCES

PANOV, T.; PANOVA, M., 2005. *Teoria na organizatsiyata*. Sofia. ISBN 954-90993-6-9. [in Bulgarian].

Acknowledments. This paper incorporates elements from SOF Connect's submission for the 2025 Annual HR Awards of the Bulgarian Association for People Management. The presentation of this paper at the 2026 Annual Scientific Conference of the G. S. Rakovski Military Academy was made possible through the support of Mr Juan Ramon Matas Sebastia, Chief Operating and Services Officer, and Ms Anelia Dimova, Chief Human Resources Officer, of SOF Connect EAD.

A NEW MODEL FOR AVIATION SECURITY ORGANISATION AND MANAGEMENT AT VASIL LEVSKI SOFIA AIRPORT: FROM TRADITION TO INNOVATION

Abstract. Ensuring the security and protection of passengers, crew members, staff, the public, aircraft, and airport infrastructure against acts of unlawful interference is a strategic priority and a core responsibility of the airport operator SOF Connect. To maintain a consistently high level of security, operational performance, and business continuity, the company's senior management initiated an innovative approach to transforming the organization and management of security, aimed at enhancing efficiency, developing human resources, and strengthening the security culture. The transformation was achieved through a shift from a traditional management model to one based on teamwork, accountability, and the achievement of measurable results. The new approach to security management was designed and implemented as an integral part of the company's broader operational, cultural, and digital transformation, with a focus on enhancing the passenger experience, improving efficiency, and positioning Vasil Levski Sofia Airport as a modern five-star regional hub.

Keywords: airport; transformation; aviation security; innovative approach; efficiency; security culture

Dr. Albena Popova
Security Executive Advisor
Sofia Airport – SOF Connect EAD
Sofia, Bulgaria
E-mail: popova@sof-connect.com
albenaipopova@gmail.com

https://doi.org/10. 66334/annu26_managsimul

МЕНИДЖМЪНТ НА СИСТЕМИТЕ ЗА СИМУЛИРАНЕ И МОДЕЛИРАНЕ В БЪЛГАРСКАТА ВОЕННООБРАЗОВАТЕЛНА СИСТЕМА

майор Анатоли Палев
Военна академия „Георги Стойков Раковски“

Абстракт. В контекста на динамично променящата се глобална среда за сигурност системите за моделиране и симулации се утвърждават като критичен инструмент за повишаване на стратегическата и оперативната готовност на въоръжените сили. Ранното възприемане и ефективното внедряване на тези технологии предоставят значителни предимства, докато забавянето може да доведе до сериозни последици за военните способности. Докладът разглежда управлението на системите за моделиране и симулации (M&C) в ключови български военни образователни институции. Изследването използва документален анализ, сравнителен подход и авторски модел за оценка на зрелостта на M&C средата, допълнен от матрица „предизвикателство – решение“. Идентифицирани са основните предизвикателства: технологично остаряване, фрагментация на системите, ограничения в данните и човешкия капитал, необходимост от стандартизация и киберсигурност. Формулирани са препоръки за национална стратегия, приоритизиране на инвестициите и развитие на човешкия капитал.

Ключови думи: военнообразователна система; мениджмънт; системи за симулиране и моделиране

I. Увод

В съвременната динамична и сложна среда на сигурност, която се характеризира с хибридни заплахи и бърз технологичен напредък, системите за моделиране и симулации се утвърждават като критичен инструмент за повишаване на отбранителните способности на въоръжените сили (ВС) на Република България. Приоритетите са в съответствие с рамката, заложена в Актуализираната стратегия за национална сигурност на Република България[7] и Доктрината на въоръжените сили на Република България[8]. Те представляват съвкупност от методи, процеси и технологии за виртуално пресъздаване на оперативната среда, които позволяват провеждането на реалистична подготовка, анализ на тактически варианти и развитие на нови способности при значително намаляване на риска и разходите.

Управлението на тези системи в рамките на българската военнообразователна система е от ключово значение за подготовката на следващото поколение офицери и команден състав. Целта на настоящата статия е да извърши цялостен анализ на системата за управление (мениджмънт) на системите за моделиране и симулации в българските военни учебни заведения, като се базира на преглед на ключови национални стратегически документи, концепции, планове и нормативни актове (фигура 1).



Фигура 1. Моделирането и симулациите заемат централно място в процеса на трансформация и са свързани с всички останали аспекти – от планирането и придобиването на техника, до обучението и реалните операции

II. Глобални тенденции и технологичен напредък в моделирането и симулациите

В глобален план системите за моделиране и симулации се развиват с безпрецедентна скорост, движени от напредъка в изчислителната мощ, изкуствения интелект (ИИ) и технологиите за виртуална и добавена реалност (*VR/AR*). Водещите армии в света инвестират масирано в следните направления:

• Изкуствен интелект и машинно обучение: ИИ се използва за създаване на адаптивни и интелигентни виртуални опоненти, които могат да предизвикат обучаемите по непредсказуеми начини. Алгоритмите за машинно обучение анализират огромни масиви от данни от симулации, за да идентифицират оптимални тактики и да прогнозират изхода от различни сценарии.

• Виртуална и добавена реалност (*VR/AR*): Тези технологии осигуряват потапящи и силно реалистични тренировъчни среди. VR се използва за пълно потапяне в симулирана среда, докато AR наслагва цифрова информация върху реалния свят, подпомагайки поддръжката на техниката и тактическата подготовка.

• Цифрови близнаци (*Digital Twins*): Създаването на детайлни виртуални копия на реални оръжейни системи, терени и инфраструктура позволява провеждането на тестове, прогнозна поддръжка и планиране на мисии с изключителна точност.

• Облачни и крайни изчисления (*Cloud and Edge Computing*): Облачните технологии позволяват достъп до сложни симулации от всяка точка, докато крайните изчисления обработват данни директно на бойното поле, осигурявайки анализи в реално време.

• Модулен отворен системен подход (*MOSA*): Тази архитектура позволява бърза интеграция на нови технологии и компоненти от различни производители, предотвратявайки зависимостта от един доставчик и улеснявайки модернизацията.

Тези тенденции променят фундаментално начина, по който се провежда обучение, планиране и вземане на решения в отбраната.

III. Приложение и управление на моделиране и симулации в българската военнообразователна система

3.1. Нормативна рамка

Управлението и развитието на системите за моделиране и симулации се регламентират от многослойна рамка от документи (фигура 2).



Фигура 2. Документален модел на управлението на системите за моделиране и симулации

Националната отбранителна стратегия[9], приета с Решение № 131 на Министерския съвет от 6 март 2025 г. и с хоризонт на действие 10 години, отменя предходната стратегия и поставя като приоритет изграждането на модерни и технологично напреднали въоръжени сили. Сред приоритетните области за развитие на комуникационно-информационната система на въоръжените сили стратегията изрично посочва внедряването на „системи за подпомагане вземането на решения, моделиране и симулации“ като част от процеса на цифрова трансформация в отбраната, което придава пряка стратегическа легитимност на управлението на системите за M&C в обхвата на настоящата статия.

На по-високо йерархично ниво нормативната рамка се допълва от Актуализираната стратегия за национална сигурност на Република България[10], приета от Народното събрание на 14 март 2018 г.[11], която извежда сред другите важни национални интереси развитието и гарантирането на сигурно киберпространство, а сред приоритетите на отбранителната политика – модернизацията на въоръжените сили и координираното придобиване на ново въоръжение, техника и комуникационно-информационни системи, в която рамка логично се вписва и управлението на системите за M&C.

Основополагащ документ е Концепцията за моделиране и симулации[12], която определя целите, ръководните принципи и приоритетните области на приложение, разработена в рамките на по-широката Концепция за технологични области, подобласти и технологии за прилагане на стратегията за изслед-

вания и технологии в сигурността и отбраната.[13] Дейността се регулира и от редица наредби, които поставят конкретни технологични изисквания, като например съхранение на електронен архив и осигуряване на мрежова сигурност.

Нормативната рамка беше актуализирана с въвеждането на ново издание на Доктрината на въоръжените сили на Република България (Издание Б), утвърдено със Заповед на министъра на отбраната № ОХ-1126 от 03.12.2025 г.[14] Документът потвърждава изрично статута на доктрината като част от военнообразователната система и нейното използване в процеса на професионална военна подготовка и обучение, което пряко подкрепя тезата на настоящата разработка за централната роля на системите за M&C в подготовката на командния състав. Новото издание въвежда киберпространството, космоса и електромагнитния спектър като самостоятелни оперативни домейни наред с традиционните суша, море и въздух, а по отношение на електромагнитните операции предвижда способности на командирите за моделиране на електромагнитната среда с цел подготовка на оперативното пространство. Тази разширена концептуална рамка засилва аргумента за необходимостта от стандартизация и киберсигурност на симулационните системи, разгледана в параграф 5.4.



Фигура 3. Структура на управление

Мениджмънтът е йерархично организиран:

• Стратегическо ниво (МО): Дирекция „Операции и подготовка“ координира и определя политиките.

• Оперативно ниво (Съвместно командване на силите – СКС): Отдел „Съвместна подготовка“ отговаря за практическото приложение в учения.

• Институционално ниво (висши военни училища): Военна академия

„Георги Стойков Раковски“ разполага с Център за компютърно-подпомагани учения и симулации (ЦКПУС); НВУ „Васил Левски“, ВВМУ „Н. Й. Вапцаров“ и ВВВУ „Георги Бенковски“ управляват собствени симулационни центрове и специализирани тренажори.

• Основен център за учения: НВУК „Чаралица“ е основният симулационен център на армията.

3.3. Технологична среда

Наличните системи са разнообразни, но с различна степен на актуалност между отделните институции. НВУК „Чаралица“, като основен симулационен център на армията, разполага с най-широк набор от платформи: конструктивна симулация *JCATS (v19.1)*, виртуална симулация *VBS2* и система за реална симулация *DITS*. Военна академия „Георги Стойков Раковски“ използва актуалната поддържана версия *JCATS v20.0*, което създава по-добри предпоставки за оперативна съвместимост при многонационална подготовка, докато НВУ „Васил Левски“ работи с по-ранната версия v12.1.

Данните за използваните версии и системи са събрани чрез информация от съответните военни образователни структури към 2026 г.

3.4. Модел за оценка на зрелостта

За целите на настоящото изследване авторът предлага четиристепенен аналитичен модел за оценка на зрелостта на M&C средата (*M&S Maturity Model*), който позволява систематично позициониране на институциите спрямо тяхната технологична и организационна готовност (Таблица 1).

Таблица 1. Модел за оценка на зрелостта на системите за M&C: нива и характеристики

Ниво	***Наименование***	***Характеристики***
1	Фрагментирана	Изолирани системи, липса на обмен на данни, остарели версии на софтуер
2	Интегрирана	Вътрешна съвместимост между собствени системи, но ограничена връзка с НАТО стандарти
3	Интероперативна	Съвместимост с актуални версии и приложими стандарти на НАТО, участие в съвместни учения
4	Адаптивна	Внедрени ИИ-базирани и облачни решения, цифрови близнаци, автоматизиран анализ на данни

Таблица 2. Индикативно позициониране на институциите (на база данните от раздел III и IV)

Институция	***Текущо ниво***	***Основна пречка за преминаване на следващо ниво***
ВА „Г. С. Раковски“ (ЦКПУС)	3	Внедряване на ИИ-базирани и автоматизирани решения (преход към Ниво 4)
НВУ „Васил Левски“	1	По-ранна версия на *JCATS (v12.1)* и ограничена съвместимост с актуалната технологична среда
НВУК „Чаралица“	3	Унификация на *JCATS* с актуалната поддържана версия и интеграция на ИИ-базирани компоненти

Оценката има индикативен характер и е извършена въз основа на наличните данни за технологична актуалност, интероперативност и интеграция на разглежданите M&C системи. Тя не представлява цялостна институционална оценка. Моделът предоставя възпроизводим инструмент, който би могъл да се прилага периодично за проследяване на напредъка на институциите.

Забележка: ВВВУ „Георги Бенковски“ и ВВМУ „Н. Й. Вапцаров“, посочени в параграф 3.2 като разполагащи със собствени симулационни центрове, не са включени в модела за оценка на зрелостта (Таблица 2) и в сравнителния анализ по институции (параграф 4.5, Таблица 3) поради липса на достатъчно данни за техните системи към момента на подготовка на статията.

IV. Предизвикателства пред моделирането и симулациите в България

Ефективният мениджмънт на системите за моделиране и симулации се сблъсква със сериозни предизвикателства.

4.1. Технологично остаряване и несъвместимост

Сред най-съществените идентифицирани проблеми е технологичното остаряване и несъвместимостта. Използваната версия на *JCATS* варира съществено между институциите – от v12.1 в НВУ „Васил Левски“, през v19.1 в НВУК „Чаралица“, до актуалната поддържана версия v20.0 във Военна академия „Георги Стойков Раковски“. Това разминаване възпрепятства пълноценната съвместна работа и участието в учения при уеднаквена технологична среда.

4.2. Фрагментация и липса на системна интеграция

Информационната среда се характеризира с наличие на частично интегрирани и в определени случаи изолирано функциониращи информационни и симулационни системи. Недостатъчната интеграция налага ръчен обмен на данни и затруднява цялостното управление на учебния процес.

4.3. Ограничения в данните и човешкия капитал

Ефективността на ИИ-базираните симулации зависи от наличието на големи и висококачествени масиви от данни, които често са ограничени. Същевременно Концепцията за развитие на изкуствения интелект в България до 2030 г.[15] идентифицира ниското ниво на цифрови умения като национално предизвикателство, което пряко засяга способността за управление на сложни технологични системи.

4.4. Ресурсно осигуряване и финансиране

Планът за развитие на въоръжените сили на Република България до 2026 г.[16] залага достигане на разходи за отбрана от 2% от БВП, но подчертава, че намаляване на разходите под този праг ще има негативно въздействие върху способностите. Тази цел вече е постигната: Националната отбранителна стратегия[17] потвърждава, че разходите за отбрана на Република България достигат 2,0% от БВП още през 2024 г., като това ниво се разглежда като минимално необходимо и основа за последващото му повишаване, а поне 20% от прогнозните разходи за отбрана следва да се насочват към придобиване на ново въоръжение и техника. Въпреки постигнатото ниво на финансиране, високите първоначални инвестиции за модернизация на симулационните системи остават сериозно предизвикателство, доколкото ресурсното осигуряване за M&C се конкурира с останалите приоритетни капиталови разходи на Министерството на отбраната. Впоследствие на срещата на върха на НАТО в Хага (2025 г.) съюзниците, включително Република България, поеха ангажимент за поетапно повишаване на разходите за отбрана до 5% от БВП до 2035 г. – не по-малко от 3,5% от БВП за основни разходи за отбрана и до 1,5% от БВП за свързани с отбраната и сигурността инвестиции. В изпълнение на този ангажимент Министерският съвет прие на 10 юни 2026 г. Национален план за повишаване на разходите за отбрана на 5% от БВП до 2035 г.[18], който съществено разширява средносрочния финансов хоризонт за модернизация, включително за системите за M&C, отвъд рамката на вече постигнатата цел от 2% от БВП.

4.5. Сравнителен анализ по институции

Таблица 3 съпоставя използваните системи и нивото на съвместимост между институциите.

Таблица 3. Сравнителен анализ по институции: използвани системи и ниво на съвместимост

Институция	***Основна платформа***	***Версия/ тип***	***Предпоставки за оперативна съвместимост***	***Основно приложение***
ВА „Г. С. Раковски“	JCATS	v20.0	Високи – актуална поддържана версия на JCATS	Щабни тренировки
НВУ „Васил Левски“	JCATS	v12.1	Ограничени – по-ранна версия	Начална щабна подготовка
НВУК „Чаралица“	J C A T S , VBS2, DITS	J C A T S v19.1	Високи – близка до актуалната версия и разнообразни системи	Командно-щабни учения, индивидуална и реална симулация

Извод от съпоставката: Разминаването във версиите на *JCATS* между отделните институции – от v12.1 в НВУ „Васил Левски“, през v19.1 в НВУК „Чаралица“, до актуалната поддържана v20.0 във Военна академия „Г. С. Раковски“, е съществен фактор за вътрешната несъвместимост. Актуалната версия създава по-добри предпоставки за оперативна съвместимост, но институционалната зрелост не следва да се определя единствено от версията на една платформа.

4.6. Липса на стандартизация и киберсигурност

Липсата на единна архитектура и общи технически стандарти между институциите (параграф 4.2) се допълва от нарастващи изисквания за киберсигурност на симулационните системи. Актуализираната стратегия за национална сигурност[19] извежда гарантирането на сигурно киберпространство сред водещите национални интереси, а новото издание на Доктрината на въоръжените сили[20] въвежда киберпространството като самостоятелен оперативен домейн. Симулационните системи като част от комуникационно-информационната среда на въоръжените сили попадат в обхвата на тези изисквания, което налага прилагането на модулен отворен системен подход (*MOSA*) и укрепване на процесите по верификация, валидация и акредитация (*VV&A*), разгледани в параграф 5.4.

V. Препоръки и стратегически насоки за развитие

За да се преодолеят предизвикателствата и да се реализира пълният потенциал на системите за моделиране и симулации, са необходими координирани и целенасочени действия.

5.1. Разработване на цялостна национална стратегия

Необходимо е да се разработи единна стратегия, която да интегрира усилията на всички родове войски и образователни институции под обща архитектура. Тази стратегия трябва да дефинира ясни приоритети, пътни карти за модернизация и механизми за координация, надграждайки съществуващата Концепция за Моделиране и Симулации.[21]

5.2. Приоритетни инвестиции в напредничави технологии

Инвестициите трябва да бъдат насочени към технологиите на бъдещето:

- Изкуствен интелект: за създаване на адаптивни симулации и подпомагане на вземането на решения.
- VR/AR: за потапящи и реалистични тренировъчни среди.
- Цифрови близнаци: за прецизно планиране и поддръжка.
- Облачна инфраструктура: за гъвкавост, достъпност и сигурност, както е предвидено в стратегическите документи.

5.3. Развитие на човешкия капитал

Важно е да се инвестира в развитието на човешкия капитал чрез целенасочени програми за обучение и квалификация на оператори, анализатори и системни администратори. Необходимо е насърчаване на сътрудничеството между академичните среди, индустрията и военните за създаване на устойчива експертна общност.

5.4. Стандартизация и сигурност

Приемането на модулен отворен системен подход (*MOSA*) ще осигури гъвкавост и ще улесни бъдещите модернизации. Процесите по верификация, валидация и акредитация (*VV&A*) трябва да бъдат укрепени, за да се гарантира надеждността и достоверността на симулационните системи.

5.5. Матрица предизвикателство – решение

Обвързването на идентифицираните предизвикателства (раздел IV) с конкретните препоръки (раздел V) в рамките на единна матрица позволява проследяване на изпълнението и отговорностите (Таблица 4).

Таблица 4. Матрица предизвикателство – решение

Предизвикателство (р. IV)	***Препоръка (р. V)***	***Отговорна институция***	***Времева рамка***	***Индикатор за успех***
Технологично остаряване (4.1)	Унификация на версията на JCATS	МО/Дирекция „Операции и подготовка“	Краткосрочно (до 2 г.)	Всички институции на v20.0
Фрагментация (4.2)	Национална стратегия за M&C	МО, СКС, ВВУ	Средносрочно (2 – 4 г.)	Приета единна стратегия за M&C, надграждаща концепцията от 2016 г.
Ограничения в данните и кадрите (4.3)	Развитие на човешки капитал	ВВУ, академични партньори, НВУК „Чаралица“	Средносрочно (2 – 4 г.)	Брой обучени специалисти/година
Ресурсно осигуряване (4.4)	Приоритизация на инвестициите	МО, бюджетно планиране	Дългосрочно (4 – 6 г.)	Дял на изпълнените спрямо планираните инвестиционни проекти за M&C за съответния период
Липса на стандартизация (4.6)	MOSA + VV&A процеси	СКС, ВВУ	Средносрочно (2 – 4 г.)	Брой сертифицирани по VV&A системи

VI. Заключение

Мениджмънтът на системите за моделиране и симулации е важен компонент от усилията за модернизация на българската военнообразователна система. Налице е ясна визия за тяхното развитие, подкрепена от национални стратегии и концепции. Успешното внедряване на съвременни симулационни технологии е демонстрирано в редица национални и международни учения, особено в институции като ВА „Георги Стойков Раковски“, както и при провеждането на командно-щабни обучения и разнородна симулационна подготовка чрез НВУК „Чаралица“.

Въпреки това, за да се постигне пълният потенциал на системите за моделиране и симулации и да се гарантира стратегическо предимство, е необходимо преодоляване на съществуващите предизвикателства. Фраг-

ментираният подход, високите инвестиции, ограниченията в данните и човешкия капитал, както и необходимостта от стандартизация и киберсигурност, изискват координирани и целенасочени действия.

Предложеният авторски модел за оценка на зрелостта и матрицата „предизвикателство – решение“ могат да се използват като основа за периодично измерване на развитието на M&C средата и за приоритизиране на управленските решения.

Чрез разработване на цялостна национална стратегия, приоритизиране на инвестициите и развитие на човешкия капитал България може да трансформира своята военнообразователна система, осигурявайки висококвалифициран и адаптивен команден състав, готов да посрещне предизвикателствата на бъдещето.

БЕЛЕЖКИ

1. НС, 2018. *Актуализирана стратегия за национална сигурност на Република България*. София: Народно събрание

2. МО, 2025. *Доктрина на въоръжените сили на Република България*. Издание Б. София: Министерство на отбраната

3. МО, 2025. *Национална отбранителна стратегия.* София: Министерство на отбраната

4. НС, 2018. *Актуализирана стратегия за национална сигурност на Република България*. София: Народно събрание

5. НС, 2018. *Актуализирана стратегия за национална сигурност на Република България*. София: Народно събрание

6. МО, 2016. *Концепция за моделиране и симулации във въоръжените сили на Република България.* София: Министерство на отбраната

7. МО, 2015. *Концепция за технологични области, подобласти и технологии за прилагане на „Стратегия за изследвания и технологии в сигурността и отбраната“*. София: Министерство на отбраната.

8. МО, 2025. *Доктрина на въоръжените сили на Република България*. Издание Б. София: Министерство на отбраната

9. МС, 2020. *Концепция за развитието на изкуствения интелект в България до 2030 г.* София: Министерски съвет

10. МС, 2021. *План за развитие на въоръжените сили на Република България до 2026 г.* София: Министерски съвет

11. МО, 2025. *Национална отбранителна стратегия.* София: Министерство на отбраната

12. МС, 2026. *Национален план за повишаване на разходите за отбрана на 5% от брутния вътрешен продукт на Република България до 2035 г.* София: Министерски съвет

13. НС, 2018. *Актуализирана стратегия за национална сигурност на Република България*. София: Народно събрание

14. МО, 2025. *Доктрина на въоръжените сили на Република България*. Издание Б. София: Министерство на отбраната

15. МО, 2016. *Концепция за моделиране и симулации във въоръжените сили на Република България.* София: Министерство на отбраната

MANAGEMENT OF MODELING AND SIMULATION SYSTEMS IN THE BULGARIAN MILITARY EDUCATION SYSTEM

Abstract. This report analyzes the management of Modeling and Simulation (M&S) systems in the Bulgarian military education system. In a dynamically changing global security environment, M&S systems are becoming a critical tool for enhancing the strategic and operational readiness of the armed forces. Early adoption and effective implementation provide significant advantages, while delays can seriously affect military capabilities. M&S systems are not merely a means of cost reduction, but a fundamental requirement for maintaining a competitive advantage and adapting to evolving threats. Using documentary analysis, a comparative approach, and an author-developed maturity-assessment model, the report examines current M&S applications in key Bulgarian military educational institutions. It identifies the main challenges, including technological obsolescence, system fragmentation, data and human-capital limitations, and the need for standardization and cybersecurity, and proposes an inter-institutional comparison and a challenge-solution framework, together with recommendations for a national M&S strategy, technology investment, and human-capital development.

Keywords: management; military education system; modeling and simulation systems

Major Anatoli Palev, PhD Student
ORCID iD: 0009-0002-5019-4635
Department of Distance Learning, Language Training and Qualification
Rakovski National Defence College
1504 Sofia, Bulgaria
E-mail: a.palev@rndc.bg

https://doi.org/10. 66334/annu26_allblood

ПРОДЪЛЖИТЕЛНИ ГРИЖИ ЗА ПОСТРАДАЛИ НА БОЙНОТО ПОЛЕ: ПРИЛОЖЕНИЕ НА ПРЕДВАРИТЕЛЕН ДОНОРСКИ РЕЗЕРВ ЗА ОСИГУРЯВАНЕ НА ЦЯЛА КРЪВ

лейтенант д-р Антония Пушкарова
Военномедицинска академия – София
Военна академия „Георги Стойков Раковски“

Абстракт. Съвременните широкомащабни бойни действия се характеризират с висока интензивност, разсредоточено разполагане на формированията и ограничени възможности за наземен и авиационен санитарен транспорт. Тези особености на оперативната обстановка могат значително да забавят извеждането на пострадалите и достъпа до своевременна медицинска помощ. Концепцията за „Продължителни грижи за пострадали на бойното поле“ позволява поддържане на жизнените функции на мястото на нараняването до възстановяване на условията за евакуация. Ефективността на този подход зависи от наличието на медицински ресурси за продължителен период. При тежка кръвозагуба особено значение придобива способността за хемотрансфузия (кръвопреливане). Използването на цяла кръв може да бъде необходимо преди достигане до военномедицинско полево лечебно заведение. Интегрирането на донорски резерв създава възможност за извършване на трансфузия в непосредствена близост до мястото на нараняване чрез предварителен подбор и медицински скрининг на доброволни кръводарители. Целта на настоящата раз-

работка е да анализира възможностите за прилагане на този подход като допълваща способност в системата за медицинско осигуряване на въоръжените сили на Република България.

Ключови думи: бойни действия; продължителни медицински грижи за пострадали; медицинска евакуация; цяла кръв; донорски резерв; масивна кръвозагуба

Въведение

Съвременните широкомащабни бойни действия поставят нови изисквания към организацията на медицинското осигуряване и налагат преоценка на съществуващите военномедицински доктрини и подходи за планиране. Провеждането на операции в сухопътния, въздушния, морския, кибернетичния и космическия домейн създава сложна и динамична среда, в която медицинското осигуряване трябва да функционира при едновременно въздействие на множество фактори и ограничения.

Сред основните предизвикателства е осигуряването на своевременна медицинска евакуация. Ограниченият достъп до въздушни коридори, разрушаването на пътната инфраструктура и заплахата за транспортните средства могат да затруднят или временно да възпрепятстват специализираната медицинска евакуация (MEDEVAC) и евакуацията на пострадали с неспециализирани транспортни средства (CASEVAC).

Тези условия поставят под изпитание традиционната концепция за т.нар. „Златен час“, основана на необходимостта пострадалият да достигне своевременно до хирургична помощ. Когато евакуацията е забавена или временно невъзможна, животоспасяващите интервенции и последващото лечение трябва да бъдат осигурени на мястото на инцидента или в непосредствена близост до него. Отлагането на медицинските действия може да влоши състоянието на пострадалия, да намали възможностите за пълно възстановяване и да забави връщането на личния състав в строя (Gurney et al. 2025).

В отговор на тези ограничения се развива концепцията за „Продължителни грижи за пострадали на бойното поле (*Prolonged Casualty Care – PCC*). Тя обхваща поддържане на жизнените функции, извършване на животоспасяващи интервенции и продължаване на лечението за период, надхвърлящ обичайния капацитет на доболничната медицинска помощ, когато евакуацията е временно невъзможна. По този начин PCC разширява възможностите за стабилизация на пострадалия при ограничени ресурси и

в неблагоприятна среда (*austere environments*). Това превръща концепцията във важен елемент от медицинската устойчивост на формированията.

Материали и методи

Извършен е обзор на научни публикации, специализирана военномедицинска литература, нормативни документи и други достъпни онлайн информационни ресурси на български и английски език. Подборът на източниците е осъществен чрез търсене, анализ и оценка на тяхната тематична релевантност, достоверност и приложимост в системата за военномедицинско осигуряване. Разгледани са материали, публикувани в периода 2003 – 2026 г., посветени на продължителните грижи за пострадали на бойното поле, преливане на цяла кръв в доболнични и бойни условия, концепция за донорски резерв. Обобщени са наличните данни относно приложимостта и потенциалните ползи и ограничения на този подход при забавена евакуация. Въз основа на тях са формулирани предложения за прилагане на концепцията във въоръжените сили на Република България. Изключени са източници без пряка връзка с темата или с недостатъчна информация за оценка на съдържанието.

Масивният кръвоизлив като основен фактор за предотвратима смъртност и ролята на ранната хемотрансфузия в РСС

В анализ на бойната смъртност в Ирак и Афганистан кръвозагубата и последващите от нея патофизиологични промени са водещ механизъм при 90,9% (Eastridge et al. 2012) от потенциално предотвратимите смъртни случаи. Тази критична загуба на кръв бързо задвижва каскада от усложнения, известна във военната медицина като „летална триада“ – хипотермия (понижаване на телесната температура), ацидоза (патологично понижаване на pH на кръвта) и коагулопатия (нарушение в кръвосъсирването). В съвременната бойна травматология тази концепция се актуализира до „диамант на смъртта“ чрез добавянето на четвърти фактор – хипокалциемия (понижаване на нивата на йонизирания калций в кръвта, което допълнително нарушава коагулацията и повлиява неблагоприятно сърдечно-съдовата функция).

При условия на значително забавена медицинска евакуация, водеща роля има провеждането на ранна хемотрансфузия. Поради усложнената оперативна обстановка това трябва да се осъществява максимално близо до точката на нараняване (Daniel et al. 2025) или в пункта за събиране на ранени и пострадали (Far-Forward Hemotransfusion).

Възстановяването на изгубения кръвен обем, кислородопренасящия и коагулационния капацитет на кръвта са основен компонент в поддържането на жизнените функции до осигуряване на възможност за извеждане и хирургично лечение. Ето защо настоящата разработка се съсредоточава върху осигуряването и прилагането на цяла кръв като фундаментален компонент от концепцията за РСС.

Физиологични и логистични предимства на цялата кръв

В цивилната болнична трансфузионна медицина се прилага фракциониране (разделяне) на дарената цяла кръв на отделни кръвни компоненти (Basu 2014), включително:

● **Еритроцитен концентрат.** отделените червени кръвни клетки (еритроцити) от една единица цяла кръв. Осигурява транспорта на кислород към тъканите и въглероден диоксид от тъканите към белите дробове за елиминирането му. Съхранява се при температура +2 до +6° С, за срок от 42 дни. Преди трансфузия е необходимо предварително затопляне.

● **Прясно замразена плазма.** Течната съставка на кръвта, в която са диспергирани формените елементи. Съдържа фактори на кръвосъсирването и други протеини, които заедно с тромбоцитите са отговорни за спиране на кървенето. Замразява се до осмия час от получаването (оттам и наименованието „прясно замразена“), съхранява се при температура под –30° С, за срок до една година. Преди приложение изисква технически възможности за размразяване и затопляне на водна баня до +37° С.

● **Тромбоцитен концентрат.** Тромбоцитите са клетъчни фрагменти, които имат основна роля в кръвосъсирването и заздравяването на раните. Съхраняват се при температура от +20 до +24° С при непрекъснато разклащане в специални агитатори (тромбомиксери) и имат срок на годност едва 5 – 7 дни.

Докато в болнични условия този подход оползотворява максимално дарената кръв според нуждите на пациентите, прилагането му на бойното поле при логистични затруднения е сериозно предизвикателство. По тази причина цялата кръв е по-оптимално решение в полевата военна медицина (Shackelford et al. 2021). Тя представлява нефракциониран биопродукт – прилаган във вида, в който се получава при кръвовземането, без да преминава лабораторно разделяне.

В сравнение с поддържането на резерв от традиционните кръвни компоненти цялата кръв осигурява всички клетъчни и плазмени елементи

в една единица (Gurney et al. 2022). По този начин се доставят необходимите съставки, които подпомагат преодоляването на „диаманта на смъртта“. Това се постига при преливане на значително по-малък обем и предпазва ранения от допълнително разреждане на кръвта и последващи усложнения.

Вместо поддържането на сложна и уязвима студена верига за съхранение, съвместима (АВО системата и резус-фактор) или нискотитърна цяла кръв от кръвна група О (Low-Titer Group O Whole Blood – LTOWB) се използва като предпочитан продукт в съвременната полева военна медицина. LTOWB изисква управлението единствено на една температура за съхранение (+2 до +6°C) със срок на годност 21 – 35 дни (Braathen 2025), а при използването на прясна цяла кръв (Warm fresh whole blood – *wFWB)* от полеви донори нуждата от студена верига отпада напълно.

Предварителен донорски резерв Walking Blood Bank, Walking Blood Donors

Концепцията за предварителен донорски резерв се основава на предварително организирана, проучена и поддържана система за осигуряване на цяла кръв на предна линия. В международната литература се използват понятията:

– Walking Blood Bank – представлява система за предварително идентифициране, медицински скрининг и при необходимост – мобилизиране на донори за осигуряване на цяла кръв при липса или недостатъчност на наличните кръвни продукти;

– Walking Blood Donors – предварително подбрани и медицински проучени военнослужещи от състава на формированието, които поддържат готовност за кръводаряване при активация на протокола.

За осъществяването на концепцията се провежда скрининг още в мирно време или в периода на подготовка преди дислокация. Примерен модел за обема на изследванията е:

– **информирано съгласие**;

– **кръвногрупова принадлежност и титър на антитела –** определяне на кръвна група и RhD (резус-фактор) по системата АВО, както и Kell кръвногрупова типизация. Идентифицират се както съвместими, така и универсални донори от кръвна група О с нисък титър на анти-А и анти-В антитела;

– **скрининг за трансмисивни инфекции –** извършват се стандартни серологични тестове, както и NAT (Nucleic Acid Testing – техника за амп-

лификация на нуклеиновите киселини). NAT позволява директно откриване на вирусната РНК/ДНК на ХИВ (HIV), Хепатит В (HBV) и Хепатит С (HCV). Чрез този метод се съкращава т.нар. „прозоречен период“ (времето между евентуално заразяване на донора и откриването на вируса).;

– **количествено определяне на броя на еритроцити и тромбоцити.**

Всички данни се събират и обобщават в защитен регистър, с контролиран достъп за оторизиран медицински персонал, който е леснодостъпен при ситуация, изискваща активиране на протокола.

Критерии за активация на протокола и приложение *Критерии за активация*

Концепцията за предварителен донорски резерв е критичен механизъм, подпомагащ медицинското осигуряване в извънредни ситуации. Задействането му има пряко отношение не само към спасяването на ранените, но и към боеспособността на кръводарителите. Взимането на кръв временно понижава физическите възможности. Поради това решението за активиране на протокола следва да се взима съвместно от командира и медицинския му съветник, при ясно дефинирани критерии (Degueldre 2024). В предложения модел клинични/оперативни индикатори за активиране могат да бъдат:

● **Сложна оперативна обстановка и невъзможност за евакуация.** При сложна оперативна обстановка, изолация или интензивен противников огън медицинската евакуация може да бъде напълно блокирана или забавена (извън медицинските реанимационни стандарти). Това води до увеличаване броя на безвъзвратните загуби и намалява шансовете за възстановяване и връщане в бойните редици на по-леко пострадалите. В този контекст медицинското осигуряване възприема концепцията за РСС. В нея осигуряването на възможности за предна хемотрансфузия е основен фактор за поддържането на жизнените функции на пострадалите до освобождаване на евакуационен коридор.

● **Ситуация с голям брой пострадали (MASCAL).** Инцидентите с голям брой пострадали значително натоварват системата за медицинско осигуряване. Внезапен поток от пациенти с тежки бойно-травматични увреждания надхвърля реанимационния капацитет и изчерпва предварително заделените кръвни продукти. Донорският резерв може да бъде допълнителен източник на цяла кръв при недостатъчни запаси до справяне с кризисната ситуация.

● **Необходимост от активиране на протокол за масивна хемотрансфузия**. При тежка кръвозагуба и пациент в критично състояние (хеморагичен шок) е необходимо преливане на голямо количество кръвни продукти – масивна хемотрансфузия. Поради различията в използваните дефиниции и протоколи в настоящата разработка терминът се използва в клиничния смисъл на животозастрашаваща хеморагия, изискваща интензивна трансфузионна ресусцитация. Съхраняваните биопродукти са бързо изчерпващ се ресурс и попълването им е времеемко. Активиране на донорския резерв обезпечава медицинските екипи с достатъчно кръв до овладяване на състоянието на пострадалите и попълване на кръвните банки.

● **Логистични ограничения.** При изчерпване на стандартните запаси или когато поддържането на студена верига и традиционните биопродукти не е възможно.

Място на приложение

В класическата военномедицинска доктрина, способностите на хемотрансфузия са придадени на военномедицински полеви лечебни заведения, извършващи специализирана и високоспециализирана медицинска помощ – „Роля 2“ и „Роля 3“. С промяната на способите на водене на бойни действия се налага и обновяване на бойната травма доктрина – Tactical Combat Casualty Care (Deaton et al. 2021) и Prolonged Casualty Care.[1]

В актуализираните насоки на Департамента по отбрана на САЩ[2] и Здравната агенция на отбраната на САЩ[3] кръвните продукти и по-специално нискотитърната цяла кръв от кръвна група О, са предпочитана терапия при хеморагичен шок. Друго обновяване е свързано с изтеглянето на мероприятията по кръвопреливане максимално напред във военномедицинската верига – на мястото на нараняването, по време на евакуацията или в батальонния медицински пункт – „Роля 1“. Последващи проучвания на военномедицинските органи на САЩ потвърждават, че поддържането на капацитет за преливане на цяла кръв в „Роля 1“ или по-напред е критичен фактор за преодоляване на предотвратимата смъртност от кървене на бойното поле (Shackelford et al. 2021).

Изпълнители

В мирновременни условия хемотрансфузията е медицинска манипулация, назначавана от правоспособен лекар, който определя и вписва в медицинската документация вида, количеството и начина на прилагането на кръвните продукти[4]. На бойното поле медицинският персонал е недос-

татъчен, за да осигури извършване на всички реанимационни мероприятия при интензивни бойни действия.

Научните данни и опитът, получени от пилотната програма Ranger O Low Titer (ROLO) (Song et al. 2023) на Сухопътните войски на САЩ, демонстрират практическата приложимост на предварително организиран донорски резерв и обучени бойни санитари и бойци спасители (немедицински състав) за преливане на цяла кръв на мястото на нараняване. Това не доказва автоматично безопасното извършване на процедурата от немедицински персонал и налага независима оценка на подготовката, компетентността и нормативния статут на изпълнителите.

При недостиг на медицински персонал може да се разгледа възможността за обучение на определени категории военнослужещи за изпълнение на ограничен набор от действия, свързани с прилагането на процедурата. Следва военнослужещите да бъдат теоретично и практически обучени относно техниката на кръвовземане, кръвопреливане, както и симптомите и поведението при наличие на трансфузионна реакция (Hildreth 2025). Примерен обем на обучение:

– правила за идентификация на донора и ранения;

– техника за венепункция и боравене с полеви комплекти за взимане на кръв;

– работа с гравитационни инфузионни системи;

– разпознаване на ранните симптоми на трансфузионни реакции и прилагане на алгоритъм за поведение и лечение при появата им.

За да бъде този подход приложим във въоръжените сили на Република България, е необходимо нормативната уредба да регламентира правото на сертифицирани бойци спасители да извършват кръвопреливане:

– **автономно –** по утвърдени стандартни оперативни процедури (СОП) при липса на медицинско лице;

– **под пряко ръководство на лекар –** чрез телемедицина, когато телекомуникационните канали го позволяват.

Това оправомощаване следва да бъде обвързано с промени в нормативната уредба, преминаване на специализиран курс, издаване на сертификат за правоспособност и регулярна атестация.

Изводи

Прилагането на цяла кръв на бойното поле изисква внимателна преценка на съотношението полза/риск и познаване на предимствата

и ограниченията от страна на командира и неговия медицински съветник.

Предимства

– Осигуряване на кръв непосредствено до ранения. Ранното приложение на кръвни продукти при тежка хеморагия е свързано с по-добър изход и възможност за възстановяване на пострадалия.

– Намаляване на зависимостта от евакуация. Донорският резерв не замества медицинската евакуация, а осигурява временна допълваща способност при нейното забавяне.

– **Преодоляване на логистичните ограничения**. При непосредствено взимане и приложение на цяла кръв може да се избегне необходимостта от предварителното съхраняване на запас в студена верига.

– **Бърза активация и доставка на кръвните продукти**. Минимален прозорец от време от взимане на решение до кръвопреливане, благодарение на предварително организирания донорски резерв.

Ограничения

– Предварителна подготовка. Безопасното прилагане на концепцията изисква предварително мирновременно тестване на личния състав и създаване на защитена база данни, което изисква времево и ресурсно обезпечаване.

– Трансфузионни и инфекциозни рискове. При преливане на кръвни продукти съществува опасност от трансфузионни реакции и трансмисивни инфекции (инфекции предавани по кръвен път). С предварителния скрининг на донорите рискът за предаване на инфекции се свежда до минимум.

– Необходимост от време за обучение на персонал. За да се осъществяват безопасно и ефективно процедурите по взимането и преливането на кръв, се изисква системна теоретична и практическа подготовка. Сертифициращият се състав следва да провежда занятия в среда максимално близка до реална бойна обстановка.

– Нормативни ограничения. Действащата нормативна уредба регламентира хемотрансфузията като лекарска манипулация. Това поставя законови ограничения пред автономното извършване на процедурата от немедицински състав, както и от младшия и средния медицински персонал. Имплементирането на концепцията налага преглед на действащото законодателство и, при необходимост, създаване на специален режим за прилагане на протокола във военна среда.

– Намалена боеспособност на донорите. При даряване на една единица кръв (450 мл ± 10%) временно се повлиява физиологичното състояние на военнослужещия. Кръводаряването води до спад на циркулиращия кръвен обем и кислородопренасящия капацитет. Това води до транзиторно понижаване на физическата издръжливост и толерантност към физическо натоварване. Плазменият обем се възстановява сравнително бързо, докато възстановяването на еритроцитите и железните депа продължава в рамките на седмици. Настоящите препоръки за минимален интервал между кръводаряванията в Република България са 60 дни, а в Съединените американски щати – 56 дни. Тези биологични особености трябва добре да се познават от медицинския съветник и от командира, като последният взима крайно решение за активация на протокола, тъй като това може да повлияе боеспособността на формированието и да застраши успеха на мисията. Това поставя затруднения пред командира – да поддържа постоянен баланс между медицинска нужда и съхраняване боеспособността на подразделението.

Заключение

Прилагането на цяла кръв на мястото на нараняване чрез концепцията за „Предварителен донорски резерв“ е необходимо за овладяване на масивни кръвотечения в условия на забавена или блокирана евакуация. Макар процедурата да носи съпътстващи рискове, те могат да бъдат ограничени чрез предварителен подбор, скрининг на донорите, стандартизирани процедури и системна подготовка на състава, но не могат да бъдат напълно елиминирани.

Въпреки това животоспасяващият потенциал на цялата кръв за предотвратяване на ранната смъртност от хеморагичен шок значително превъзхожда съпътстващите рискове. Поради необходимостта от донорски резерв за спасяване на ранените следва той да се разглежда като допълваща способност в системата за военномедицинско осигуряване. Успешното внедряване на концепцията за „Предварителен донорски резерв“ във въоръжените сили на Република България би могло да се изгради на следните три основни стълба:

– **законодателни изменения –** нормативно оправомощаване на обучен медицински (среден и младши) и немедицински състав да извършва кръвопреливане във военно време или по заповед по време на мисия/операция/криза;

– **обучение и доктрина –** внедряване на стандартизирани програми за подготовка и практически занятия в условия максимално близки до реална бойна обстановка;

– **материално осигуряване –** окомплектоване на подразделенията с полеви комплекти и поддържане на актуален донорски регистър.

БЕЛЕЖКИ

1. JOINT TRAUMA SYSTEM, 2021. Prolonged Casualty Care Guidelines. *Clinical Practice Guideline,* no. 91. Available from: https://jts.health.mil/assets/docs/cpgs/Prolonged_Casualty_Care_Guidelines_21_Dec_2021_ID91.pdf. [viewed: 29.09.2026].

2. UNITED STATES DEPARTMENT OF DEFENSE, 2022. DoD Instruction 6480.04: Armed Services Blood Program. Change 1, effective 29 June 2023. Available from: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/648004p.pdf. [viewed: 29.09.2026].

3. DEFENSE HEALTH AGENCY, 2023. Damage Control Resuscitation: Quick Reference Guide for Physicians, Providers, Nurses, and Paramedics. Clinical Practice Guideline Update (JTS CPG ID: 18). Available on: https://jts.health.mil/assets/docs/damage_control/Damage_Control_Resus_Quick_Reference_Guide_Physicians_Providers_Nurses_2023.pdf. [last viewed: 29 September 2026].

4. МИНИСТЕРСТВО НА ЗДРАВЕОПАЗВАНЕТО, 2003. Закон за кръвта, кръводаряването и кръвопреливането. [Решение на Народното събрание от 06 Ноември 2003 г.] София: *Държавен вестник*, бр. 102 от 21.11.2003.

ЛИТЕРАТУРА

BASU, D. & KULKARNI, R., 2014. Overview of blood components and their preparation. *Indian Journal of Anaesthesia*, vol. 58, no 5, pp. 529 – 537. Available from: doi:10.4103/0019-5049.144647. [viewed: 29.09.2026].

BRAATHEN, H.; LUNDE, T.H.F.; STRANDENES, G. & APELSETH, T. O., 2025. Extended storage of leukoreduced whole blood for transfusion stored in CPD from 21 to 35 days to improve prehospital blood supply logistics in rural areas. *Transfusion*, vol. 65, no S1, pp. 204 – 211. Available from: doi:10.1111/trf.18170. [viewed: 29.09.2026].

DANIEL, Y.; SAILLIOL, A.; POUGET, T.; PEYREFITTE, S.; AUSSET, S. & MARTINAUD, C., 2017. Whole blood transfusion closest to the point-of-injury during French remote military operations. J*ournal of Trauma and Acute Care Surgery*, vol. 82, no 6, pp. 1138 – 1146. Available from: doi:10.1097/TA.0000000000001456. [viewed: 29.09.2026].

DEATON, T.G.; AUTEN, J.D.; BETZOLD, R.; BUTLER, F.K.Jr.; BYRNE, T.; CAP, A.P.; DONHAM, B.; DUBOSE, J.J.; FISHER, A.D.; HANCOCK, J.; JOURDAIN, V.; KNIGHT, R.M.; LITTLEJOHN, L.F.; MARTIN, M.J.; TOLAND, K. & DREW, B., 2021. Fluid Resuscitation in Tactical Combat Casualty Care; TCCC Guidelines Change 21-01. J*ournal of Special Operations Medicine*, vol. 21, no 4, pp. 126 – 137. Available from: doi:10.55460/JYLU-4OZ8. [viewed: 29.09.2026].

DEGUELDRE, J.; DESSY, E.; T'SAS, F. & DENEYS, V., 2024. A systematic review of indications when and how a military walking blood bank could bridge blood product unavailability. *Blood Transfusion,* vol. 22, no 5, pp. 395 – 404. Available on: doi:10.2450/BloodTransfus.603. [viewed: 29.09.2026].

EASTRIDGE, B. J.; MABRY, R.L.; SEGUIN, P.; CANTRELL, J.; TOPS, T.; URIBE, P.; MALLETT, O.; ZUBKO, T.; OETJEN-GERDES, L.; RASMUSSEN, T.E.; BUTLER, F.K.; KOTWAL, R.S.; HOLCOMB, J.B.; WADE, C.; CHAMPION, H.; LAWNICK, M.; MOORES, L. & BLACKBOURNE, L.H., 2012. Death on the battlefield (2001 – 2011): Implications for the future of combat casualty care. *Journal of Trauma and Acute Care Surgery*, vol. 73, no 6, pp. 431 – 437. Available from: doi:10.1097/TA.0b013e3182755dcc. [viewed: 29.09.2026].

FRESCALINE, N.; DELASSUS, F.; CHUECA, M. & LATAILLADE, J.-J., 2024. Modern military medicine: Focus on transfusion practices in forward deployed environments. *International Review of the Armed Forces Medical Services*, vol. 97, no 2 – 3, pp. 32 – 36. Available from: https://cimm-icmm.org/wp-content/uploads/2024/12/97-2-32-36.pdf. [viewed: 29.09.2026].

GURNEY, J.M.; STAUDT, A.M.; DEL JUNCO, D.J.; SHACKELFORD, S.A.; MANN-SALINAS, E.A.; CAP, A.P.; SPINELLA, P.C. & MARTIN, M.J., 2022. Whole blood at the tip of the spear: A retrospective cohort analysis of warm fresh whole blood resuscitation versus component therapy in severely injured combat casualties. *Surgery*, vol. 171, no 2, pp. 518 – 525. Available from: doi:10.1016/j.surg.2021.05.051. [viewed: 29.09.2026].

GURNEY, J.M.; TADLOCK, M.D.; FERGUSON, D.M.; CARLSON, A.N.; DONALDSON, C. & WILSON, J.A., 2025. When the Golden Hour Goes Away: Prolonged Casualty Care in LSCO – Considerations for Commanders and Decision-Makers. *Military Review,* vol. 105, no 4, pp. 126 – 137. Available from: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2025/Golden-Hour-Prolonged-Care/. [viewed: 29.09.2026].

HILDRETH, A.F.; COLE, R.; HENDERSON, J. & SHEN, C., 2025. Time Is a Tool: Evaluation of a Prolonged Casualty Care Curriculum With a Focus on Temporal Fidelity. *Military Medicine*, vol. 190, no 7 – 8, pp. 1727 – 1733. Available from: doi:10.1093/milmed/usaf017. [viewed: 29.09.2026].

SHACKELFORD, S.A.; GURNEY, J.M.; TAYLOR, A.L.; KEENAN, S.; CORLEY, J.B.; CUNNINGHAM, C.W.; DREW, B.G.; JENSEN, S.D.; KOTWAL, R.S.; MONTGOMERY, H.R.; NANCE, E.T.; REMLEY, M.A.; CAP, A.P., 2021. Joint Trauma System, Defense Committee on Trauma, and Armed Services Blood Program consensus statement on whole blood. *Transfusion*, vol. 61, no S1, pp. 333 – 335. Available from: doi:10.1111/trf.16454. [viewed: 29.09.2026].

SONG, K.; WINEBRENNER, H.; ABLE, T.; BOWEN, C.; DUNN, N.; SHEVCHIK, J., 2023. Ranger O Low Titer (ROLO): Whole Blood Transfusion for Forward Deployed Units. *Military Medicine*, vol. 188, no 7 – 8, pp. 2733 – 2737. Available from: doi:10.1093/milmed/usab473. [viewed: 29.09.2026].

VOLLER, J.; TOBIN, J.M.; CAP, A.P.; CUNNINGHAM, C.W.; DENOYER, M.; DREW, B.; JOHANNIGMAN, J.; MANN-SALINAS, E.A.; WALRATH, B.D.;

GURNEY, J.M. & SHACKELFORD, S.A., 2021. Joint Trauma System Clinical Practice Guideline (JTS CPG): Prehospital Blood Transfusion. *Journal of Special Operations Medicine*, vol. 21, no 4, pp. 11 – 21. Available from: doi:10.55460/P685-L7R7. [viewed: 29.09.2026].

PROLONGED CASUALTY CARE ON THE BATTELFIELD: APPLICATION OF A WALKING BLOOD BANK FOR WHOLE BLOOD TRANSFUSION

Abstract. Modern large-scale combat operations are characterised by high intensity, dispersed deployment of units, and limited capabilities for ground-based and air medical transport. These characteristics of the operational environment can significantly delay the evacuation of casualties and the timely access to medical care. The concept of "Prolonged casualty care – PCC" allows for the maintenance of vital functions at the site of injury until conditions for evacuation are restored. The effectiveness of this approach depends on the availability of medical resources over an extended period of time. In cases of severe blood loss, the ability to perform blood transfusions becomes particularly important. The use of whole blood may be necessary before reaching a military hospital. The integration of the concept of Walking Blood Bank makes it possible to perform transfusions on the point of injury through the preliminary selection and medical screening of volunteering blood donors. The purpose of this study is to analyse the possibilities for implementing this approach, as a complementary capability, within the medical support system of the Bulgarian Armed Forces.

Keywords: combat; prolonged casualty care; medical evacuation; whole blood; walking blood bank; blood loss

2nd Lt Dr. Antonia Pushkarova, MD
Military Medical Academy
Rakovski National Defence College
82, Evlogi i Hristo Georgievi Blvd.
Sofia, Bulgaria
E-mail: a.pushkarova@rndc.bg

https://doi.org/10. 66334/annu26_indipodana

ИНДИКАТОРЕН ПОДХОД ЗА КОЛИЧЕСТВЕН АНАЛИЗ И ОЦЕНКА НА РЕЗУЛТАТИТЕ ОТ ОБУЧЕНИЕТО ВЪВ ВИСШЕТО ВОЕННО ОБРАЗОВАНИЕ

доц. д-р Боти Видолов
Софийски университет „Св. Климент Охридски“

Абстракт. Докладът представя методологическа рамка за количествен анализ и оценка на резултатите от обучението във висшето образование, приложима към професионално ориентирани програми в сферата на сигурността и отбраната. Обучението е разгледано като системен процес, включващ входни характеристики, образователен процес и изходни резултати. Предлага се интегрирана система от показатели, обхващаща академична успеваемост, структурна сложност, стабилност на резултатите и компетентностен баланс, както и интегрален индекс на качеството на обучението. Разглежда се приложението на дескриптивен, корелационен и регресионен анализ за установяване на зависимости и тенденции. Формулирани са изводи и управленски препоръки за вътрешно осигуряване на качеството, оптимизиране на учебните програми и стратегическо управление.

Ключови думи: анализ на обучението; качество на висшето образование; индикаторна система; интегрален индекс; академична успеваемост; количествен анализ; образователна ефективност; управление на качеството; статистически методи; компетентностен подход

1. Въведение

В условията на нарастващи изисквания към качеството на висшето образование и необходимостта от съответствие с международни стандарти, анализът на резултатите от обучението се утвърждава като ключов инструмент за оценка и управление на образователния процес. В институции като Военна академия „Г. С. Раковски“, където подготовката е пряко свързана с професионалната реализация в сферата на сигурността и отбраната, системният анализ придобива особено значение.

Съвременните педагогически концепции разглеждат обучението като сложна система, включваща входни характеристики на обучаемите, образователен процес и изходни резултати под формата на знания, умения и компетентности. В този контекст анализът на резултатите изпълнява ролята на механизъм за обратна връзка, който позволява идентифициране на отклонения и оптимизация на системата[1].

Подходът, базиран на резултатите от обучението, поставя акцент върху степента на постигане на предварително дефинирани учебни цели. Количественият анализ позволява измерване на съответствието между планирани и реално постигнати резултати и подпомага идентифицирането на факторите, влияещи върху академичната успеваемост[2].

Необходимостта от системен анализ се обуславя от неговата диагностична, контролна, прогностична и управленска функция. Чрез измерими показатели се създават условия за обективност, сравнимост между випуски, проследяване на тенденции и вземане на информирани решения[3,4,5,6,7].

2. Теоретична и методологична рамка

Концептуални основания

Обучението като системен процес

Съвременната педагогическа теория разглежда обучението като **сложна, многофакторна система**, включваща:

- вход (входно ниво на студентите);
- процес (методи, съдържание, преподаване);
- изход (резултати, компетентности).

В този контекст анализът на резултатите изпълнява функцията на **обратна връзка**, която позволява оптимизиране на системата чрез:

- идентифициране на отклонения;
- оценка на ефективността;
- адаптация на образователните стратегии.

Подход, базиран на резултатите

Съвременните образователни модели са ориентирани към резултатите от обучението. Това предполага:

- измерване на степента на постигане на компетентности;
- оценка на съответствието между цели и резултати;
- количествено проследяване на академичната успеваемост.

Без систематичен анализ не може да се установи дали обучението реално води до формиране на заложените знания, умения и нагласи.

За професионално ориентирани специалности, включително „Сигурност и отбрана“, количественият подход има допълнителна практическа значимост, тъй като подпомага оценката на съответствието между придобитите компетентности и изискванията на професионалната среда, както и баланса между теоретична и практическа подготовка.

Критериалната рамка включва: академична успеваемост; динамика на обучението; ефективност на образователния процес; качествени показатели; реализация и приложимост; сравнителен и стратегически анализ; статистически методи.

3. Система от индикатори

За количествен анализ на резултатите от курса на обучение се предлага система от взаимосвързани индикатори, групирани в четири основни направления: академична успеваемост, структурна сложност, стабилност на резултатите и компетентностен баланс.

Обект на анализа са академичните резултати от дисциплините в рамките на учебния план. Единица на наблюдение е учебната дисциплина, а изследваната съвкупност обхваща всички дисциплини от учебния план.

Академичната успеваемост се характеризира чрез среден успех, претеглен среден успех по кредити, разпределение на оценките, процент успешно завършили, процент прекъснали/отпаднали и динамика спрямо предходни випуски. Допълнително се оценява степента на покриване на резултатите от обучението и овладяването на компетентностите.

Динамиката на обучението включва прогреса между семестрите, критичните дисциплини, рисковите точки и връзката между входното ниво и крайния резултат.

Ефективността на образователния процес се разглежда чрез съотношението преподаватели – студенти, използваните методи, студентската натовареност и адекватността на учебните планове.

Академична успеваемост.
Количествени показатели:

- Среден успех от изпити (по дисциплини и общо);
- Разпределение на оценките (слаб – отличен);
- Процент успешно завършили курса;
- Процент прекъснали/отпаднали;
- Дял на студентите с отличен успех;
- Сравнение с предходни випуски (динамичен анализ).

Степен на покриване на учебните резултати:

- Постигане на заложените резултати от обучението;
- Степен на овладяване на компетентностите (знания, умения, нагласи);
- Съответствие с квалификационната характеристика на специалността.

Динамика на обучението:

- Прогрес на студентите между семестрите;
- Анализ на критични дисциплини (с висока степен на неуспеваемост);
- Идентифициране на „рискови точки“ в учебния процес;
- Връзка между входното ниво (приемни резултати) и крайния резултат.

Ефективност на образователния процес:

- Съотношение преподаватели – студенти;
- Използвани методи на обучение (лекции, казуси, симулации и др.);
- Натовареност на студентите (кредити);
- Адекватност на учебните планове.

Във военен или специализиран контекст може да се включат и:

- Ниво на практическа подготовка;
- Тактико-специални компетентности;
- Интердисциплинарна подготовка.

Качествени показатели:

- Анкетни проучвания сред студентите;
- Обратна връзка от преподаватели;
- Удовлетвореност от учебната среда;
- Самооценка на обучаемите.

Реализация и приложимост:

- Професионална реализация след завършване;
- Време до първа заетост;
- Съответствие между придобита квалификация и заемана длъжност;
- Оценка от работодатели.

Сравнителен и стратегически анализ:

- Сравнение с други висши училища;
- Съпоставяне с национални стандарти;
- Тенденции във времето (3 – 5-годишен период);
- SWOT анализ на курса.

Статистически методи:

- Дескриптивна статистика;
- Корелационен анализ;
- Регресионен анализ;
- Коефициент на вариация;
- Анализ на надеждност;
- Хипотезно тестване.

Във военен и специализиран контекст се включват показатели за практическа подготовка, тактико-специални компетентности и интердисциплинарна подготовка.

4. Формален апарат и интегрален индекс

Основните статистически показатели са аритметичен среден успех, претеглен среден успех по кредити, стандартно отклонение и коефициент на вариация. За обобщаване на резултатите се предлагат индекси на академична ефективност (IAE), стратегическа сложност (ISC), практическа приложимост (IPI) и балансов коефициент (BC).

$$\bar{X} = \frac{1}{n}\sum_{i=1}^{n} X_i \qquad (1)$$

където:

X_i – среден успех по дисциплина

n – брой дисциплини

Претеглен среден успех (по кредити)

$$\bar{X}_w = \frac{\sum_{i=1}^{n} X_i \cdot C_i}{\sum_{i=1}^{n} C_i} \quad (2)$$

където:

C_i – ECTS кредити

Стандартно отклонение

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(X_i - \bar{X})^2}{n}} \quad (3)$$

Коефициент на вариация

$$V = \frac{\sigma}{\bar{X}} \times 100 \quad (4)$$

Интерпретация:

- V < 10% – висока стабилност
- 10%–20% – умерена вариативност
- 20% – нестабилност

Индекс на академична ефективност (IAE)

$$IAE = \alpha \bar{X}_w + \beta(1 - V) \quad (5)$$

където:

$\alpha + \beta = 1$

Препоръчително:

$\alpha = 0.7$ (успеваемост)

$\beta = 0.3$ (стабилност)

Индекс на стратегическа сложност (ISC)

Измерва средната стойност в стратегическия блок:

$$ISC = \frac{\sum_{j=1}^{m} X_j^{(str)}}{m} \quad (6)$$

където:

m – брой стратегически дисциплини

Индекс на практическа приложимост (IPI)

$$IPI = \frac{\sum_{k=1}^{p} X_k^{(prac)}}{p} \quad (7)$$

Балансов коефициент (BC)

$$BC = \frac{ISC}{IPI} \quad (8)$$

Интерпретация:

- BC ≈ 1 → балансиран модел
- BC < 0.9 → доминира практическа насоченост
- BC > 1.1 → доминира теоретична насоченост

Интегралната индикаторна система използва четири групи показатели със следните тегла: академична успеваемост – 0,40; стабилност – 0,20; стратегическа подготовка – 0,20; практическа подготовка – 0,20. Преди агрегиране показателите се нормализират, за да се избегне влиянието на различните им мащаби.

Интегралният индекс на качеството на обучението (IIQO) позволява обективно измерване, сравнимост между випуски и проследяване на динамиката. Интерпретационната скала е: 0,85 – 1,00 – отлично качество; 0,70 – 0,84 – много добро; 0,55 – 0,69 – добро; 0,40 – 0,54 – задоволително; под 0,40 – ниско качество.

5. Статистически анализ и възможности за приложение

Разширеният аналитичен модел включва корелационен анализ за изследване на връзката между кредитната тежест и средния успех, и регре-

сионен анализ за проверка дали кредитната стойност влияе статистически значимо върху резултатите. Дескриптивната статистика, коефициентът на вариация, анализът на надеждност и хипотезното тестване допълват инструментариума.

Предложената рамка позволява количествено измерване на качеството, сравнимост между випуски, времеви анализ и използване в институционална система за вътрешно осигуряване на качеството. Моделът може да бъде разширен чрез индикатори за отпадане, работодателска оценка, анкетен индекс и многокритериален анализ.

Внедряването на индикаторната система предполага ежегодно изчисляване и мониторинг на IIQO, сравнителен анализ между програми, динамична адаптация на теглата според профила на обучението, контрол на вариативността, ранна диагностика на проблемни области и интеграция на резултатите в системите за качество. Перспективни са дигитализацията и автоматизацията на изчисленията, визуализацията чрез табла и сценарийният подход за оценка на ефекта от управленски решения.

6. Изводи и управленски препоръки

Качеството на обучението е многомерна категория и не следва да се оценява чрез един-единствен показател. Интегралният индекс позволява редуциране на сложна образователна система до измерима и сравнима форма, като същевременно съхранява нейната многоизмерност.

Стабилността на резултатите е индикатор за системна надеждност. Ниската вариативност отразява предсказуемост и устойчивост, но прекомерната хомогенност може да сигнализира за стандартизиране за сметка на диференциацията. Балансът между теоретична и практическа подготовка е критичен за формиране на пълноценни професионални компетентности.

Управленските решения следва да се основават на системното управление на взаимовръзките между показателите. Препоръчва се институционализиране на IIQO като KPI, ежегоден мониторинг, оптимизация на тегловите коефициенти, управление на баланса теория – практика, контрол на вариативността, ранна диагностика, дигитализация на анализа и развитие на преподавателския капацитет.

7. Заключение

Системният количествен анализ на резултатите от обучението представлява ключов инструмент за оценка и управление на качеството във

висшето образование. Интегрираната индикаторна система позволява обективно измерване на академичните резултати, идентифициране на проблемни области и вземане на обосновани управленски решения.

Разработеният интегрален индекс на качеството осигурява възможност за сравнимост между различни випуски, проследяване на динамиката и адаптиране на образователните политики спрямо стратегическите цели на институцията. Внедряването на методологията в системите за вътрешно осигуряване на качеството създава предпоставки за повишаване на ефективността, подобряване на управлението и устойчиво развитие на академичните програми.

Бъдещите изследвания могат да бъдат насочени към разширяване на модела чрез многокритериални методи, дигитализация на анализа и автоматизирани системи за мониторинг и прогнозиране на резултатите от обучението.

Таблица 1. Групи индикатори и теглови коефициенти

Група индикатори	***Символ***	***Тегло***
Академична успеваемост	A	0,40
Стабилност	S	0,20
Стратегическа подготовка	T	0,20
Практическа подготовка	P	0,20

Таблица 2. Интерпретационна скала на IIQO

IIQO	***Оценка***
0,85 – 1,00	Отлично качество
0,70 – 0,84	Много добро
0,55 – 0,69	Добро
0,40 – 0,54	Задоволително
< 0,40	Ниско качество

NOTES

1. COHEN, L.; MANION, L. & MORRISON, K, 2018. *Research Methods in Education*, 8th ed. London, UK: Routledge. https://doi.org/10.4324/9781315456539.

2. CRESWELL, J., 2018. *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research*, 5th ed. Boston, MA, USA: Pearson.

3. NITKO, A. & BROOKHART, S., 2013. *Educational Assessment of Student*s, 7th ed. Boston, MA, USA: Pearson.

4. MCCLAVE, J. & SINCICH, T., 2017. *Statistics*, 13th ed. Boston, MA, USA: Pearson.

5. FIELD, A., 2018. *Discovering Statistics Using IBM SPSS Statistics*. London, UK: SAGE Publications.

6. BIGGS, J. & TANG, C., 2019. *Teaching for Quality Learning at University*, 5th ed. Maidenhead, UK: McGraw-Hill Education.

7. HARVEY, L., 2019. *Quality Assurance in Higher Education: Trends in Regulation, Monitoring and Assessment*. Cham, Switzerland: Springer.

8. MILLMAN, J. & GREEN, J., 2015. *Examining Student Performance: A Guide for Teachers and Administrators*. New York, NY, USA: Teachers College Press.

9. OECD, N/A. *Education at a Glance*, [annual series]. Paris, France: OECD Publishing.

10. CEDEFOP, 2019. *Indicators for Monitoring Education and Training Systems*. Luxembourg: Publications Office of the European Union.

INDICATOR-BASED APPROACH TO QUANTITATIVE ANALYSIS AND ASSESSMENT OF LEARNING OUTCOMES IN HIGHER MILITARY EDUCATION

Abstract. The paper presents a methodological framework for the quantitative analysis and assessment of learning outcomes in higher education, applicable to professionally oriented programmes in security and defence. Education is considered as a systemic process comprising input characteristics, the educational process and output results. An integrated indicator system is proposed, covering academic performance, structural complexity, result stability and competency balance, together with an Integral Index of Education Quality (IIQO). Descriptive, correlation and regression analyses are considered for identifying relationships and trends. The paper formulates conclusions and managerial recommendations for internal quality assurance, curriculum optimisation and strategic management.

Keywords: learning outcomes analysis; higher education quality; indicator system; integral index; academic performance; quantitative analysis; educational effectiveness; quality management; statistical methods; competency-based approach

Dr. Boti Vidolov, Assoc. Prof.
ORCID iD: 0009-0009-9054-9614
Faculty of Physics
Sofia University "St. Kliment Ohridski"
5, James Bourchier Blvd.
1164 Sofia, Bulgaria
E-mail: bvvidolov@uni-sofia.bg

https://doi.org/10. 66334/annu26_problpredvsyst

ПРОБЛЕМИ НА ПРЕДВИДИМОСТТА НА СИСТЕМНИТЕ СЪСТОЯНИЯ ПРИ НЕУСТОЙЧИВИ УСЛОВИЯ НА СРЕДАТА

Валентин Василев
Висше военноморско училище „Никола Йонков Вапцаров“

Абстракт. Неопределеността в многомерното бойно пространство поражда необходимост от познаване на условията, при които дадено въздействие върху системата нарушава устойчивостта на процеса на управление. В изследването са разгледани три безкрайно близки възможни траектории, по които системата преминава от началното си състояние към своето крайно състояние. Първата обикновено е развитието „по план“, т.е. тази траектория води до желаното крайно състояние. В нея са предвидени съответни усложнения, под формата на външни смущения от околното пространство. Втората е идеалната траектория, която се реализира при благоприятно стечение на обстоятелствата. Третата траектория на състоянията е реалната, която се реализира в сложни условия на обстановката след осъществяване на управляващи въздействия в отговор на неблагоприятни външни смущения, засягащи системната структура или функционалните процеси на системата. Сложността определя закономерна фракталност на възможните траектории спрямо планираната, но крайните състояния се отличават със значителни разлики. Предвидимостта на измененията зависи от определянето на началото и скоростта на разделянето на безкрайно близките траектории на състоянията.

Ключови думи: военна система; командване и управление; многомерно бойно пространство; фракталност

Критерий за успех на управлението на военна система е достигането и поддържането на системните процеси в устойчиво желано състояние. Стремежът на сложната система към самоорганизиране естествено разчита на свързаността на системата с външната среда за използване на възможностите за удовлетворяването на вътрешната потребност от негентропия, така че да се приспособи към динамично изменящите се нелинейни състояния на средата. Затова е необходимо да се отдели необходимото внимание на логиката в изследването на поведението на система в условия на нелинейност и хаотичност в зоната на операцията. Корелацията между домейните в многомерното пространство следва да бъде отчитана като основен фактор за появата на сложност в зоната на операцията. Неопределеността в многомерното бойно пространство поражда необходимост от познаване на условията, при които дадено въздействие върху системата нарушава устойчивостта на процеса на управление.

Сложността в бойното пространство нараства в течение на времето, подхранваща ентропията на системите без достатъчно управление, адаптиращо се към неустойчивата околна среда. Сложността може да се сравни с възел, който се затяга без необходимите адекватни на условията на средата управляващи въздействия (Rescher 2019). От своя страна управляващите въздействия стават възможни и ефективни единствено чрез своевременното вземане на решения в резултат от познанието за околната среда. Така сложността става преодолима чрез помощта на системното мислене (Velichkov 2003). Системният подход позволява да се повиши нивото на познаваемост чрез организиране на бойното пространство на принципа „система от системи“.

Закономерността на еволюцията на процеса на управление зависи от закономерността на отклонение на траекторията на възможните системни състояния от желаната траектория. Желаната траектория на състоянията е именно тази, която води от началното системно състояние към желаното крайно системно състояние. Поради нелинейността на измененията в околната среда, особено при повишаване на динамиката на измененията, на практика става невъзможно управляващите въздействия да бъдат непроменени в течение на времето и да следват някаква открита закономерност (Kalinov 2017). Това е възможно, разбира се, единствено в един ограничен интервал от време, в ограничена област на многомерното бойно пространство. В общия случай организацията на системата за управление се намира във фрактална зависимост с организацията на бойното пространство, тъй като е проектираната в него и във всеки отрязък от време отразява настъп-

ващите деформации в траекторията на състоянията. Формирането на организация на дадена системата за управление от съставни системи повишава устойчивостта на протичане на процеса на управление дори в динамична нелинейна среда, когато дискретните линейни участъци стават прекалено кратки периоди от време, в които реално не може да се организира ефективен пълноценен итеративен когнитивен цикъл на Бойд „наблюдение – ориентиране – решение – действие“.

Нека да бъдат разгледани условия на многомерното бойно пространство, в които съществуват най-малко три възможни алтернативни траектории на бъдещите състояния на дадена сложна система. Траекториите представляват мислени линии, по които се извършва преминаването на системата от дадено начално състояние към разчетното крайно състояние. Така дадената условна траектория представлява своеобразен план за реорганизация на бойното пространство, или в зависимост от поставените задачи, напротив – план за запазване на устойчивостта на системите и системните процеси в разглежданото бойно пространство (Velichkov 2003). Траекториите си приличат в началото, след което се развиват фрактално, образувайки семейство от пространствени многомерни линии.

Първата траектория обикновено представлява вероятното развитие на системното състояние „по план“. Тази траектория води до планирано желано крайно състояние. При идентифицирането на тази траектория в голяма степен е предвидено реализирането на неблагоприятни въздействия, които са свързани със съответните усложнения, проявявани под формата на външни енергийни, материални или информационни смущения от околното пространство или инициирани от страна на опонента в зоната на операцията.

Втората траектория на вероятни бъдещи състояния на системата е идеалната траектория, която се реализира при благоприятно стечение на обстоятелствата. Развива се в условията на благоприятна външна среда. Липсват значителни смущения, а управляващите въздействия са достатъчни, за да бъдат компенсирани.

Третата условна траектория на състоянията е реалната, която се реализира на практика в сложни условия на обстановката след осъществяване на управляващи въздействия в отговор на неблагоприятни външни смущения, засягащи системната структура или функционалните процеси на системата. Отклоненията на тази траектория от плана започва в определен начален момент с определена скорост, когато се реализират неблагоприятни въздействия и обратно, реалният ход на състоянието се доближава към

плана, когато се упражняват управляващи въздействия с цел компенсиране на допуснатите отклонения.

Началният (нулев) вектор на разделяне $\delta(0)\delta(0)$ служи за определяне на началото на разделянето на безкрайно близките траектории на състоянията във фазовото пространство (Panchev 2001). Нека да бъде разгледана траекторията на възможните състояния, записана с помощта на аналитичната геометрия като:

$$y = x(t) + \delta(t)y = x(t) + \delta(t). \quad (1)$$

При наличие на динамични неблагоприятни въздействия и съответните управляващи въздействия се формират условия за последващо разделяне на траекториите на вероятните системни състояния. Безкрайно близката нова траектория на вероятните системни състояния аналогично ще притежава аналитичния вид (Panchev 2001):

$$y = x(t) + e^{\lambda t}\|\delta(0)\|y = x(t) + e^{\lambda t}\|\delta(0)\|. \quad (2)$$

Разделянето на траекториите на системните състояния започва в момента t = 0, в който е в сила записът за линейно приближение:

$$y = \|\delta(t)\| \approx e^{\lambda t}\|\delta(0)\|,y = \|\delta(t)\| \approx e^{\lambda t}\|\delta(0)\|, \quad (3)$$

където λ е показател на Ляпунов;

‖δ(0)‖ – начален вектор на разделяне и на практика дава представа за разликата между безкрайно близките траектории на две състояния на системата (Panchev 2001).

Оттук е видима закономерността, че скоростта, с която се раздалечава траекторията на новите вероятни състояния на системата вследствие на случайно ново въздействие, зависи от ориентацията и големината на началния вектор ‖δ(0)‖, нормиран с показателя на Ляпунов. Този показател влияе по експоненциален закон на раздалечаването на траекториите на състоянията в течение на времето. Различните стойности на показателя на Ляпунов се намира в релация с ориентацията на началния вектор на разделяне и има конкретна реализация във всяко измерение на многомерното пространство, т.е. реализациите са равни на размерността на фазовото пространство.

С други думи, това математическо описание показва, че неблагопри-

ятните въздействия и съответните управляващи въздействия, от своя страна, са обвързани независимо в кой домейн на многомерното бойно пространство протичат процесите и също така силата, посоката и мащаба на управляващите въздействия може да се оценяват чрез показателя на Ляпунов в съответствие с приложението на трифакторния модел на риска (сила на управляващото въздействие, продължителността на управляващото въздействие и очакваните мащаби на последствията от въздействията).

Освен това скоростта на раздалечаването на крайните състояния на системата при различни стойности на дихотомната двойка въздействия от вида „неблагоприятно въздействие – управляващо въздействие“ е най-вероятно да бъде различна в различни условия на средата. Казано с други думи, при различна ориентация в пространството на началния вектор на разделяне на траекториите на състоянията, е най-вероятно да се очаква съответстващ различен краен резултат от вземането на определено управленско решение. Важно тук е определянето на интервала от стойности на показател на Ляпунов λ, като в общия математически случай $\lambda \in (-\infty;+\infty)$.

Стойностите на показателя за конкретни динамични системи се ограничават от изискванията в теоретичен план към векторното поле и характеристиките на конкретното фазово пространство, които не са предмет на настоящото изследване. Като цяло определените емпирично стойности могат да бъдат използвани, за да определят три характерни състояния на съседните траектории: стабилност, неутрална стабилност и детерминиран хаос (Panchev 2001).

При стойности $\lambda < 0$ състоянието е стабилно. Траекториите на алтернативните състояния на системата при взето управленско решение или при реализиране на външно въздействие се сближават експоненциално към определено стабилно състояние или определен зададен атрактор.

При стойности $\lambda = 0$ състоянието се определя като неутрална стабилност. Траекториите на алтернативните състояния са напълно предвидими, т.е. същите са и управляеми. Подобна реализация е възможна при:

– идеални консервативни системи (при които няма реална загуба на енергия);

– пределни цикли, които представляват изолирана затворена траектория, около която няма други затворени траектории; съществуващите съседни траектории или се приближават към нея (навиват се около нея), или се отдалечават от нея (развиват се);

– квазипериодично (или сложно непериодично) движение, при което системата никога не се връща точно в първоначалното си състояние, въ-

преки че преминава безкрайно близо до него, тъй като траекторията се определя от две или повече независими една от друга честоти (например едновременно въздействие на неблагоприятно и управляващо въздействие).

При стойности на показателя $\lambda > 0$ възможните траектории на системните състояния са подчинени на закономерностите на детерминирания хаос в зависимост от нивото на бифуркация. В този случай съществуват условия за експоненциално раздалечаване на безкрайно близки траектории. Състоянието се характеризира с присъщата за сложните системи чувствителност към начални условия. В този случай времето на предвидимост е обратнопропорционално на показателя на раздалечение на алтернативните траектории.

Неопределеността в многомерното бойно пространство поражда необходимост от познаване на условията, при които дадено въздействие върху системата нарушава устойчивостта на процеса на управление. Резултатите от изследването на приложимостта на максималните стойности на показателя на Ляпунов върху устойчивостта на управлението показва, че той може да бъде използван за обобщен критерий за предвидимостта на сбъдването на определено желано крайно състояние.

Предвидимостта на достигането до дадено крайно състояние следва да се използва в интерес на оптимизирането на характеристиките на управляващите въздействия върху динамичната сложна система. Освен това, определянето на показателя на Ляпунов има още едно важно приложение – положителните стойности на максималните стойности на показателя във фазовото пространство са условие за хаотичност на динамичната система.

Намаляването на хаотичността допринася за намаляването на разделянето на трите условни линии на състоянията. При проактивното адаптиране на системата, което е изключително характерно в условията на подготовка за отбранителни действия, трябва да се търси постигане на баланс, което е възможно чрез изграждането на огледален образ на противостоящата страна в качествен и в количествен аспект. В интерес на подготовката и формирането на познание за организацията на бойното пространство същото се представя с възможно най-линейната пропорционална и закономерна подредба. Плановете може да бъдат в структуриран текст и таблици, описващи условията, формирани от дискретни състояния на оперативните фактори. По този начин в хода на генерирането на силите системата ще бъде подготвена по възможно най-добрия начин да противодейства на силите и средствата на опонента. Тук е важно да бъде обърнато внимание, че целта е реализиране на „противодействие“, а не „противопоставяне“,

защото е изключително вероятно да не е събрана достатъчно достоверна разузнавателна информация и входните данни в процеса на планиране да са грешни, а това означава – подвеждащи. Огледалният образ по естествен начин определя качеството на елементите. Напълно приложими са класическите принципи във военното дело от идеалната симетрия до пълната асиметрия. Идеалните условия за симетрия са стари колкото света. Победата се търси чрез измерване на количеството на силите.

Подходът на симетрията изисква влагането на не по-малко ресурси от тези, които е вложил опонентът, а функцията командване и управление в значителна степен е облекчена и не се изисква висока креативност. Търсенето на успеха чрез превъзходство на качеството над количеството поражда условия за класическа асиметрия. Например срещу танковото формирование се подготвя противотанково формирование, срещу подводница – противоподводна корабна група.

Така или иначе, с началото на бойните действия, състоянието на бойното пространство следва да бъде променено. В хода на взаимодействията между системите, т.е. например с началото на бойните действия, предвидимостта следва да бъде намалявана, т.е. хаотичността в бойното пространство позволява да се формират условия за асиметричност при взаимодействието на противостоящите системи. Асиметрията се търси винаги, когато няма баланс при разпределението на ресурсните потенциали.

В заключение може да бъде направен изводът, че в значителна степен влияние върху вероятните алтернативни траектории на бъдещите системни състояния оказват факторите в средата. Сложността прави изходните състояния да бъдат изключително чувствителни към промените във входните състояния, така че когато даже и да се прави едно и също планиране в щаба, но в различни условия на средата, то резултатът с много висока степен на вероятност ще бъде различен. Познанието за „околната среда“ и за присъстващите в нея съвкупност от физически обекти, заедно с възможната свързаност между обектите и процесите е критично важно за устойчивостта на процеса на управление. Понякога в условия на недостиг на информация се налага да се спекулира при вземане на решение. В този контекст може да се говори за опит да се направи информирано предположение за бъдещи състояния на сложни системи чрез анализ и оценка на сигнали от моментното състояние на средата заедно с формиралите се минали тенденции. Сложността в околната среда и организационната сложност на силите предопределят

закономерна фракталност на възможните траектории спрямо планираната, но крайните състояния се отличават със значителни разлики. В резултат става ясно, че предвидимостта на настъпващите изменения зависи от точността, с която е възможно да бъдат определени началният момент от време и скоростта на разделянето на алтернативните безкрайно близки траектории на състоянията. Нещо повече – възможно е да бъде заложен критерий за успех на управлението на военна система, който се заключава в достигането и поддържането на системните процеси в планираното устойчиво желано състояние. Поведението на военната система в условия на нелинейност и хаотичност в зоната на операцията се намира в корелацията с домейните в многомерното пространство и следва да бъде отчитано като основен фактор за появата на сложност в зоната на операцията. Неопределеността в многомерното бойно пространство поражда необходимост от познаване на условията, при които дадено въздействие върху системата нарушава устойчивостта на процеса на управление. Нерядко планирането почива на разнообразна основа при търсенето на вероятните варианти на отговор, но предизвикателството винаги е скрито в разбирането на закономерностите на неопределеността, предизвикана от сложността на организацията на многомерното бойно пространство.

Благодарности. Докладът е подготвен с финансовата подкрепа на Национална научна програма „Сигурност и отбрана“, финансирана от Министерството на образованието и науката на Република България, в изпълнение на Решение на Министерския съвет на Република България № 731 от 21.10.2021 г.

REFERENCES

KALINOV, K., 2017. *Aspekti na teoriyata na organizatsiite*. Varna: DANGRAFIK. ISBN: 978-954-9418-95-8 [in Bulgarian].

PANCHEV, S., 2001. *Teoriya na haosa*. Sofia: Akademichno izdatelstvo Prof. Marin Drinov. ISBN: 954-430-725-7 [in Bulgarian].

RESCHER, N., 2019. *Complexity: A Philosophical Overview*. NJ: Routledge. ISBN 13: 978-1-138-50837-8.

VELICHKOV, V., 2003. *Tseleva ustoichivost na voennite sistemi*. Sofia: Voenna academia [in Bulgarian].

Acknowledgments. This report was prepared with the financial support of the National Scientific Program "Security and Defense", funded by the Ministry of Education and Science of the Republic of Bulgaria, in implementation of Decision No. 731 of the Council of Ministers of the Republic of Bulgaria dated October 21, 2021.

PREDICTABILITY PROBLEMS OF SYSTEM STATES UNDER UNSTABLE ENVIRONMENTAL CONDITIONS

Abstract. Uncertainty in the multi-dimensional battlespace gives rise to the need to understand the conditions under which a given impact on the system disrupts the stability of the control process. The study examines three infinitely close possible trajectories along which the system transitions from its initial state to its final state. The first is usually the “as planned” progression. The trajectory leading to the desired final state in which corresponding complications are anticipated in the form of external disturbances from the surrounding environment. The second is the ideal and desired trajectory, which is realized under a favorable combination of external circumstances. The third state trajectory is the actual one, realized under complex operational conditions following the execution of control actions in response to adverse external disturbances affecting the system structure or functional processes. Complexity defines an inherent fractality of the possible trajectories relative to the planned one, yet the final states exhibit significant differences. The predictability of changes depends on determining the onset and rate of divergence of the infinitely close system`s trajectories.

Keywords: command and control; fractality; military system; multi-dimensional battlespace

Dr. Valentin Vasilev, Assoc. Prof.
ORCID iD: 0000-0002-4383-2590
Faculty of Navigation
Nikola Vaptsarov Naval Academy
73, Vasil Drumev St.
Varna, Bulgaria
E-mail: valentin-vasilev@naval-acad.bg

https://doi.org/10. 66334/annu26_forcefact

ФАКТОРЪТ „СИЛИ“ В МНОГОМЕРНОТО ПРОСТРАНСТВО

Валентин Василев
Висше военноморско училище „Никола Йонков Вапцаров“

Абстракт. Усложняването на организацията на бойното пространство е процес, който съпътства неизменно еволюцията на потребностите на сигурността и отбраната. Постигането на състояние на превъзходство изисква добиването на уникални системни свойства, което е възможно чрез създаване на фундаментално различен конструкт на организацията на силите в съществуващата реалност на многомерното пространство, отразявайки потребностите и технологичния напредък. Силите, изпълняващи задачи в многомерното пространство се сблъскват с комплексността на въздействията и диверсификацията на физическите източници на заплахи. Изграждането на силите на принципа „системи от системи“ е адаптиран естествен отговор на системната сложност, характерна за многомерното пространство. Тук възниква един важен проблем – необходимо е осигуряването на устойчивост на управлението в различни условия на средата, включително при нелинейност и повишена динамика.

Ключови думи: военна система; командване и управление; нелинейност; оперативни фактори

Усложняването на организацията на бойното пространство е процес, който произтича от еволюцията на потребностите в областта на сигурността и отбраната. Постигането на състояние на превъзходство в условията на нелинейна динамична среда изисква добиване на адекватни системни свойства на силите в зоната на операцията, провеждана в многомерното бойно пространство. Възможен подход за адаптиране към измененията на средата е създаването на уникален конструкт на организацията на силите във всяко конкретно проявление на съществуващата реалност на многомерното пространство, отразявайки потребностите от системни свойства на военната система, произтичащи от поставените цели и произтичащите задачи, технологичния напредък и ресурсната осигуреност. В теоретичен план, силите представляват съвкупност от сложни системи, изградени и взаимодействащи със системи. Прилагането на системния подход позволява да бъдат разкрити функционален аспект, структурен аспект и да бъдат идентифицирани определени свойства. Така например, във функционален аспект, в съответствие със зададените рамки и дълбочина на мултидомейните операции от Съвместната съюзна доктрина AJP-01, военните сили следва да са организирани и подготвени така, че да притежават способности за организирано кинетично и некинетично въздействие при гарантиране на суверенитета, и възпиране на потенциални агресори. В този контекст, силите са силовия инструмент при реализиране на концепцията за мощта на държавата.

Функционалните процеси протичат едновременно и непрекъснато в три интегрирани типа среди на въздействие. Първият обособен тип въздействия се реализират във физическата среда на мултидомейните операции. Петте домейна са основния, но лимитиран сухопътен домейн, и необятните свързващи морски домейн, въздушен домейн, кибер-пространството и космическия домейн. В контекста на сложността на многомерното пространство, силите се използват в хода на операциите да създават интегрирани ефекти в тези пет домейна. От своя страна оперативните домейни се намират във функционално взаимодействие с информационното пространство и когнитивната среда.

Друга част от функционалните процеси протичат в информационната среда, в пределите на която са размити границите на многомерното бойно пространство. Въпреки неопределеността в информационната среда, тук еволюира световната информационна мрежа, различими са процесите на наблюдение и разузнаване, осъществяват се комуникационните връзки, извършва се обработка, защита и разпространение на данни, провежда се електронна война, водят се кибернетични бойни действия.

Функционалните процеси протичат и във все по-обособяващата се в последните десетилетия когнитивна среда. С развитието на информационната свързаност и възможността на практика неконтролируемо в реално време да се обменят информация и емоции, ноосферата придобива все по-конкретни измерения при формиране на влияние върху процеса на вземане на решения от страна на противника, възприятията на населението и морално-психологическото състояние на собствените сили.

Свойствата на силите като сложни системи в значителна степен кореспондират със способностите на силите. Този подход за описание на силите дава възможност за ефикасно измерване, като се избягва механичното „броене на щикове“, което би било нецелесъобразно в многомерното пространство. Така например, военната теория показва, че измерването на силите в мултидомейна операция може да бъде извършвано чрез рамка от вида DOTMLPF-I, т.е. с отчитането на съответните показатели по отношение на критерии като прилагане на доктрини, организация на силите, обучение и тренировки, въоръжение и техника, лидерство, личен състав, инфраструктура и ниво на оперативна съвместимост (Veebel 2018).

Силите, изпълняващи задачи в многомерното пространство се сблъскват с комплексността на въздействията и диверсификацията на физическите източници на заплахи. Прилагането на системния подход прави възможно да се извърши представяне на организацията на бойното пространство като „система от системи“. Пряк резултат от имплементирането на системния подход е повишаването на познаваемостта на условията на обстановката – фактори, процеси, закономерности, рискове и заплахи, което в края на краищата води до намаляване на неопределеността.

Използвайки системния подход, нека да погледнем организацията на военната система като съвкупност от по-малки подчинени военни системи, които си взаимодействат, обменяйки енергия, информация или други материални или нематериални ресурси. Всяка една свързана система от своя страна притежава своя мисия, своя структура и характеристики. Те са „потопени“, в преносен смисъл, в една обща заобикаляща ги среда (Velichkov 2003). В тази среда се намира и театърът на военните действия, който, от своя страна, може да се опише като обособено пространство в зона на операция в мултидомейното пространство. Когато задачите се решават в многомерно пространство, управлението на системното състояние зависи от оперативните фактори. Оперативните фактори определят условията на обстановката, която влияе на присъстващите субекти в разглежданата област на пространството.

В тези условия, една реална военна система взаимодейства с външната среда. Характерно за военните системи е, че от съображения за повишаване на бойната устойчивост, същите са в голяма степен изолирани от околната среда, и въпреки че по подразбиране носят белезите на затворените сложни системи, същите се намират в ресурсна свързаност с околната среда. Свързаността обикновено е информационна и енергийна. Например, в хода на изпълнението на поставени задачи, военната система събира информация от околната среда, осъществява електронни въздействия върху цели, осъществява огнево въздействие или получава бойни повреди. Както е показано в елементарните примери, голяма е вероятността системата да бъде обект на неблагоприятни въздействия, които носят значителен потенциал да повишат вътрешната ентропия на системата, силно изместващи точката на бифуркация надясно, т.е. засилвайки неопределеността на състоянието ѝ (Kalinov 2017).

Усложняването на организацията на бойното пространство е процес, който съпътства неизменно еволюцията на потребностите на сигурността и отбраната. Постигането на състояние на превъзходство изисква конструирането на нещо фундаментално различно от съществуващата реалност в пространството, отразявайки потребностите и технологичния напредък. Различният, иновативен подход към организацията на бойното пространство позволява да се постигне военно превъзходство на оперативно ниво чрез адаптивно трансформиране на ресурсите на разположените сили и средства и своевременно извършване на маньовър, така че нито отделните платформи или бойни единици, нито техния брой са от решаващо значение в даден момент. Спечелването на превъзходство винаги е зависело от способността да се маневрира със силите и да се трансформират наличните ресурси от един вид, който се намира в излишък, в друг вид, който недостига, и който е критично важен за достигането на превъзходство над противостоящите сили. Особено това е полезно в условия на ограниченост на силите в качествен и количествен аспект и недостиг на системни ресурси.

Създаването на организация тип „система от системи“ позволява да се повишава свободата при използването на оперативните фактори и комбинациите от тях при достатъчност на оперативния фактор „информация“, в резултат на което да се постигне предимство на оперативно ниво (Nielsen 2015). Използването на предимствата, които съществуват в контекста на оперативните фактори „време“, „пространство“ и „сили“, придобиват различни измерения, когато системите са изградени от интегрирани в тях понякога почти самодостатъчни, силно адаптивни към измененията на среда-

та подсистеми, които се управляват устойчиво във времето, независимо от условията на външната среда, въпреки несигурността и непредсказуемите неблагоприятни въздействия (Millan 2025). Всъщност, устойчивостта на управлението е критично важна за постигане на военно превъзходство в описаните условия на бойното пространство. Затова способностите за командване и управление са първите, върху които ще бъде съсредоточено неблагоприятното влияние на опонента.

Организацията на системите за управление е основана на принципите на непрекъснатост, резервираност, скритост и т. н. именно с цел да се повишава бойната устойчивост, т.е. способността на силите или оръжейните системи да противостоят на неблагоприятните въздействия от страна на противника. Бойната устойчивост от своя страна пряко е обвързана с бойната ефективност на силите и оръжейните системи. Бойната ефективност следва да се разбира като способността на силите и оръжейните системи да въздействат на противника.

При изграждане на бойното пространство като система от системи трябва да бъде отчетена взаимосвързаността на средата на сигурност, изразяваща се по отношение на отбраната като свързаност между оперативните фактори, взаимосвързаността между различните оперативни домейни, свързаност на ресурсите и информационните потоци. Освен това трябва да се отбележи, че връзките в зоната на операцията имат именно ресурсен характер – основно информационна и енергийна свързаност, и в по-малка степен – материална, финансова и икономическа.

Бойното пространство променя непрекъснато своята организация. Успехът е на страната на тези сили, които притежават висока бойна устойчивост, ресурсна осигуреност и способност за непрекъснато динамично адаптиране към изменящите се условия на околната среда. Мощните центрове, в които са съсредоточени ресурсите губят своята актуалност. Съществуването в зоната на операцията на критична инфраструктура е уязвимост. Локалните военни конфликти показват, че трудно може да се гарантира безопасността на стационарни командни пунктове, неподвижната критична информационно-комуникационна инфраструктура, огромни логистични центрове, обвързани с фиксирани линии на логистичните комуникации. Силите, изпълняващи задачи в многомерното пространство се сблъскват с комплексността на въздействията и диверсификацията на физическите източници на заплахи. Концентрацията на системни ресурси на едно място, в ограничено пространство, носи риск да бъде поразено с един удар, или по-абстрактно казано – да бъде засегнато от едно неблагопри-

ятно въздействие, било то с голяма сила, голяма интензивност, сериозен мащаб и продължителност. И това не е нещо напълно ново. Сбъдването на едно случайно събитие в този случай има потенциала да въздейства драматично върху цялата система, чрез поразяването на критични подсистеми, управленски центрове, критична свързаност и критична инфраструктура. Развитието на системите за наблюдение, комуникациите, имплементирането на радикално нови високи технологии, подкрепяни от амбициите за влияние, пълен контрол и дори господство в определена сфера, водят до появата и усъвършенстването на мощни оръжия от ново поколение. В условия, когато ударните способности на силите са по-развити в технологично отношение от противодействащите военни системи, показват своята бойна ефективност оръжия, притежаващи висок разрушителен потенциал и висока вероятност за поражение на целта, като например маневриращите балистични и хиперзвуковите ракети. Технологичният бум и еволюцията на схващанията за организацията на бойното пространство, позволяват да се достигне до внезапност и висока мощност на удара, повишавайки значително дистанциите на стрелба, и висока скорост на полета при някои образци на изделията. Анализът показва, че на практика отбраната на нито един стационарен физически обект, разположен в зоната на операцията, не може да бъде гарантирана непрекъснато във времето, а по-скоро отбраната може ефективно да бъде организирана за определено време в определена зона на операцията. Така, променените условия в бойното пространство провокират търсенето на радикално променен отговор.

Как изглежда възможният отговор, погледнат през призмата на многомерното пространство, в което се намират сложни системи, обменящи системни ресурси чрез мрежови или мрежово-центрични взаимовръзки, и вече по-рядко чрез строго йерархични отношения? На театъра на военните действия, технологичният „бум“ се материализира с появата на сложни бойни платформи от ново поколение. Те са носители на значителен боен потенциал и представляват системни елементи в мултидомейното пространство. Локалните въоръжени конфликти показват, че като физически единици комуникационните технологии, усъвършенстваните артилерийски системи, управляемите крилати ракети, системите за електронна война, радарите и носещите ги платформи не са достатъчни да гарантират превъзходство. Реалността на многомерното пространство налага изграждането на устойчива и ефикасна отбранителна система, съставена от множество самостоятелно обособени „системи от системи“. Всяка адаптивна интегрирана подсистема организационно е изградена от разсредоточени и

разпределени в бойното пространство физически системни елементи, които представляват съвкупност от командни и комуникационни пунктове, заедно със съответните сензори и ефектори.

Силите, изпълняващи задачи в многомерното пространство се сблъскват с комплексността на въздействията и диверсификацията на физическите източници на заплахи. Видоизменя се характера на реализиране на заплахите. Традиционните заплахи се допълват от концептуално нови въздействия. Усложнява се бойно използване на силите. В резултат на тази непредсказуемост на средата, отговорът включва интегриране на разнородни отбранителни технологии, свързани по функционален признак, т.е. способни да осигуряват надеждно противодействие срещу широк спектър от въздействия в реално време, в няколко домейна.

Оръжейните системи се развиват, получавайки по-висока бойна устойчивост и автономност. Обикновено се цели да се достигне до универсалност при решаване на широк спектър от тактически задачи и повишаване на самата бойна ефективност. Изграждането на бойните системи на принципа „система от системи“ е адаптиран естествен отговор на системната сложност, характерна за многомерното пространство. Тук възниква един важен проблем – необходимо е осигуряването на устойчивост на управлението, както и предвидимост на поведението на системите, в различни условия на средата, включително при нелинейност и повишена динамика на факторите и процесите (Rescher 2019).

Разработват се концептуални архитектурни рамки, в които към оръжейните системи в многомерното пространство, като неделима част от силите, се предявяват изисквания, надхвърлящи стандартите за оперативна съвместимост между взаимодействащи си сили. Тези системи от ново поколение трябва да функционират устойчиво и координирано в бойното пространство. Същите следва да притежават адаптивна организационна структура, в която се интегрират динамично в течение на времето: система за командване и управление; комуникационно-информационни системи, подпомагащи вземането на решение; сложни сензори за възприемане измененията в многомерното бойно пространство; множество ефектори, способни да поразяват цели синхронизирано в множество домейни. Така става възможно в определена зона на операцията в определено време, системата на даден сензор да бъде интегрирана в бойната система и да се използва за подаване на целеуказване, което системата на определен ефектор може да изпълни в конкретен времеви интервал.

За пример, с който да се онагледи концепцията за силите тип „система от системи“, може да послужи изграждането на дизайн на ешелонирана противовъздушна отбрана с ранно предупреждение. Целта се открива и класифицира първоначално със технически системи с далечно действие. Впоследствие, контактът може да се предаде на космическа система на ниска орбита, която да продължи с процесите на следене и идентификация. Информацията се обменя устойчиво чрез комуникационно-информационни защитени мрежи, достигайки през цялото време до интелигентна система за подпомагане на командването и управлението, синхронизираща работата на системата от системи със строго ограничено закъснение на предаването на сигналите и устойчивост при обмяната на данни. Следваща фаза е възможно да включва предаване на контакта за проследяване от радари и електрооптични технически станции с наземно, въздушно с морско базиране или чрез безпилотни платформи. След обработка на информацията необходимите данни се подават към системи за управление на ефекторите. Анализът и оценката на рисковете и заплахите се осъществяват от алгоритми в реално време, така че да се гарантира кинетично или некинетично прехващане в определени участъци от траекторията на боеприпаса. По време на откриването, класифицирането и поразяването на целта в системата за командване и управление се поддържа обща многослойна оперативно-тактическа картина на обстановката, съгласувайки функциите на отделните системи в многодомейните операции. Изграждането на силите на принципа „система от системи“ позволява да се достигне до динамично адаптиране към условията на многомерното бойно пространство, чрез гъвкаво разпределяне на системните ресурси в реално време между различните домейни.

Синергията между разнородните ефекти в различните оперативни домейни позволява силите в многомерното бойно пространство да постигат превъзходство. За разлика от съвместните операции, при които видовете въоръжени сили действат физически съвместно в разграничени оперативни, синергията в многодомейното пространство търси ефекта на умножаване на усилията. Така например, синергията позволява компенсирането на дадена уязвимост или постигане на критично предимство в един домейн чрез прилагане на кинетични или некинетични въздействия от други домейни.

В заключение се достига до резултата, че изграждането на организацията на силите на принципа „системи от системи“ представлява адаптиран естествен отговор на неопределеността и системната сложност, характерна за многомерното бойно пространство. Заедно с това възниква

необходимост от гарантиране на устойчивост на управлението на силите в различни условия на средата, включително при нелинейност и повишена динамика. Усилията за повишаване на бойната устойчивост на силите в многомерното пространство при изграждането на организационни структури от вида „системи от системи“ се идентифицират със следните три основни предизвикателства пред управлението – възниква относителен информационен праг на претоварване на системата за управление, повишава се уязвимостта на системните връзки, проявяват се критични натрупвания на организационна сложност. Огромният поток от данни от различни домейни изисква внедряване на алгоритми с изкуствен интелект за бързо филтриране и приоритизиране. Достигането на количествения праг на информационно претоварване, при който количеството на информацията е в състояние да предизвика деформация на процесите, е нежелано състояние. Усложняването на вътрешната и външната системна свързаност се превръща в уязвимост. Повишаването на сложността на връзките и отношенията, заедно с повишаването на нивото на интегрираност на системите, като функция на сложността на средата прави силите зависими от комуникационните информационни ресурсни връзки. Така например, прекъсването на спътниковата връзка или смущаването на преноса на данни може временно да разпокъса или да деформира „системата от системи“. Натрупванията на организационна сложност представляват своеобразни бариери пред общата система за управление, водещи до изкривяване на корелациите и вътрешни флуктуации на системите. Проявленията могат да бъдат наблюдавани в широк спектър на неблагоприятни въздействия, породени от дублирането на структури и функционалности, съперничество за ресурси между различни подсистеми, деформиране на централизираното командване и управление – като повишена латентност на системата или фрактално изкривяване на управляващите въздействия.

Благодарности. Докладът е подготвен с финансовата подкрепа на Национална научна програма „Сигурност и отбрана“, финансирана от Министерството на образованието и науката на Република България, в изпълнение на Решение на Министерския съвет на Република България № 731 от 21.10.2021 г.

REFERENCES

KALINOV, K., 2017. *Aspekti na teoriata na organizaciite.* Varna: Dangrafik. ISBN: 978-954-9418-95-8. [in Bulgarian].

MILLAN, A. et al., 2025. Topology shapes dynamics of higher-order networks. In: *Nature Physics*, no. 21, pp. 353 – 361. [online]. Available from: https://doi.org/10.1038/s41567-024-02757-w. [last viewed: 09 September 2026]. ISSN (online) 1745-2481.

NIELSEN, Cl. et al., 2015. Systems of Systems Engineering: Basic Concepts, Model-Based Techniques, and Research Directions. In: *ACM Computing Surveys*, vol. 48, no. 18, pp. 1 – 41. [online]. Available from: https://doi.org/10.1145/2794381. [last viewed: 12 September 2026]. ISSN 0360-0300.

RESCHER, N., 2019. *Complexity: A Philosophical Overview*. NJ: Routledge. ISBN 13: 978-1-138-50837-8 (pbk).

VEEBEL, V., 2018. *Challenges Dilemmas and Progress in Developing Estonian Armed Forces.* Lambert Academic Publications. ISBN-13: 978-613-9-57847-4.

VELICHKOV, V., 2003. *Celeva ustoichivost na voennite sistemi*. Sofia: Voenna akademia “G. S. Rakovski”. [in Bulgarian].

FORCES AS A FACTOR OF MULTIDOMAIN ENVIRONMENT

Abstract. The growing complexity of battlespace is a process that inherently accompanies the evolution of security and defense factors. Achieving a state of superiority requires acquiring unique systemic properties, which is achievable through the creation of a fundamentally different force organization construct within the existing reality of multi-domain environment, reflecting current needs and technological advancement. Forces executing tasks in multi-domain space face the complexity of effects and the diversification of physical threat sources. Building forces based on the “systems of systems” principle is an adapted, natural response to the systemic complexity characteristic of multi-domain environment. Here, a critical challenge arises. It is to ensure command and control resilience of military forces across diverse environmental conditions, including nonlinearity and hyper-dynamics.

Keywords: command and control; military system; non-linearity; operational factors

Dr. Valentin Vasilev, Assoc. Prof.
ORCID iD: 0000-0002-4383-2590
Faculty of Navigation
Nikola Vaptsarov Naval Academy
73, Vasil Drumev St.
9002 Varna, Bulgaria
E-mail: valentin-vasilev@naval-acad.bg

https://doi.org/10. 66334/annu26_newconceptresh

НОВА КОНЦЕПЦИЯ И НОВО РЕШЕНИЕ НА ПРОБЛЕМА FPV ДРОН И ДРОНОВА ЗАЩИТА НА КРИТИЧНА, ВОЕННА И ГРАЖДАНСКА ИНФРАСТРУКТУРА

Валентин Каравълчев
„Конструкторско бюро Кар“ ЕООД

Абстракт. Настоящият доклад разглежда асиметричната заплаха, породена от масираното използване на евтини FPV (First-Person View) дронове и квадрокоптери и други безпилотни летателни апарати в съвременните въоръжени конфликти, както и неспособността на традиционните кинетични (Hard Kill) и радиоелектронни (Soft Kill) системи за противодействие да осигурят пълна защита на критичната, военната и гражданската инфраструктура. Представена е Синергичната интелигентна роботизирана архитектура – иновативна, автономна, кинетична система с изкуствен интелект, проектирана за откриване, проследяване и неутрализиране на високоскоростни въздушни и надземни цели. Анализират се балистичните характеристики, механичната прецизност, алгоритмите за компютърно зрение и икономическата ефективност на решението при поразяване на малки, динамични цели с конвенционални боеприпаси.

Ключови думи: FPV дронове; критична инфраструктура; СИРА; изкуствен интелект; кинетично поразяване; радиоелектронна борба; автономни системи

I. Въведение

Динамиката на съвременните въоръжени конфликти през последното десетилетие претърпя фундаментална парадигмална промяна, индуцирана от стремителната демократизация, технологичния скок и сближаването на цивилните и военните приложения на безпилотните летателни апарати (БПЛА). Ако в началото на XXI век използването на дронове бе изключителен монопол на високотехнологични държавни субекти, разполагащи с милиардни бюджети за платформи като MQ-1 Predator или MQ-9 Reaper, то днес асиметричната война изведе на преден план нискобюджетните, достъпни и изключително ефективни търговски и модифицирани системи.

Еволюцията на концепцията за дронова война премина през няколко ключови етапа. Първият осезаем сигнал за тактическата промяна бе регистриран по време на конфликта в Нагорни Карабах (2020 г.), където за първи път бе демонстрирано масирано, координирано използване на оперативно-тактически безпилотни комплекси (като Bayraktar TB2) и баражиращи боеприпаси (Loitering Munitions, известни още като дронове-камикадзе от типа Harop). Тези системи успешно парализираха класическата противовъздушна отбрана (ПВО) и бронетанковите съединения, показвайки уязвимостта на традиционните доктрини спрямо малки радиочестотни и оптични сигнатури във въздуха.

Истинският поврат и концептуална революция в използването на безпилотни апарати обаче настъпи в мащабния военен конфликт на територията на Украйна (от 2022 г. до днес). В този сблъсък се наблюдава двустранна еволюция:

1. Стратегическо и оперативно ниво. Масирано внедряване на далекобойни баражиращи боеприпаси (като фамилията „Геран“/Shahed-136) за систематично унищожаване на критична енергийна, транспортна и промишлена инфраструктура в дълбокия тил.

2. Тактическо и микониво. Повсеместното навлизане на FPV (First-Person View) дронове и модифицирани цивилни квадрокоптери (напр. DJI Mavic, Autel), трансформирани от средства за разузнаване в прецизни ударни платформи.

FPV дроновете, управлявани от оператор чрез очила за виртуална реалност и аналогова/цифрова видеовръзка с ниско закъснение, се превърнаха в основен фактор на бойното поле. Притежавайки максимална скорост, надхвърляща 150 – 200 km/h, изключителна маневреност и възможност за носене на полезен товар (кумулативни или осколочно-фугасни боеприпаси

от RPG-7, PGM и др.) с тегло от 1 до 4 kg, тези апарати постигат хирургическа точност при цена на компонентите между $500 и $800. Това създава колосален икономически и тактически дисбаланс: боеприпас за неколкостотин долара е в състояние да унищожи или изведе от строя основен боен танк на стойност над $10 милиона, високотехнологична радарна система за десетки милиони или критичен трансформатор от националната енергийна мрежа.

Тази реалност постави под сериозно съмнение ефективността на съществуващите концепции за защита на критичната, военната и гражданската инфраструктура. Възниква неотложната необходимост от създаването на принципно нови системи за противодействие, които да съчетават висока вероятност за бързо кинетично поразяване, пълен автоматизъм, устойчивост на радиоелектронни смущения и изключително ниска себестойност на единичен изстрел.

II. Изложение

2.1. Еволюция на заплахата от безпилотни летателни апарати и FPV дронове

Съвременната заплаха от БПЛА се характеризира с висока динамика, преход от единични атаки към атакуващи ята (swarm technologies) и бърза адаптация към използваните честотни диапазони. FPV дроновете представляват особено трудна за неутрализиране цел поради следните специфични фактори:

Малка ефективна повърхност за разсейване (ЕПР). Повечето FPV рамки са изработени от въглеродни влакна (карбон) и пластмаса, което прави тяхната радиолокационна отражателна способност изключително ниска (ЕПР < 0.01 m^2).

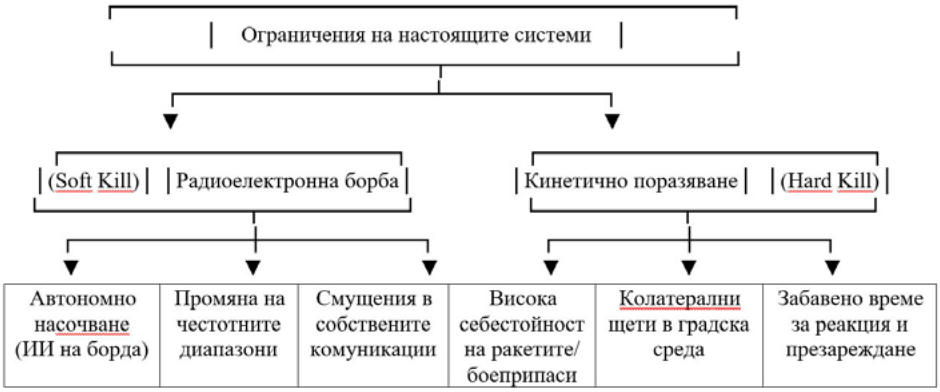
Ниска топлинна сигнатура. Безчетковите електромотори (BLDC) и литиево-полимерните (LiPo) батерии отделят минимално количество топлина в сравнение с двигателите с вътрешно горене, което затруднява откриването им с класически термични/инфрачервени глави за самонавеждане.

Полет на екстремно малки височини. FPV дроновете използват релефа на местността, сгради и растителност, движейки се в зоната на радиохоризонта и извън обсега на стандартните обзорни радари.

Високоскоростно маневриране. Възможността за моментална промяна на траекторията с претоварвания над 5G прави прогнозирането на позицията им с традиционни линейни филтри на Калман неефективно.

2.2. Недостатъци на съществуващите системи (радиоелектронна борба и кинетично поразяване)

Настоящите методи за противодействие на БПЛА се разделят на две основни категории: радиоелектронна борба (Soft Kill) и кинетично поразяване (Hard Kill). Анализът на реалните бойни действия показва драматични пропуски и в двете концепции.



Недостатъци на радиоелектронната борба (Soft Kill):

1. Адаптивни и пренастройваеми честоти. Модерните FPV системи използват нестандартни честотни ленти (например 400 – 700 MHz, 1.2 GHz, 5.8 GHz) и технологии за бързо пренастройка на честотата (FHSS). РЕБ (радиоелектронна борба) комплексите често се оказват неспособни да затиснат целия спектър.

2. Автономност чрез изкуствен интелект на борда. Навлизането на микрокомпютри (напр. NVIDIA Jetson Orin Nano) директно на борда на FPV дрона позволява автономно оптично самонавеждане (Auto-Targeting/ Optical Flow) в последния етап от полета. В този случай дронът не се нуждае от радиовръзка с оператор или GPS/GNSS сигнал, което прави РЕБ напълно безполезен.

3. Радиоелектронно заслепяване на приятелски сили. Мощните РЕБ предаватели блокират собствените комуникации, радари и безпилотни апарати в района на действие.

Недостатъци на кинетичните системи (Hard Kill):

1. Икономически дисбаланс. Използването на зенитни управляеми ракети (ЗУР) от комплекси като NASAMS, IRIS-T, Patriot или дори MANPADS (Stinger, Игла) за унищожаване на дрон за €20 000 е икономически неустойчиво (една ракета струва от €100 000 до €1 000 000). В допълнение, запасите от такива ракети са силно ограничени. Същото е валидно и за

унищожаване на FPV дрон за €500 с разход на боеприпаси за 1000 и повече.

2. Колатерални щет.: Използването на тежки зенитни оръдия или осколочни боеприпаси в градска среда създава огромен риск за цивилното население и инфраструктура от падащи осколки и неизбухнали снаряди.

3. Физически ограничения на реакциите. Скоростта на въртене и насочване на стандартните тежки дистанционно управляеми огневи модули (ДУОМ) е крайно недостатъчна за проследяване на бързо прелитащ FPV дрон на малка дистанция.

2.3. Синергична интелигентна роботизирана архитектура

За преодоляване на посочените недостатъци е разработена концепцията *СИРА (Синергична интелигентна роботизирана архитектура).* СИРА представлява робототехнически комплекс от ново поколение, съчетаващ ултрабърза кинематика, оптико-електронно откриване с изкуствен интелект и балистичен изчислител, работещ в реално време.

Основните архитектурни принципи на СИРА включват:

Интелигентна сензорна синергия. Оптичният модул на СИРА използва комбинация от широкоъгълни камери за първоначално откриване на движение и тесноъгълни камери с висока резолюция и висока честота на кадрите за класификация и проследяване. Данните се обработват от невронни мрежи, обучени за откриване на специфични силуети и динамика на полет на БПЛА.

Механика от последно поколение. Системата разполага с пряко задвижване с безчеткови сервомотори с висок въртящ момент и енкодери с висока резолюция. Това осигурява ъглова скорост на въртене по азимут и елевация, надхвърляща 120°/s, и ускорение над 300°/s^2, което е неколкократно по-бързо от традиционните куполни системи. Също така осигурява безконечно въртене на 360°.

Динамична приоритизация на целите. При поява на рояк от дронове, ИИ (изкуствен интелект) алгоритъмът моментално оценява вектора на движение, скоростта и дистанцията на всеки обект, изчислява степента на заплаха за защитената инфраструктура и съставя оптимална последователност за неутрализация.

2.4. Въоръжение и интеграция на различни платформи

СИРА е проектирана като модулна платформа, която може да бъде интегрирана с широк спектър от стрелково и артилерийско въоръжение, в зависимост от оперативния профил:

Калибри:

• *5.56×45 mm / 7.62×51 mm.* Оптимални за точково поразяване на FPV дронове в градска среда на дистанции до 300 – 500 m. Осигуряват минимален риск от колатерални щети.

• *12.7×99 mm (.50 BMG).* Предназначени за увеличен обсег (до 1000 – 1200 m) и поразяване на по-тежки БПЛА или бронирани надземни/надводни цели.

• *40 mm автоматични гранатомети (с програмируем подрив):* За създаване на облак от осколки при борба с масирани рояци от дронове.

Платформи за базиране:

Стационарни. Монтаж върху покриви на критични сгради (подстанции, подстанции на Електроенергийния системен оператор, правителствени комплекси), трансформаторни площадки, рафинерии и военни бази.

Мобилни сухопътни. Интеграция върху колесни и верижни бронирани машини (БТР, БМП, 4х4 тактически автомобили) за ескорт на конвои и охрана на маневрени единици.

Морски платформи. Защита на търговски и военни кораби, както и офшорни ветропаркове и газови платформи от FPV катери-камикадзе (USV) и нисколетящи дронове.

Оперативен профил:

Градски профил. Набор от правила за безопасност, ограничаващи ъглите на стрелба спрямо цивилни обекти и използващи високоефективни кинетични боеприпаси без рикошет.

Извънградски/Открит профил. Използване на пълния балистичен потенциал и максимизиране на дистанцията на откриване и поразяване.

III. Същност на изследването

Изследването се фокусира върху експерименталната проверка и балистичното моделиране на реакцията на системата СИРА при прихващане на FPV дрон, движещ се по сложна пространствена траектория.

3.1. Емпирични данни и хардуерни параметри

Системата СИРА използва матрица от оптични сензори с висока честота на опресняване и невронна мрежа за проследяване с ниска латентност. Задвижващият механизъм на люлката (ос за елевация) и основата (ос за азимут) постига механична резолюция от 0.015° чрез използване на абсолютни ротационни енкодери.

При провеждане на стрелковите тестове са използвани стандартни боеприпаси калибър 7.62×51 mm и 12.7x99 mm NATO. С оглед на екстрем-

ните ъгли, под които може да се наложи поразяване на FPV дронове, връхлитащи от висока височина, са направени балистични изчисления и изпитвателни серии при максимален ъгъл на наклон на люлката (55°).

В таблица 1 са представени обобщените балистични характеристики и геометрията на стрелбата, получени по време на изпитвателния цикъл.

Таблица 1. Балистични характеристики и геометрия на стрелбата при работа при максимален ъгъл на наклон на люлката (55°)

Параметър	***Калибър 7.62×51 mm***	***Калибър 12.7×99 mm***	***Мерна единица***	***Забележка/Описание***
Ъгъл на издигане на люлката (θ)	55.0	55.0	градуси °	Максимален работен ъгъл за купола
Начална скорост на куршума (V_0)	830.0	860.0	m/s	Стандартен заряд
Балистичен коефициент (C_b)	0.435	0.620	G1 BC	Стандартна аеродинамична форма
Маса на проектила (m)	9.5	44	g	Стандартни Ball
Ефективна дистанция на поразяване (Reff)	450.0	1000	m	За цел с размери 20 x 20 cm
Време на полет (t_f)	~0.62	~2.42	s	С отчитане на гравитацията и съпротивлението
Максимална височина на траекторията (Ymax)	~312.4	~964.8	m	При θ=55° и дистанция 450 m
Остатъчна скорост на ефективната дистанция за поразяване (Vrem)	~582.1	~410.5	m/s	Достатъчна за пълно разрушаване на карбон/LiPo
Остатъчна енергия на ефективната дистанция за поразяване (Vrem)	~1,610 J	~4,105	J	Достатъчна за пълно разрушаване на карбон/LiPo
Максимална ъглова скорост на проследяване	125.0	125.0	°/s	Серводвигатели
Грешка в позиционирането (RMS)	< 0.2	< 0.2	mrad	В условия на динамичен вятър с висока скорост

Математическият модел за изчисляване на предверието ($\vec{P}\ aim$) взема предвид вектора на скоростта на дрона ($\vec{V}\ drone$), разстоянието $\vec{R}$, балистичните девиации и закъснението на механичната система (τ_{sys}):

$$\vec{P}\ aim = \vec{P}\ drone\ (t) + \vec{V}\ drone.\left(\ t_f + \tau sys\right) + \frac{1}{2}\vec{g}.t_f^2 \qquad (1)$$

Благодарение на високата опреснителна честота на ИИ алгоритъма, системата преизчислява точката на среща непрекъснато, компенсирайки опитите на дрона да избяга от линията на огъня чрез хаотични маневри.



Фигура 1. Кадри от поразяване на FPV дрон с 12,7x99 mm проектил Ball (по часовниковата стрелка)

IV. Резултати от изследването

Внедряването и изпитанията на Синергичната интелигентна роботизирана архитектура показват радикално подобрение във всички ключови оперативни метрики в сравнение с традиционните кинетични и РЕБ средства:

1. Изключителна икономическа ефективност

Изпитванията доказаха, че средният брой изстрели, необходим за пълно неутрализиране (кинетично разрушаване на витла, LiPo батерия

или контролер) на FPV дрон на дистанция от 350 m, е между 3 и 7 патрона калибър 7.62×51 mm и 12,7x99 mm при стрелба с кратки, високопрецизни откоси. Това свежда финансовите разходи за неутрализация на една цел до приблизително **€18 (осемнадесет евро)**. В сравнение с разходите от стотици хиляди или милиони евро за зенитни ракети, СИРА предлага радикално икономически устойчиво решение за продължителни конфликти с висока интензивност.

2. Етичен изкуствен интелект и прецизност

Системата включва вграден алгоритмичен модул за етичен избор и оценка на риска ("Ethical AI Targeting Rules"). Алгоритъмът анализира заден фон зад целта (Background Target Analysis). Ако зад дрона в сектора на стрелба се детектира цивилен обект, жилищна сграда или критичен горивощ резервоар, ИИ автоматично забавя изстрела с частици от секундата, докато дронът промени позицията си спрямо безопасен вектор, или превключва на алгоритъм с единични изстрели.

3. Автономия и оцеляемост

СИРА разполага с интегриран хибриден захранващ блок (батериен масив и соларен/генераторен интерфейс), осигуряващ над **24 часа напълно автономна работа** в режим на непрекъснато дежурство без външно захранване. Отсътствието на активни излъчващи радари (системата разчита на пасивна оптико-електронна и термична детекция) прави СИРА практически „невидима" за противорадарни ракети и средства за радиоелектронно разузнаване на противника.

В таблица 2 са представени данните от извършения сравнителен анализ на ефективността.

Таблица 2. Сравнителен анализ на ефективността

Критерий	***Традиционна ПВО/ Скъпи РЕБ***	***СИРА (Кинетичен ИИ модул)***
Цена за неутрализация на една цел	€100 000 – €1 500 000 (Ракета/Инфрастр.)	~ €18 (Кратък откос 7.62 mm/12,7 mm)
Време за реакция	3.5 – 8.0 секунди	< 0.25 секунди
Зависимост от радиоканал	Висока (при РЕБ)	Нулева (Оптичен ИИ)
Автономна работа	Ограничена (Изисква висококвалифициран оператор)	24 часа (Автономно захранване)

V. Заключение

Резултатите от настоящото изследване потвърждават, че Синергичната интелигентна роботизирана архитектура представлява качествен скок в технологията за защита на критична, военна и гражданска инфраструктура от нарастващата заплаха от FPV дронове и автономни БПЛА. Чрез съчетаването на ултрабърза прецизна механика, изкуствен интелект за оптично откриване и проследяване и евтини конвенционални кинетични боеприпаси, СИРА успешно разрешава основния парадокс на съвременната противовъздушна отбрана – икономическата асиметрия между цената на нападението и цената на защитата.

Системата показва пълна готовност за интеграция в многослойни системи за сигурност, предоставяйки надеждна, високоскоростна и етично управлявана защита на стратегически обекти в условията на съвременната високотехнологична война.

Благодарности. Настоящият ръкопис е написан благодарение на разработка на Валентин Каравълчев, д-р инж. Александър Стефанов и на екипа на „Конструкторско бюро Кар“ ЕООД.

БЕЛЕЖКИ

1. Технологичният прототип, балистичните изпитвания и хардуерната интеграция на системата СИРА са реализирани от инженеринговия екип на компанията KBKAR (КБКАР) – специализирано предприятие за научно-развойна дейност в областта на роботиката и отбранителните технологии.

2. Резултати от демонстрация проведена на ЦАТИП – Стара Загора на 09.07.2026 г.

3. Протокол от полигонни изпитвания на Антидрон система “SIRA” чрез стрелба с 12,7 мм картечница на ЦАТИП на 09.07.2026 г.

4. ИВАНОВ, И.; ПЕТРОВ, Г. & ДИМИТРОВ, В., 2022. *Асиметрични заплахи и еволюция на безпилотните летателни апарати*. София: Издателство на Министерството на отбраната.

5. BENGO, Y., & GUY, N., 2025. *The FPV Revolution and Its Implications for Land Warfare and Other Dimensions of Warfare*. Ramat Gan: Begin-Sadat Center for Strategic Studies. [online]. Available from: http://www.jstor.org/stable/resrep71873.

6. DOBIJA, K., 2026. Protection of Critical Infrastructure from Unmanned Aerial System Attacks: Challenges and Solutions. *Safety & Defense*, vol. 12, no. 1, pp. 44 – 53. [online]. Available from: https://doi.org/10.37105/sd.287.

7. RUSSELL, S. & NORVIG, P., 2020. *Artificial Intelligence: A Modern Approach*. 4th ed. Hoboken: Pearson. ISBN 978-0134610993.

8. SMITH, J.A. & DAVIS, M.R., 2023. Kinetic Counter-UAS Solutions for Urban Infrastructure Protection. *Journal of Defense Technology and Robotics*, vol. 15, no. 3, pp. 112 – 126. ISSN 1548-5129.

NEW CONCEPT AND NEW SOLUTION TO THE FPV DRONE PROBLEM AND DRONE PROTECTION OF CRITICAL, MILITARY, AND CIVILIAN INFRASTRUCTURE

Abstract. This paper addresses the asymmetric threat posed by the widespread deployment of low-cost FPV (First-Person View) drones and quadcopters and others UAVs in modern warfare, along with the limitations of conventional kinetic (Hard Kill) and electronic warfare (Soft Kill) systems in protecting critical, military, and civilian infrastructure. The Synergistic Intelligent Robotic Architecture is introduced – an innovative, autonomous, AI-driven kinetic system designed to detect, track, and neutralize high-speed aerial and surface targets. The study presents ballistic characteristics, mechanical precision, computer vision algorithms, and cost-efficiency analysis of neutralizing dynamic targets using standard ammunition.

Keywords: FPV drones; critical infrastructure; SIRA; artificial intelligence; kinetic interception; electronic warfare; autonomous systems

Valentin Karavalchev
Konstructor Bureau Kar Ltd.
105, Arsenalski Blvd.
Sofia, Bulgaria
E-mail: ceo1@kbkar.eu

https://doi.org/10. 66334/annu26_aideepstrikes

AI-DRIVEN DEEP STRIKES VIA UAVS IN THE WAR IN UKRAINE: NEW CAPABILITIES AND OPERATIONAL ART

Valentin Peychev
Rakovski National Defence College (Bulgaria)

Abstract. The war in Ukraine demonstrates the growing importance of unmanned aerial vehicles (UAVs) for combat operations beyond the immediate frontline. This study examines the development of Ukrainian "middle strike" UAV operations targeting Russian assets in operational depth. Particular attention is paid to logistics infrastructure, command posts, air defense assets, transport networks, and other second-echelon elements supporting Russian frontline forces. The analysis covers the integration of artificial intelligence, autonomous capabilities, reconnaissance, and long-range precision strikes within Ukrainian operational art. Finally, the research explores not only the destruction of individual targets but also the capacity of these systems to disrupt the enemy's overall supply and support network.

Keywords: artificial intelligence; operational depth; precision strikes; second-echelon elements; Ukrainian operational art; unmanned aerial vehicles (UAVs)

1. Introduction

The current battlefield environment in eastern Ukraine is increasingly shaped by unmanned aerial systems (UAS). Drones – including first-person-view (FPV) platforms, the Hornet 2, and quadcopters – are used extensively for reconnaissance and strikes. In some areas, the density of unmanned systems creates a persistent threat to mechanised forces and logistics, including within approximately 15 km of the frontline.[22]

The rapid evolution from short-range tactical drones to systems capable of operating at operational and strategic depth represents a significant change in modern warfare. What began in 2022 with the adaptation of commercial quadcopters has developed into a more structured deep-strike capability.[23]

In Ukrainian military discourse, "middle strike" refers to drone operations against targets in the operational depth of the battlefield, commonly described as reaching approximately 30 – 200 or 300 kilometres behind the front line. This concept occupies an intermediate space between tactical frontline operations and deep strikes against strategic targets.[24]

The shift from isolated drone attacks to organised middle-strike campaigns may affect military operations in several ways. Beyond destroying individual vehicles or warehouses, such campaigns can disrupt logistics, challenge air-defence networks, interfere with command and control, and create cost asymmetries between attackers and defenders.[25]

1. Logistical disruption. Supply hubs were traditionally positioned beyond the effective range of many frontline weapons. Middle-strike systems can threaten some of these rear-area locations, reducing the assumption that distance alone provides protection.[26]

2. Pressure on air defences. Ukrainian middle-strike operations have targeted radar systems and mobile air-defence assets, including systems such as Pantsir, Tor, and Buk. Such attacks can degrade the coverage and survivability of air-defence networks.[27]

3. Disruption of command and control. Strikes against command posts and communications infrastructure can interfere with coordination and decision-making, affecting more than the units directly engaged on the frontline.[28]

4. Cost asymmetry. The use of comparatively inexpensive uncrewed systems against costly military assets can create an unfavourable cost exchange for the defender, although the actual balance depends on system performance, production, and interception rates.[29]

Artificial intelligence (AI) and autonomy are becoming increasingly important in uncrewed-system development. Electronic warfare (EW), including

interference with radio links and Global Navigation Satellite Systems (GNSS), can limit remotely piloted operations. AI-enabled navigation and onboard processing may allow some systems to continue parts of their mission when communications or satellite navigation are degraded; however, capabilities vary by platform and should not be treated as universal.[30]

The growing use of autonomous systems may influence operational art – the link between battlefield action and strategic objectives. Rather than relying solely on mass and attrition, forces may increasingly seek to disrupt an opponent's networks, decision-making, and ability to coordinate. Terms such as "software-defined kill webs" describe this emerging concept, but its practical effectiveness remains dependent on technical and operational conditions.[31]

2. Conceptual Framework: From Tactical UAVs to Middle Strike

Before Russia's full-scale invasion in 2022, Ukrainian UAV use was more limited and often focused on tactical reconnaissance and support. Between the beginning of the war in Donbas in 2014 and late 2021, development involved gradual institutional adoption and substantial improvisation by civilian volunteers and military units.[32]

UAS now support a wide range of tasks, including reconnaissance, artillery correction, battlefield surveillance, target acquisition, and tactical strikes. Their operational reach has also expanded beyond the immediate line of contact. Depending on their design and payload, systems can threaten personnel, vehicles, armoured platforms, ammunition depots, radar installations, roads, and command infrastructure. Middle- and deep-strike operations extend this threat into the adversary's operational rear.[33]

The term "middle strike" describes drone operations directed at the operational rear, commonly associated with targets approximately 30 – 200 or 300 kilometres behind the front line. Unlike tactical strikes against forces in immediate contact, these operations aim to disrupt the systems that sustain battlefield activity, including air-defence radars, ammunition depots, command centres, and transport corridors. Their intended effects may unfold over days or weeks by making it harder for frontline units to receive supplies and coordinate operations. The Ukrainian Ministry of Defence describes this role directly: "Middle-strike operations fill the gap between them, enabling systematic strikes at ranges of around 30 – 200 km".[34] This supports the distinction between tactical frontline strikes and attacks against the operational rear.[35]

One intended effect of middle-strike operations is to increase the logistical burden on frontline units and complicate their coordination. In response, Russian forces may disperse or relocate vulnerable assets farther from the front, including ammunition depots, repair facilities, command posts, and logistics hubs. Such relocations can reduce exposure to some drone threats, but they may also lengthen supply routes and increase delivery times. The extent of these effects varies by location and operational circumstances.[36]

The types of Russian equipment reported as lost have changed over the course of the war, but any claim that logistics vehicles overtook armoured vehicles in 2026 requires a clearly defined dataset and time period. The comparison should therefore be supported with a specific loss-tracking source before being presented as a confirmed trend.[37]

The operational effects of strikes against logistics depend partly on geography and the location of the line of contact. Kherson, Crimea, and Zaporizhzhia are relevant areas for examining how terrain, distance, and access routes shape Russian supply networks. However, the direction of advances alone does not determine whether logistics become easier or more difficult; the analysis must also account for available roads, railways, bridges, ports, and the distance to supply bases.[38]

3. The Technological Transformation

AI-assisted UAS are attracting considerable attention, but they should not be treated as a single, standardised technology. Capabilities differ between platforms, and systems may combine different software and sensors depending on their intended operating environment. It is therefore more accurate to view AI-enabled drones as platforms that can incorporate different navigation, perception, and decision-support functions. Bondar cautions that "the current deployment of AI is partial in scope, enhancing certain functions and addressing some operational challenges rather than enabling full system autonomy".[39] This qualification is important: AI assistance should not be equated with a fully autonomous ability to conduct an entire engagement.[40]

The following section outlines several functions that may be incorporated into uncrewed systems, depending on the platform and mission.

AI-assisted navigation

1. autonomous navigation
2. route planning
3. terrain/obstacle avoidance

4. operation under degraded GNSS conditions
Target recognition and identification
1. object detection
2. classification
3. target recognition
4. imagery analysis

Ukraine's use of relatively low-cost drone systems has made UAS an important part of its military capabilities. AI-enabled image processing may support the detection or classification of objects such as personnel, vehicles, and structures, using data from visible-light or thermal sensors. Some systems may also use onboard processing during the terminal phase of flight, potentially allowing them to continue toward a target if the communication link is disrupted. These capabilities differ significantly between systems, and claims about shared databases or specific engagement ranges require direct technical sourcing.[41]

Autonomous navigation and onboard target-recognition functions may reduce a drone's dependence on continuous communication or GNSS signals. They do not, however, make electronic warfare ineffective in every case: the effect of jamming depends on the system's sensors, navigation method, software, and degree of autonomy. Bondar notes that such systems "typically do not perform the entire process of finding, selecting, and engaging targets independently".[42] This reinforces the need to distinguish between autonomy in individual functions and autonomy across the full targeting-and-engagement process.[43]

4. Operational Implications: The Death of the Sanctuary

Compressing the rear echelon. Command posts, supply hubs, and staging areas have traditionally been positioned at a distance from the front line to reduce their exposure to frontline weapons. Middle-strike systems can threaten some of these locations, weakening the assumption that rear areas are inherently safe. The level of risk depends on the range, accuracy, availability, and survivability of the attacking systems.[44]

The limits of traditional electronic warfare. Jamming radio-control links or disrupting GNSS can interfere with some uncrewed systems. Platforms that use alternative navigation methods or onboard image processing may be more resilient under certain conditions, but they are not necessarily immune to electronic warfare or other countermeasures.[45]

The radar-horizon challenge. Low-flying drones can exploit terrain masking and the curvature of the Earth to reduce the time available for detection by some radar systems. This can complicate defence, particularly where terrain or infrastructure obstructs radar coverage. Responses may include layered air defence, point-defence weapons, and other counter-UAS measures; the most suitable combination depends on the threat and local conditions.[46]

The transition to algorithm-assisted command. As the number and complexity of uncrewed systems increase, automated tools may help operators process information, plan routes, and identify potential targets. This does not make a wholesale transfer of command to AI inevitable. Human oversight, communications, rules of engagement, and reliable identification remain important operational and legal considerations.[47]

Cost asymmetry. Relatively inexpensive drones may threaten much more costly infrastructure or military equipment, creating an unfavourable cost exchange for the defender. However, specific comparisons – such as the cost, range, and target value of a particular strike – should be supported by verifiable figures rather than presented as general facts. The economic balance also depends on production costs, interception rates, and the cost of defensive measures.[48]

5. Limitations and Risks

5.1. Technological Bottlenecks and Failure Modes

The fragility of computer vision in edge cases. AI systems that rely on visual recognition may perform less reliably when environmental conditions differ from their training data. Snow, fog, smoke, fire, and seasonal changes can alter the appearance of terrain and targets, increasing the risk of navigation errors or misidentification.[49]

Navigation fragility. Autonomous navigation depends on the quality and consistency of sensor data. Errors in camera calibration, inertial measurement, or sensor fusion can accumulate and degrade a system's estimate of its position or orientation, potentially causing it to deviate from its intended route. The severity of this risk depends on the system's design and safeguards.[50]

The compute-power trade-off. Advanced onboard perception and target-recognition models require processing resources. On small airframes, constraints on computing power, battery capacity, weight, and payload can force design compromises. These limitations may affect endurance, sensor performance, and mission capability.[51]

5.2. Operational Vulnerabilities to Physical Countermeasures

Camouflage and visual deception. Systems that rely on visual target recognition may be confused by decoys, changes to vehicle silhouettes, smoke, or other forms of visual concealment. The effectiveness of these countermeasures depends on the sensors and recognition models used by the drone.[52]

Kinetic and low-tech point defences. Low-altitude drones may be vulnerable to localised countermeasures, including guns, interceptor systems, and physical barriers or nets where these are practical. No single measure provides universal protection; effective defence generally depends on detection, warning, and a layered response suited to the particular threat.[53]

5.3. Strategic Risks and Cascade Effects

Software brittleness. Dependence on software and trained models creates a risk that a weakness discovered in one system could be exploited against other systems using the same design. Captured hardware or software could also help an adversary develop countermeasures. The scale of any resulting disruption would depend on how widely the vulnerable components are shared across a fleet.[54]

Unintended escalation and loss of human control. Greater autonomy can complicate intervention when communications are lost or a target changes during flight. Misidentification or an inability to abort a mission could lead to unintended damage, including harm to civilian infrastructure, and increase the risk of escalation. These risks reinforce the importance of testing, human oversight, and clearly defined limits on autonomous weapon functions.[55]

6. Conclusion

The development of Ukraine’s uncrewed aerial systems (UAS) illustrates how rapidly drone warfare and operational practice are evolving. Since 2014, Ukrainian forces have expanded from improvised and largely tactical uses of drones toward more organised systems for reconnaissance, strike, and operations against targets in the operational rear. Middle-strike campaigns can place pressure on logistics and air-defence networks and may create cost asymmetries for the defender.[56]

AI-assisted navigation and onboard perception may help some systems operate when communications or satellite navigation are degraded, but these capabilities are not universal and do not eliminate the effects of electronic warfare or physical countermeasures. They also introduce technical and strategic risks, including sensor error, visual deception, software vulnerabilities, and unintend-

ed escalation. The future operational impact of these systems will depend not only on autonomy, but also on reliability, human oversight, production capacity, and the ability of both sides to adapt.[57]

NOTES

1. WATLING, Jack, 2025. *Emergent Approaches to Combined Arms Manoeuvre in Ukraine*; CSIS, 2025. *Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience*

2. WATLING, Jack, 2025. *Emergent Approaches to Combined Arms Manoeuvre in Ukraine*; CSIS, 2025. *Operational Fires in the Age of Punishment*

3. Ukrainian Ministry of Defence, 2026. 2*5 Russian Air Defense and Radar Systems Were Hit: Results of Middle-Strike Operations in April;* FAY, Wong Yee, 2026. *Intermediate-Range Strike Drones: Lessons from the War in Ukraine*

4. Ukrainian Ministry of Defence, 2026. *Middle-Strike Operations: How Ukrainian Drones Are Degrading Russia's Military Potential*; CSIS, 2025. *Operational Fires in the Age of Punishment*

5. Ukrainian Ministry of Defence, 2026. *Middle-Strike Operations: How Ukrainian Drones Are Degrading Russia's Military Potential*; WELSCH, Marcus; ATALAN, Yasir; JENSEN, Benjamin; TIERSTEN-NYMAN, Erik, 2026. *The Geography of Coercion: Russian Missile and Drone Campaigns in Ukraine*

6. Ukrainian Ministry of Defence, 2026. *25 Russian Air Defense and Radar Systems Were Hit: Results of Middle-Strike Operations in April*

7. Ukrainian Ministry of Defence, 2026. *Middle-Strike Operations: How Ukrainian Drones Are Degrading Russia's Military Potential*; WATLING, Jack, 2025. *Emergent Approaches to Combined Arms Manoeuvre in Ukraine*

8. CSIS, 2025. *Operational Fires in the Age of Punishment*; NATO Science and Technology Organization, 2023. *NATO STO Highlights*

9. BONDAR, Kateryna, 2025. *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*; NATO Science and Technology Organization, 2023. *NATO STO Highlights*

10. BONDAR, Kateryna, 2025. *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*; CSIS, 2025. *Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience*

11. WATLING, Jack, 2025. *Emergent Approaches to Combined Arms Manoeuvre in Ukraine*; NATO Science and Technology Organization, 2023. *NATO STO Highlights*

12. WATLING, Jack, 2025. *Emergent Approaches to Combined Arms Manoeuvre in Ukraine*; Ukrainian Ministry of Defence, 2026. *Middle-Strike Operations: How Ukrainian Drones Are Degrading Russia's Military Potential*; WELSCH, Marcus; ATALAN, Yasir; JENSEN, Benjamin; TIERSTEN-NYMAN, Erik, 2026. *The Geography of Coercion: Russian Missile and Drone Campaigns in Ukraine*

13. Ukrainian Ministry of Defence, 2026. *Middle-Strike Operations: How Ukrainian Drones Are Degrading Russia's Military Potential*

14. FAY, Wong Yee, 2026. *Intermediate-Range Strike Drones: Lessons from the War in Ukraine*

15. Ukrainian Ministry of Defence, 2026. *Middle-Strike Operations: How Ukrainian Drones Are Degrading Russia's Military Potential;* WELSCH, Marcus; ATALAN, Yasir; JENSEN, Benjamin; TIERSTEN-NYMAN, Erik, 2026. *The Geography of Coercion: Russian Missile and Drone Campaigns in Ukraine*

16. WELSCH, Marcus; ATALAN, Yasir; JENSEN, Benjamin; TIERSTEN-NYMAN, Erik, 2026. *The Geography of Coercion: Russian Missile and Drone Campaigns in Ukraine*

17. WELSCH, Marcus; ATALAN, Yasir; JENSEN, Benjamin; TIERSTEN-NYMAN, Erik, 2026. *The Geography of Coercion: Russian Missile and Drone Campaigns in Ukraine*

18. BONDAR, Kateryna, 2025. Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare

19. NATO Science and Technology Organization, 2023. *NATO STO Highlights*

20. BONDAR, Kateryna, 2025. Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare; NATO Science and Technology Organization, 2023. *NATO STO Highlights*

22. BONDAR, Kateryna, 2025. Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare

22. NATO Science and Technology Organization, 2023. *NATO STO Highlights*

23. Ukrainian Ministry of Defence, 2026. *Middle-Strike Operations: How Ukrainian Drones Are Degrading Russia's Military Potential*; FAY, Wong Yee, 2026. *Intermediate-Range Strike Drones: Lessons from the War in Ukraine*

24. BONDAR, Kateryna, 2025. Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare; NATO Science and Technology Organization, 2023. *NATO STO Highlights*

25. NATO Science and Technology Organization, 2023. *NATO STO Highlights*; Ukrainian Ministry of Defence, 2026. *25 Russian Air Defense and Radar Systems Were Hit: Results of Middle-Strike Operations in April*

26. BONDAR, Kateryna, 2025. *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*; NATO Science and Technology Organization, 2023. *NATO STO Highlights*

27. CSIS, 2025. *Operational Fires in the Age of Punishment*; NATO Science and Technology Organization, 2023. *NATO STO Highlights*

28. BONDAR, Kateryna, 2025. *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*; NATO Science and Technology Organization, 2023. *NATO STO Highlights*

29. BONDAR, Kateryna, 2025. *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*; NATO Science and Technology Organization, 2023. *NATO STO Highlights*

30. BONDAR, Kateryna, 2025. *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*; NATO Science and Technology Organization, 2023. *NATO STO Highlights*

31. BONDAR, Kateryna, 2025. *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*; NATO Science and Technology Organization, 2023. *NATO STO Highlights*

32. NATO Science and Technology Organization, 2023. *NATO STO Highlights*

33. BONDAR, Kateryna, 2025. *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*; NATO Science and Technology Organization, 2023. *NATO STO Highlights*

34. BONDAR, Kateryna, 2025. *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*; NATO Science and Technology Organization, 2023. *NATO STO Highlights*

35. WATLING, Jack, 2025. *Emergent Approaches to Combined Arms Manoeuvre in Ukraine*; Ukrainian Ministry of Defence, 2026. *Middle-Strike Operations: How Ukrainian Drones Are Degrading Russia's Military Potential*; *WELSCH, Marcus; ATALAN, Yasir; JENSEN, Benjamin; TIERSTEN-NYMAN, Erik, 2026.* The Geography of Coercion: Russian Missile and Drone Campaigns in Ukraine

36. BONDAR, Kateryna, 2025. *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*; NATO Science and Technology Organization, 2023. *NATO STO Highlights*; CSIS, 2025*. Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience*

Valentin Peychev
Rakovski National Defence College
82, Evlogi i Hristo Georgievi Blvd.
1504 Sofia, Bulgaria
E-mail: v.s.peychev@rndc.bg

https://doi.org/10. 66334/annu26_micromilisymb

МИКРОСЪЮЗИТЕ – ВОЕННО-ИКОНОМИЧЕСКАТА СИМБИОЗА В СРЕДАТА ЗА СИГУРНОСТ

Валери Тодоров
Военна академия „Г. С. Раковски“

Абстракт. Настоящият доклад разглежда влиянието на съвременната среда за сигурност върху формирането и развитието на микросъюзите като инструмент за повишаване на отбранителните способности и регионалната устойчивост. Анализирана е взаимовръзката между военното сътрудничество, икономическите възможности и развитието на отбранителната индустрия. Проучен е историческият опит и развитието на процесите на взаимодействие между държавите от Балканския полуостров. Поставен е акцент върху проблемите на военно-промишления капацитет, изразяващ се в ресурсен, технологичен и научно-експертен аспект. Направен е извод, че необходимостта от преодоляване на тези дефицити стимулира създаването на микросъюзи, основани на споделяне на ресурси, индустриален капацитет и технологични способности, които се превръщат във важен елемент от съвременната архитектура на сигурността.

Ключови думи: военно сътрудничество; микросъюз; надпревара във въоръжението; сигурност; съглашения; съюз

Съвременната среда за сигурност е изключително променлива, динамична и сложна и създава усещането за надигащо се напрежение от възникването на нови военно-икономически договорености във връзка със засилените хибридни и асиметрични заплахи, геополитическата нестабилност и регионалната конфронтация, натиска от въвеждането и влиянието на изкуствения интелект във всички сфери на обществения живот и необходимостта от активното участие и гарантиране на устойчивостта и функционирането на средата за киберсигурност.

Необходимостта от бързо налагане на натиск над текущите отбранителни системи и способността им бързо да се адаптират към новата среда за сигурност за защита на критичната инфраструктура е от изключителна важност за намаляване на предизвикателствата пред националните, регионалните и международните договорености и постигането на нужната устойчивост на системата, разглеждана като сложна система, изградена от множество подсистеми.

За да бъде причислена като част от системата за сигурност на Европа е необходимо да бъде разгледана през призмата на Националната отбранителна стратегия *„В Югоизточна Европа (...) тенденцията към по-нататъшно стабилизиране и пълноценно включване на региона в евро-атлантическото пространство. За това допринасят приемането на нови отбранителни стратегии, в които на преден план са изведени противодействието на асиметричните и евентуалните хибридни заплахи и разширяването на двустранното и регионалното сътрудничество“*.[1]

Средата за сигурност в глобален мащаб поражда необходимостта от разглеждане на намеренията на поддържащите се страни в един съюз за задълбочено сътрудничество, което да генерира синергичен ефект в интерес на военно-промишления капацитет (ВПК)/потенциал и икономическия растеж, който от своя страна ще гарантира нормализиране и/или подобряване на средата за сигурност и постигане на устойчивост срещу различни заплахи.

Визията на всяка държава, която участва в политико-военен съюз на сходни по икономически възможности държави, е насочена към концентриране на усилията за изграждане на нови и развитие на съществуващите отбранителни способности с цел повишаване на националния отбранителен капацитет и стимулиране развитието на отбранителната индустрия. Този процес оказва пряко влияние върху научно-технологичния прогрес, който от своя страна формира динамиката на съвременната среда за сигурност. В този контекст укрепването на националния отбранителен потен-

циал се утвърждава като ключов фактор за гарантиране на сигурността и устойчивостта на държавата. Наред с това икономическият фактор заема съществено място при изграждането на ефективни отбранителни способности, поради което все по-голямо значение придобива установяването на партньорства между държави със сходни военно-политически интереси, общи стратегически приоритети и близки икономически възможности. Именно подобни форми на регионално сътрудничество създават предпоставки за възникването на микросъюзи, основани на взаимно допълване на отбранителния и икономическия потенциал на участниците.

Политическият стремеж за запазване на единството между съюзниците и осъзнаването на споделената отговорност представляват жизненоважна предпоставка за задълбочаване на сътрудничеството и реализиране на общите амбиции за повишаване на икономическите и отбранителните способности. Именно тази политическа, икономическа и отбранителна взаимозависимост създава условия за формирането на микросъюзи като ефективен механизъм за адаптиране към динамично променящата се среда за сигурност. Обединяването на държавите около общи цели, свързани с планиране, разработване и реализиране на проекти от взаимен интерес, съпроводено с осъществяването на инвестиции с висока добавена стойност, се утвърждава като едно от основните направления за развитие на военно-промишления потенциал и повишаване на икономическата конкурентоспособност. Наред с това сътрудничеството между държавите по постигане на стратегически цели се обусловя от динамиката на военно-политическата среда, като същевременно се отчитат националните културно-исторически особености, стратегическите приоритети и възприетите модели за интеграция и развитие. Именно съчетаването на тези фактори формира предпоставки за изграждането на устойчиви микросъюзи, основани на общи интереси, взаимно доверие и допълващи се отбранителни и икономически способности.

Всяка държава от Балканския регион (полуостров), която членува в НАТО, се стреми да развива и усъвършенства своите отбранителни способности в съответствие със специфичните си национални приоритети, като същевременно изпълнява съюзническите ангажименти в рамките на НАТО и Европейския съюз. Показателен пример в това отношение е Република България, чиято Национална отбранителна стратегия определя като основни направления за развитие на отбранителните способности изпълнението на инвестиционни проекти за превъоръжаване и модернизация, съгласуваното развитие на всички компоненти на отбранителната систе-

ма, дигиталната трансформация, внедряването на нови технологии, повишаването на устойчивостта, участието в съвместни проекти със съюзни държави в рамките на НАТО и Европейския съюз, както и използването на потенциала на науката, отбранителната индустрия и специализираните агенции на двете организации.[2]

Посочените приоритети показват стремежа към задълбочаване на интеграцията и изграждане на устойчивост като водещи принципи при развитието на системата за сигурност в регионален мащаб. Реализирането на тези принципи има за цел да осигури на системата стабилно функциониране в условията на хибридни въздействия, военно-политически кризи и въоръжени конфликти. В този контекст задълбочаването на сътрудничеството и тясното взаимодействие между държавите се утвърждават като основна предпоставка за ефективното развитие на техния отбранителен и икономически потенциал, което създава благоприятни условия за формирането и развитието на регионални микросъюзи.

Следва се политиката на средата за сигурност, като се цели постигането на интеграция и изграждането на устойчивост, което е приоритет, позволяващ стабилно функциониране на системата за сигурност при хибридно въздействие, криза от военнополитически характер и военен конфликт.

Ретроспекцията през погледа на времето разкрива, че тези съглашения носят потенциал за разширяване и развитие, като понякога не може да се уточни или гарантира на какъв етап от времето или при какви условия може да се наклонят така везните, че да се преобърнат изцяло първоначално заложените намерения.

При разглеждането на тези микросъюзи един бърз преглед назад във времето в периода непосредствено преди Първата световна война, а именно през Балканската война, води до извода, че подобна политика е била провеждана и впоследствие е довела до т.нар. Междусъюзническа война. При сключването на договорки за поддръжка и сътрудничество в различните домейни е необходимо те да се идентифицират коректно, ясно и отговорно за ограничаване на възможностите за произтичаща заплаха от въвличане в евентуален военен конфликт или блоково икономическо противопоставяне.

От гледна точка на историческия контекст следва да разгледа Балканският съюз (1912), който се характеризира като антиосманска военна коалиция, формирана в навечерието на Балканската война от България, Сърбия, Гърция и Черна гора. Технически съюзът е оформен чрез двустранни

договори на България със Сърбия (29 февруари 1912 г.); България с Гърция (16 май 1912 г.), с които се солидаризира и Черна гора. През октомври 1912 г. съюзниците повеждат бойни действия срещу Османската империя и бързо завоюват почти всичките ѝ европейски владения. Неразрешените териториални противоречия, въведени чрез тези двустранни договори, обаче пораждат напрежение помежду им, което се засилва още след първите военни успехи. Балканският съюз се разпада окончателно с избухването на Междусъюзническата война през юни 1913 г.

Направеният кратък исторически анализ с поуките от началото на XX в. показва съществуващата релация със съвременната среда за сигурност. Аналогични форми на регионално сътрудничество могат да бъдат открити и днес, включително в Западна Европа, където държавите изграждат различни формати на взаимодействие, основани както на общи отбранителни интереси, така и на икономическа взаимозависимост. Именно тези процеси представляват съвременен израз на военно-икономическата симбиоза, която стои в основата на формирането и развитието на микросъюзите.

В регионален план от гледна точка на времето и етническото противопоставяне се формира едно политическо напрежение, което натоварва процесите по добросъседство и разбирателство между страните. Единствено остава възможността чрез икономически и инфраструктурни обвързаности да бъде постигнато разбирателство и сътрудничество за преодоляване на тези дългогодишни различия.

При влошаване на средата за сигурност чрез отчитане, анализ и извличане на изводи от всички оперативни домейни[3] оказва влияние върху военно-политическите ръководства и подтиква техните правителства да прибегнат до подобен тип практика, целящи да гарантират най-малкото икономическото сътрудничество и устойчивостта средата за сигурност за достигане до относително спокойни нива.

Динамиката на геополитическите процеси на Балканския полуостров създава условия за създаването на нови регионални взаимоотношения и микросъюзи, които да са в отговор на променящата се среда за сигурност и необходимостта от защита на общи стратегически интереси.

Съществуването на подобни съюзи е обосновано и носи своята историческа препратка. В бъдеще някои от тях може да се разглеждат като изключително устойчиви и икономически обосновани за всички участници. Разширяването на съществуващите и формирането на нови с нови изисквания към способности ще намерят приложение и ще срещнат допирни точки, което ще гарантира важността и необходимостта от тяхното съществуване.

На Балканите архитектурата на сигурност е разделена между глобални алианси (НАТО) и нови регионални военно-политически оси, които се пренареждат в отговор на геополитическите промени в Европа.

Архитектурата на сигурността на Балканския полуостров се характеризира със съчетаване на установени колективни механизми за отбрана и нововъзникващи регионални формати на сътрудничество. Водеща роля за гарантиране на сигурността в региона има НАТО, в който съюз са държавите България, Гърция, Турция, Румъния, Албания, Северна Македония, Черна гора и Хърватия. В рамките на съюза те координират развитието на своите отбранителни способности, участват в съвместното отбранително планиране и изпълняват ангажиментите си, свързани с колективната отбрана. Наред с това динамиката на средата за сигурност и променящата се геополитическа обстановка стимулират формирането на нови регионални инициативи, които допълват съществуващата система за сътрудничество. Пример за това е подписаната през месец март 2025 г. „Съвместна декларация за сътрудничество в отбраната“ между Хърватия, Албания и Косово, насочена към задълбочаване на взаимодействието в областта на отбраната и сигурността. В същия период Сърбия и Унгария разширяват своето стратегическо партньорство в сферата на отбраната, като Сърбия запазва политиката си на военен неутралитет спрямо НАТО, но развива двустранно сътрудничество с Унгария. Развитието на тези инициативи показва, че наред с утвърдените механизми на колективната отбрана се наблюдава тенденция към изграждане на по-гъвкави регионални формати на сътрудничество. Те се основават на съвпадащи национални интереси, географска близост, общи предизвикателства пред сигурността и стремеж към по-ефективно използване на отбранителните и икономическите ресурси. Именно тези характеристики ги определят като съвременни проявления на микросъюзите в средата за сигурност.

Регионални инициативи за сътрудничество: освен преките съюзи, съществуват по-широки формати за координация без твърди ангажименти за взаимна защита:

– Процесът *SEDM* (Среща на министрите на отбраната от Югоизточна Европа): Включва инициативата за Балкански бригади (*SEEBRIG*) – многонационални мирни сили за бързо реагиране и хуманитарни мисии.

– Инициативата Адриатическа харта (А5): Партньорство под егидата на САЩ, насочено към подпомагане на евроатлантическата интеграция на страните от Западните Балкани.

– Противоминната военноморска група в Черно море (*MCM Black Sea*): Тази инициатива между България, Румъния и Турция е ярък пример за регионално военно сътрудничество. Очаква се то да се задълбочи чрез съвместна охрана на въздушното пространство (*Air Policing*) и изграждане на обща инфраструктура по източния флаг на НАТО, без това да изисква нов отделен договор извън пакта. Сътрудничеството между страните се надгражда чрез разширяване на обхвата на съвместната инициатива посредством изменение на Меморандума за разбирателство. Към задачите на военноморска група се включват наблюдение и разузнаване в подкрепа на защитата на критичната подводна инфраструктура. По този начин *MCM Black Sea* се утвърждава като пример за подобряване на регионалното сътрудничество от противоминни действия към изпълнение на по-широк спектър от задачи, свързани със защитата на стратегически обекти и повишаването на устойчивостта на Черноморския регион.[4]

В бъдеще може да се очаква задълбочаване на взаимоотношенията и създаването на по-дълбоки връзки между участниците, така че да може да се ангажира и акумулира съществен ресурс за поддържане и развитие, без вече да е необходимо самите участници да продължават да включват допълнителни пакети огромни ресурси.

Развитието на двустранните и многостранните споразумения, както и задълбочаването на военно-техническото сътрудничество се утвърждават като основен инструмент за повишаване на отбранителните способности и модернизацията на отбранителната индустрия. Тази тенденция е особено характерна за държавите с ограничени ресурси, които трудно могат самостоятелно да изградят пълния спектър от необходими отбранителни способности. В тази връзка Люцканов отбелязва, че „малките държави, в системата на глобализирано ресурсно осигуряване и невъзможност да изградят самостоятелна ефикасна система за защита на ценностите и интересите си, са принудени да развиват съюзни. (...) Сериозното предизвикателство за тези държави е дефинирането на непреходните национални ценности, формиране на интереси и тяхното интегриране в приетите съюзни такива“ (Lyutskanov 2017, p. 30).

В този смисъл в Югоизточна Европа е започнало формирането на специфична мрежа от регионални инициативи и партньорства, която е своеобразен „съюз в съюза“. Тези съюзи не може да се каже, че заместват съществуващите механизми за колективна отбрана, а ги допълват чрез реализиране на съвместни проекти в направление изграждане на общи способности в области от взаимен интерес.

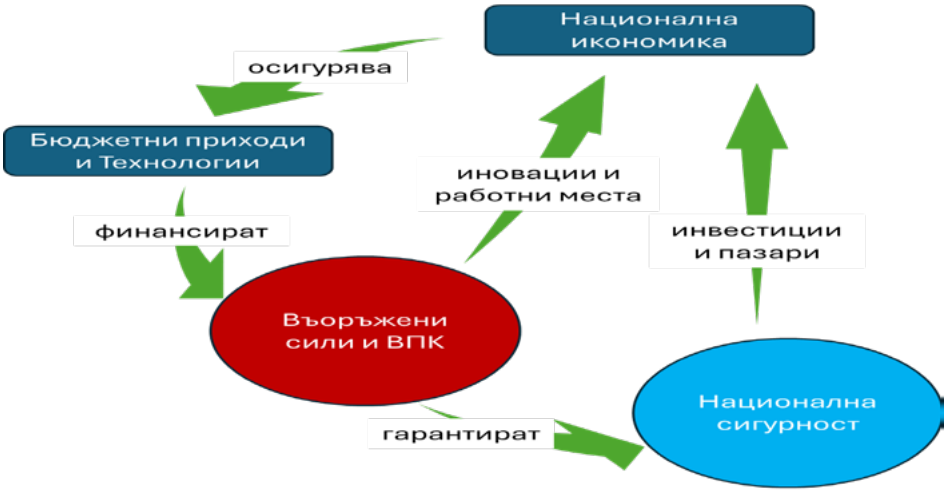
Основавайки се на историческата препратка, може да се направи изводът, че и съвременните съглашения имат потенциала да въвлекат отделни страни в определена нежелана конфронтация било то на икономическо равнище или в локален военен конфликт поради нерешени или задълбочаващи се негативно взаимоотношения, следва да се уточни, че към момента те се разглеждат само като сътрудничещи страни.

Следва да се разгледат и обединенията в името на определена кауза, която да бъде в интерес на участващите страни, така че да се облекчи икономическата тежест. Разбира се, трябва да се разглежда и възможността не само от военна, но и от икономическа полза. От друга страна, следва да се отчете и фактът от придобиването и развитието на нови развойни дейности, които активно влияят върху качеството на разработените продукти и повишаване на отбранителните способности.

Чрез повишаване на отбранителните способности тежестта върху икономиката започва да се балансира и подобрява. Тази взаимовръзка се разглежда по средния начин икономиката като фундамент на отбраната и сигурността и те като гарант за икономически растеж.

Историческият опит показва, че развитието на подобни съюзни формати следва да бъде съпътствано от ясно дефинирани цели, балансирани национални интереси и ефективни механизми за координация. При липса на подобен баланс съществува риск от възникване на политически, икономически или военни противоречия, които биха могли да окажат негативно въздействие върху регионалната сигурност. Към настоящия момент обаче разглежданите инициативи имат предимно кооперативен характер и са насочени към повишаване на регионалната устойчивост. Освен с ползите във военната сфера, тези форми на сътрудничество притежават и ясно изразен икономически ефект. Обединяването на финансови, индустриални и научно-технологични ресурси позволява реализирането на съвместни проекти, намаляването на разходите за разработване и придобиване на нови способности, както и ускоряването на иновационните процеси в отбранителната индустрия. Именно взаимодействието между отбранителното сътрудничество, икономическата ефективност и технологичното развитие формира същността на военно-икономическата симбиоза, която стои в основата на съвременните микросъюзи.

Симбиозата *отбрана – икономика* (фигура 1) може да се разгледа най-просто в схема как те се захранват взаимно във времето. В основата си това е непрекъснат цикъл: икономиката произвежда ресурси за отбраната, а отбраната произвежда сигурност, за да може икономиката да расте.



Фигура 1. Симбиоза *отбрана – икономика*

Тези взаимовръзки се разглеждат и следят, като заложените индикатори и фактори следва да бъдат разгледани индивидуално за всяка една ситуация, така че да гарантира в голяма степен на актуалността на придобитата информация. Следенето най-малко на развитието и поддържането на отбранителните способности, както и възможностите за взаимодействие и съвместимост на въоръжените сили е един от факторите, които определят готовността за отразяване на възможните рискове за сигурността и тяхното снижаване до относително поносими степени.

Развитието на отбранителните способности и военния потенциал се реализира чрез два основни подхода:

– Модернизиране на съществуващите системи въоръжение и техника;

– Придобиване на нови, технологично усъвършенствани въоръжение и техники.

Изборът и реализирането на упоменатите подходи зависи от финансовите възможности на държавата, състоянието на отбранителна индустрия, равнището на технологично развитие и стратегическите приоритети в областта на сигурността и отбраната. Когато националните ресурси са недостатъчни за усъвършенстване на военния потенциал, е наложително да се търсят възможности за участие в съвместни програми, двустранни споразумения и регионални формати на сътрудничество, чрез които компенсират слабостите в националните отбранителни способности.

Средата за сигурност „…може да бъде застрашена не само от надпревара във въоръжаването, международно военно и икономическо господство, но също така и от непреките стратегии за разубеждаване и икономически форми на отмъщение, като например ембарго и бойкоти“ (Dimitrov, Tsvetkov 2015, p. 92).

Променящата се среда за сигурност през последните 5 години в глобален мащаб и ускорените процеси на модернизация във военната сфера поставят държавите пред необходимостта от непрекъснато развитие на техните отбранителни способности. Обаче възможностите на държавите от Балканския полуостров, които са членове на НАТО, за реализиране на подобни програми не са еднакви. Докато едни държави разполагат с необходимия финансов, индустриален и технологичен капацитет (като Турция и Гърция), други са ограничени от наличието на достатъчни финансови и ресурсни фактори, които възпрепятстват самостоятелното изграждане и поддържане на исканите отбранителни способности. Именно тези ограничения формират предпоставките за задълбочаване на регионалното сътрудничество и за изграждането на различни форми на микросъюзи, основани на споделяне на ресурси, технологии и отбранителни способности. В основата на тези ограничения стои дефицитът на военно-промишлен капацитет (фигура 2), който се проявява в три взаимосвързани направления: материално-финансово, времево-технологично и научно-информационно. Взаимодействието между тях определя възможностите на отделните държави за развитие на собствена отбранителна индустрия, производство на въоръжение и реализиране на дългосрочни програми за модернизация.

Анализът на стратегическите дефицити на **военно-промишлен капацитет** се описват, както следва:

На първо място: Материално-финансови ограничения

Съвременните отбранителни технологии изискват огромен финансов ресурс, който надхвърля просто цената на придобиване. Пълният жизнен цикъл на техниката (поддръжка, логистика, модернизация) често е трикратно по-скъп. Икономически слабите държави се сблъскват с липсата на възможността за мащабен преглед – те поръчват ограничени количества, което оскъпява единичната продукция. Налице е и суровинен (ресурсен) дефицит, тъй като производството на компоненти зависи от вериги за доставка на редки земни елементи или специфично оборудване (компоненти), често ограничени и в разположение на малко доставчици.

На второ място: Времеви и технологични зависимости

Времето е критичен невъзстановим ресурс. Производственият ка-

пацитет на глобалните производствени компании е ангажиран за години напред, създавайки т.нар. *опашки за изчакване*, през които купуващата държава се намира в стратегически вакуум и уязвимост. Технологичната пропаст се задълбочава от липсата на базово научно ноу-хау и от загубеното за въвеждане в експлоатация време. Придобиването на готови системи без достъп до софтуерния им изходен код превръща техниката в „черупка“ – купувачът остава трайно зависим от външна инженерна и софтуерна поддръжка.



Фигура 2. Дефицитът на военно-промишлен капацитет

На трето място: Научно-информационен (базиран на човешки капитал и информация)

Всяка съвременна отбранителна система изисква обучен персонал за управление и поддръжка. Демографските кризи и застаряването на населението ограничават наличния мобилизационен и експертен потенциал. Накрая – съвременната прецизна техника е безполезна без информацион-

на свързаност. Липсата на собствени способности и информационна среда принуждава държавите да разчитат на чужди данни за ранно предупреждение, насочване и разузнаване.

Обобщение, което следва да се направи, е, че комбинацията от тези дефицити в съвременната епоха показва, че абсолютният отбранителен суверенитет за по-малките държави е практически недостижим. Включването в многостранни съюзи (като НАТО) или сключването на двустранни и тристранни споразумения за отбрана не е просто политически избор, а структурна необходимост. Посредством тях държавите компенсират собствената си ресурсна безпомощност чрез споделяне на способности, съвместно подпомагане при изпълнението на задачи по линия на сигурността и осъществяване на интегриран обмен на данни.

Второстепенният преглед на средата за сигурност в съвременния свят и концепцията за „пълен суверенитет“ е илюзия за малките държави, което обуславя и осмисля защо те са структурно и ресурсно принудени да търсят коалиционна сигурност.

Основният проблем при създаването на тези споразумения е, че съществуват сериозни структурни, културно-исторически и военно-политически бариери пред разрастването, които много често включват:

– неразрешени двустранни спорове – създаване на нови разделителни линии;

– налагането на ограничения/санкции – използването на надправителствени организации и институции;

– етнически и вътрешнополитически напрежения – неразрешена вътрешнополитическа поляризация и ориентация;

– различни скорости на развитие – създават се правни пречки за икономическа и правно-нормативна интеграция.

Икономическата полза от подобни споразумения следва ли да надделее над политическите и историческите пречки в съответния регион, или следва да се разглежда само като фокус върху средата за сигурност към определен период от време, без да е налице рамката от неразрешените проблеми?

Този тип формати предлага гъвкавост, която липсва при крупните международни организации и предлага основните възможности да се концентрират в няколко направления:

– Сигурност и отбрана – засяга основно споделянето на разузнавателна информация, съвместни военни учения и координиране на отбранителните документи за повишаване на оперативните способности. Сътруд-

ничество в развитието на ВПК, институционална подкрепа в изграждането на нови способности и логистика.

– Икономическа интеграция – създаване на условия за засилване на търговските взаимоотношения чрез намаляване или премахване на мита, създаване на общи пазари за стоки и услуги, предлагане на общи продукти от ВПК.

– Инфраструктурна свързаност – създаване на общи енергийни проекти и осъществяването на различни линии на комуникация.

– Допълнителна подкрепа – за отстояване на намеренията пред различни надправителствени организации за постигане на национални или съюзни цели.

– Съвместимост – покриване на единни стандарти при различни системи и оперативна съвместимост. Това означава, че различни продукти, системи или процеси са проектирани по еднакви правила, за да работят заедно безпроблемно.

– Скритост – постигане на конфиденциалност на определени типове изделия, които следва да са отнесени за определен тип и брой контрагенти.[5]

Двустранните и тристранните споразумения (микросъюзи) между държави със сходни стратегически интереси са мощен инструмент за регионална военно-политическа среда за сигурност. Тези държави споделят обща визия и цели за оказване на влияния в регионален аспект, както и поддържане на високо икономически сътрудничество за гарантиране на средата за сигурност.

Изграждането им стои върху основите на културно-историческите взаимоотношения и върху икономическите необходимости. Технологичното развитие дава невъзможността за размяна на ноу-хау и постигане на нови възможности за съвместна развойна дейност, така че да отговаря на изискванията на страните по договора. Изгодата следва да се разглежда като равна за всяка една от страните, като същите споделят положителните и отрицателните качества на системата по равно.

Синергията, която носят тези съюзи, и потенциалът, който се получава, базиран на фактора време, дава възможност на страните да планират процесите и да разполагат с изделията в точно определен етап, така че да отговаря на изискванията за допопълване, заменяне на съществуващите системи. Което от своя страна гарантира едно планово постъпване и опериране на системите, гарантиращо сигурност в системата за доставка и осигуряващо така необходимото спокойствие в средата за сигурност.

Добавянето на нови контрагенти и впоследствие включването на допълнителни участници дори и за отделни производствени мощности единствено дава така необходимото ноу-хау и „богатство“ на производствения цикъл, което от своя страна разширява портфолиото и възможните контрагенти. Разглеждайки тези възможности, е напълно вероятно и възможно съществуващите към момента микросъюзи да стигнат до момента, когато ще достигнат своите цели и ще бъде необходимо да се включат допълнителни „играчи“, за да се поддържа тяхната конкурентоспособност и да бъдат икономически оправдани.

Микросъюзите ще продължат да се образуват и да съществуват, като оказват съществено изменение в съвременната средата за сигурност. Динамиката в системата за сигурност се преформатира от кумулативния натиск на противоположни тенденции, фактори и изисквания, произтичащи от средата.

Основаните индикатори остават икономическото обвързване и ресурсен капацитет, както и възможностите на военно-промишлената производствена мощност за осигуряване и регулиране на основните контрагенти, влияещи в процеса по генериране на средата за сигурност.

Средата за сигурност ще остане в състояние, което ще подлежи на постоянен натиск и ще се усуква под напъна на развитието на технологичните приложения в различните домейни и нововъведения във военно-технологичната област.

Като основен източник за сключването на тези договорки се характеризират разходите за енергията, персонал, време, комуникации, логистика и ресурсната осигуреност. Спецификите на редките материали и възможностите на военни технологии и иновации, които се предлагат за включване в производството на определения артикул, носят своята добавена стойност и способност за съвместимост в дадената система за сигурност.

Знанието за създаването и производството на изделията, веднъж предадени в производствения цикъл, дават възможност за постигане на голяма степен на автоматизация в процеса изграждане. Така, от друга страна, необходимостта от ангажиране на специализиран работен персонал отпада като критерии за гарантиране на производствената среда. Внедряването на автоматизирани системи и системи за изкуствен интелект напълно подпомагат процесите по безпроблемно протичане на производствения цикъл.

Стремежът към сътрудничество в различните сегменти и снижаване на потенциалния натиск, произтичащ от различните регламенти и системи, е една добра основа за поддържането на тези процеси. Вплетено с иде-

ологическите виждания и разбирания, напълно допълва картината и дава една стабилна основа за изграждане на подобен тип взаимоотношения.

Включването в различни програми и договорености ще продължи да бъде на дневен ред дори и погледнато през приеманата на предходни системи и образования ще заема голямо място в бъдещите микрообразования с една основна цел – намаляване на разходите и постигане на съвместимост на системата.

БЕЛЕЖКИ

1. Национална отбранителна стратегия. София, 2016, с. 6

2. Национална отбранителна стратегия. София, 2025, с. 10

3. Военните операции и действия се провеждат в пет оперативни домейна: сухопътен, морски, въздушен, кибер и космически. Оперативните домейни предоставят структурна рамка за групиране на военни и невоенни способности и представляват обособени сфери за провеждане на военни операции и действия в рамките на оперативното пространство.

4. Вестник Българска армия, бр. 27 от 10.07.2026, с. 3

5. ГАНЕВ, Милен, 2026. САЩ разкриха тайна фабрика за ИИ дронове в Германия. *Факти* [online] [12.07.2026]. Available from: https://fakti.bg/world/1067014-sasht-razkriha-taina-fabrika-za-ii-dronove-v-germania

6. Стратегия за национална сигурност на Република България, обн., *ДВ*, бр. 26 от 23.03.2018 г.

7. *НП-01 Доктрина на въоръжените сили на Република България*, изд. Б, С, 2025, с. 33

8. ВЛАДИМИРОВ, Владимир, 2025. Заплаха ли са новите военни съюзи на Балканите. *BGLOBAL* [online] [last viewed 03.07.2026]. Available from: https://bglobal.bg/112904-zaplaha-li-sa-novite-voenni

9. БРАЙ, Томас, 2025. Нови военни съюзи на Балканите: Колко опасно е това?. *DW* [online] [last viewed 16.06.2026]. Available from: https://www.dw.com/bg/novi-voenni-suzi-na-balkanite-kolko-opasno-e-tova/a-72200278

10. Свободна Европа, 2025. Ще има ли отбранителен съюз между Хърватия, Албания и Косово. *Свободна Европа* [online] [last viewed 10.06.2026]. Available from: https://www.svobodnaevropa.bg/a/harvatia-albania-kosovo-otbrana-sarbia-balgaria-nato/33355120.html

ЛИТЕРАТУРА

ЛЮЦКАНОВ, Е.И., 2017. Изграждане на адаптивни стратегии за национална сигурност в глобализиращия се свят. *Юридически сборник*, том XXIV с. 28 – 38.

ДИМИТРОВ, Д.; ЦВЕТКОВ, Ц., 2014. Икономическа сигурност, кризи и среда за иновации в сектора за сигурност и отбрана. *Годишник на УНСС*, № 1, с. 87 – 126. DOI: https://doi.org/10.37075/YB.2014.1.03.

REFERENCES

LYUTSKANOV, E.I., 2017. Izgrazhdane na adaptivni strategii za natsionalna sigurnost v globalizirashtia se svyat. *Yuridicheski sbornik*, tom XXIV s. 28 – 38 [in Bulgarian].

DIMITROV, D.; TSVETKOV, Ts., 2014. Ikonomicheska sigurnost, krizi i sreda za inovatsii v sektora za sigurnost i otbrana. *Godishnik na UNSS*, № 1, s. 87 – 126. DOI: https://doi.org/10.37075/YB.2014.1.03 [in Bulgarian].

MICRO-ALLIANCES – MILITARY-ECONOMIC SYMBIOSIS IN THE SECURITY ENVIRONMENT

Abstract. This report examines the impact of the modern security environment on the formation and development of micro-alliances as a tool for enhancing defence capabilities and regional sustainability. The interrelationship between military cooperation, economic opportunities and the development of the defense industry is analyzed and the historical experience and the development of the processes of interaction between the countries of the Balkan Peninsula is studied. Emphasis is placed on the problems of military-industrial capacity, expressed in resource, technological and scientific-expert aspects. It is concluded that the need to overcome these deficits stimulates the creation of micro-alliances based on sharing resources, industrial capacity and technological capabilities, which have become an important element of the modern security architecture.

Keywords: agreements; Alliance; arms accumulation; micro-union; military cooperation; security

Valeri Todorov
ORCID iD: 0009-0003-3815-585X
Land Forces Department
Command and Staff Faculty
Rakovski National Defense College
82, Evlogi and Hristo Georgievi Blvd.
1504 Sofia, Bulgaria
E-mail: v.d.todorov@rndc.bg

https://doi.org/10. 66334/annu26_histodevel

ИСТОРИЧЕСКО РАЗВИТИЕ НА КОНЦЕПЦИЯТА ЗА МИСИЙНОТО КОМАНДВАНЕ

ас. Веселин Георгиев
Национален военен университет „Васил Левски“

Абстракт. В настоящия доклад се разглежда историческото развитие на концепцията за мисийното командване и прилагането на нейните основни принципи в практиката на Българската армия през периода на Балканските войни и Първата световна война. Чрез изследването на архивни документи, оперативни заповеди, дневници и исторически изследвания от Държавния военноисторически архив (ДВИА), се проследяват примери за предоставяне на инициатива, делегиране на правомощия и децентрализирано изпълнение на задачите. Изследването показва, че още преди формалното дефиниране на мисийното командване като съвременна военна концепция, българските командири прилагат редица от неговите принципи при планирането и провеждането на бойни действия. Направен е извод, че историческият опит на Българската армия представлява ценен източник за развитието на съвременната командна култура и за прилагането на мисийното командване в условията на динамична оперативна среда.

Ключови думи: мисийно командване; Auftragstaktik; Балкански войни, Българска армия

Увод

Съвременното командване и управление се нуждае от бързи, адекватни, своевременни и скоростни действия. Подходът, който включва такъв тип динамика е мисийното командване. То поставя акцент върху децентрализацията при вземане на решения и предоставя свобода на действие на подчинените командири. Тази философия насърчава инициативността и отговорността на всички нива на командване, като същевременно запазва единството на усилията и координацията между различните компоненти на силите.

Мисийното командване е концепция използвана във военното дело в познатото ни историческо минало. Според Теоретичните постановки за мисийното командване на Сухопътни войски немалко наши командири ползват концептуалните устои на мисийното командване в периода на национално обединение (1912 – 1928). Присъстват мемоари, биографични бележки, примери и директни формулировки с философията и принципите на представената концепция. Разглежданата историческа справка[1] по въпроса показва че историческото наследство, може директно да се свърже с изконните армейски ценности, нормите на поведение и принципите на командване в периода, когато Българската армия е в своя победен апогей в новото време на нейното съществуване. Концепцията на Сухопътни войски отчита и заляга нуждата от трансформация на организационната култура и за превръщането ѝ в адаптивна развиваща се стратегическа организация, която да е адекватна на съвременните и бъдещи предизвикателства на средата за сигурност.

1. Проявлението на мисийното командване в Българската армия в периода на Балканската война

Особеното при започването на Балканската война във 2-ра армия е, че се дава прекалена свобода на началниците от всички степени да поставят въпросите си, като понякога прескачат различните нива на командване и управление (КиУ). Това се потвърждава от препис от **писмото на Министъра на войната с № 53/211.01.1913 г.** до началника на щаба на Действащата армия (ДА). Дискутираният въпрос, че с обявяването на общата мобилизацията на въоръжените сили на 17 септември 1912 г. се поражда *... една особена двойственост в отправление на службата по военното ведомство, която продължава и до настояще време*. Всички отдели от щаба на ДА отправят искания направо до заместниците на началниците

на отдели в министерство на войната и правят директни разпореждания до намиращите се във вътрешността на Царството войскови части и учреждения, които не влизат в състава на тази армия. Отделно, към тях се обръщат и даже различни началници от разни степени от формирования от състава на армията. Този порядък, понякога помага, но и пречи, защото нарушава принципа на йерархичността в армията. Поради това, се изготвя и Временно положение за КиУ на въоръжените сили (ВС) на царството във военно време.[2]

Поредното илюстриране на прилагането на мисийното командване е извлечено от **дневника на оперативните писма от 8 декември 1912 г. до 2 февруари 1913 г. на Втора армия.** От него се разбира, че при обсада на Одрин към средата на декември 1912 г. обсадната артилерия е отделна част при щаба на армията с началник полк. Загорски, като последната, заедно с полската артилерия, на 18 декември същата година (с. г.) се сливат и се образува артилерията на 2-ра армия, като полк. Загорски си остава командир.[3] От оперативните преписки ясно се наблюдава историческата истина, че постоянно се предоставя свобода на командирите на батареи сами да разполагат част от подчинените си формирования. Като типичен пример за това твърдение може да отбележим как се заповядва на к-н Касифров да разположи наблюдател пункт, от където най-добре може да се вижда разположението на противника, след което да донесе телеграфически в кой голям и малък квадрант в южния или източния участък от източния сектор се намира.[4]

В **резюмето за действията** на нашите и сръбски части около Одрин през 1913 г., като пореден автентичен исторически извор, се разбира друга дедукция от прилагането на мисийното командване. Поради намаляването в рязка степен на войските от сръбската армия заради болни в леко и тежко състояние и евакуирането им за Сърбия, и непостъпването на пресни попълнения, се свежда, че без да се чака решението на Сърбия за допопълване, се прави прегрупиране с цел окомплектоване на тези сектори от обсадата на Одрин, които се нуждаят от това.[5]

От изучаването на **беловите заповеди** на 2-ра армия излизат следващите интересни факти за мисийното командване през този исторически период. От **Заповед по II армия** от 21 януари 1913 г. се разбира за конкретните действия против одринската крепост и близките ѝ околности, в която съществува конкретика за обстрелването ѝ. Въпреки това, от нея си личи до голяма степен свободата, която се дава на командирите на обсадните батарея. Пример е, че през всеки два, до три часа обстрелването може да

се прекъсне за по един, два часа, като през нощта то следва да е по-силно. Вярно е, че е заповядано за всяко оръдие от „бомбандиращите“ батареи да се използват по 50 снаряда в денонощието, но тяхното разпределение за 24-часовия период се оставя в ръцете на командирите на ниските тактически нива. От останалите батареи не трябва да се открива огън с цел неразкриване на местоположението им, а само в крайна необходимост, в случай че противникът съсредоточи силен огън против бомбардиращите батареи, срещу разположението на пехотните части. Тогава огън се открива само по заповед на началника на сектора, когато той прецени, след което се ръководи от началника на артилерията на армията.[6]

Няколко дни буквално преди осъществяването на щурма на Одринската крепост и прилежащата ѝ зона за отговорност , в **оперативните заповеди на щаба на 2-ра армия** се отличава Заповед № 56 от 1 март 1913 година. В нея, съдейки по положението и състоянието на противника в крепостта, командващият на армията **дава само основни разпореждания на началниците на секторите** по отношение на организиране и провеждане на атаката над крепостта. В този документ е записано, че колкото и да искат да скрият основния замисъл за организирането ѝ, противникът преди оставащото време най-вероятно ще се ориентира за замисъла. Затова в заповедта се посочват едва основните моменти по превземането на укрепения район, които се свеждат до: провеждане на решителната атака да е на източния сектор; останалите действия в другите сектори да са също с висока степен на активност с цел да не бъдат пасивно-демонстративни, защото противникът ще разбере, че е въведен в заблуда. Поради това, и в тях следва да се действа решително и енергично, предвид мащабността на операцията, трудността за комуникиране, късното получаване на донесения и заповеди.

Изводът е, че прилагайки основните принципи на мисийното командване, началникът на 2-ра армия издава **директива,** с която цели да ориентира началниците на сектори за предстоящите действия, за да могат те да развият в достатъчна степен нужната инициатива. Въпреки това, че не освобождават началниците на сектори от постоянна комуникация с щаба на армията, както и с тези на съседните сектори, той им дава свобода за реализиране на техните дейности с цел допринасяне на изпълнението на общия план за превземане на този стратегически обект за атака.[7] *Началниците на сектори да имате предвид, че от успешните действия, които предприемате, ще зависи завършването на войната и принуждението противника към мир.*[8]

Обобщавайки гореспоменатите паметни факти и данни за прилагането на мисийното командване в исторически период, могат да бъдат изведени **принципите на мисийното командване, ползвани от нашите предшественици,** които са дефинирани по-надолу в научната разработка.

Първият основен принцип е свързан с инициативността като основа на бойния успех.

В Концепцията за мисийното командване на Сухопътни войски[9] са заложени афоризми на бележити български пълководци. Нашите изявени военноначалници ползват принципите на мисийното командване, без то да бъде определено и заложено като методология.

Проявявай предприемчивост, що сковава свободната дейност на врага. Предприемчивост – способност да действаш самостоятелно, когато нямаш заповеди, съгласно целта и обстановката – Борис Дрангов, Помни войната.[10]

Полковник Дрангов насърчава способността на човек да проявява инициативност, находчивост и готовност да действа, особено когато се появят нови възможности или предизвикателства. Тези качества водят до следното:

– да започваш действия, без да чакаш указания;

– да намираш нови решения и подходи;

– да поемаш отговорност и рискове, когато е необходимо;

– да се приспособяваш към променящи се условия.

Тази инициативност подтиква предприемчивите хора често да виждат проблемите, като възможности и да умеят да превръщат идеите в реалност.

Концепцията акцентира върху свобода на вземане на решение от подчинените, децентрализираното изпълнение и нивата на контрол.

Борис Дрангов отчита динамиката в бойните действия и бавната природа на централизираното командване. Констатира, че командирите на терен имат най-ясна преценка за обстановката и врича тяхната отговорност да действат по правилния начин в името на общата цел:

Когато заповедта не отговаря на обстановката, подчиненият: или предизвиква нова заповед, ако има време, сир.[еч] без да пропусне сгодния миг или да влоши положението си; или пък действа по свой начин за да постигне общата цел… – Борис Дрангов, Помни войната.[11]

Документът разглежда делегирането на правомощия и разпределянето на отговорности по йерархичната стълбица на военното командване. Това допринася до възможност на по-високия ешелон да планира следва-

щите операции в срок, както и да има възможност да обръща внимание към въпросите от особена важност, докато командирите на местността вземат решения в кратки срокове, без нуждата от погледа и преценката на висшия ешелон (Iliev 2019).

Концепцията поставя децентрализирано изпълнение като възможност за реализация на инициативата на командирите изпълнители. Тук се разглежда нуждата и ефекта от подготовката за проявяване на тази способност. Засегнат е моралът и етичните норми на поведение, като фактор, определящ самостоятелното вземане на решения, ценен репер в обстановката на липса на информация или динамично променящата се среда. Определя се нуждата да се поддържа инициативата в рамките на намерението на командира, като се поддържа точният темп и интензивност на бойните действия:

... във време на самия бой, началникът [...] мъчно може да управлява бързо и своевременно действията на своите части. Неприятелската стрелба е тъй силна, свръзките повечето пъти са прекъснати, обстановките бързо се менят, тъй че почти всичко зависи от дейността на по-долните началници, които непосредствено водят борбата. Та моята главна задача е била именно да подготвя подчинените си части към сериозна борба; [...] командирите от разни степени за проявяване на инициатива... – Владимир Вазов, *Животописни* белеоюки.[12]

Така представеният исторически пример осветява необходимостта от промяна нивата на контрол вследствие на променената обстановка и поставените цели за реализация.

Вторият принцип е **доверие, споделено разбиране и подготовката на подчинените командири.**

В[ъв] всички бойни войски, в[ъв] всички времена, любовта, доверието, взаимната преданост на началници към войници и на войници към началници твореха безсмъртни дела – Борис Драгнов, Помни войната.[13]

Тук се вменява нуждата от вече притежаваща способност за вземане на решения. Обръща се внимание на командния климат, екипната работа, на споделеното разбиране и взаимното доверие (Iliev 2011). Регламентира се мисийния тип заповеди, при който фокусът е върху целта на операцията. Конкретното изпълнение на задачите се оставя на командирите на ниските нива. Тук се дава свободата на действие, дори като необходимо състояние.

На следващо място е **компетентността.**

Принципите на военното дело са малко и прости. Но военният занаят е обширен и сложен. От пълководеца се искат дълбоки и разнообразни

знания. Който мисли, че без знания може да воюва, прави си една опасна илюзия, за която се плаща – Георги Вазов, *Завет към армията.*[14]

От думите на Георги Вазов се вижда, че свободата на действие не означава отсъствие на подготовка и контрол. Напротив, проявата на инициатива е възможна само при наличие на необходимите знания, опит и умения за правилна оценка на обстановката. Мисийното командване предполага високо ниво на професионална подготовка, знания и способност за правилна оценка на обстановката. Следователно, компетентността се явява основна предпоставка за успешното прилагане на концепцията (Iliev 2011).

Четвъртият принцип се свежда до прилагането на **мисиен тип заповеди.**

В заповедта посочвай: какво знаеш за неприятеля и съседите; главно – целта (какво, а не как); *задачите на отделните части; мерки за разузнаване, охрана, наблюдение, свръзка, разпознаване; снабдяване с припаси; превързочно място и де ще бъдеш сам, та по-леко да командваш, управляваш, водиш, въодушевяваш и по-добре да наблюдаваш.*

Що именно от изброеното ще влезе в заповедта, зависи всякога от обстоятелствата – Борис Драгов, Помни войната.[15]

Посочените исторически пouки напълно съответстват на съвременното разбиране за мисиен тип заповеди, при които командирът определя крайната цел и желаното състояние, а начинът за постигането им се оставя на преценката на подчинените. Така се създават условия за инициативност и адаптивност в динамична бойна среда.

Не на последно място, **поемането на риск** се отличава като пети принцип на мисийното командване.

На война не е тъй важно, що правиш, както как го правиш – победата зависи повече от дързостта и упорството, отколкото от изкусните кроежи. Нерешителността и бездейността влекат по-тежка отговорност, отколкото грешките в избора на средствата, щом незабавно ги приведеш в действие – Борис Драгов, Помни войната.[16]

При бързо променяща се обстановка забавянето на решенията често води до по-сериозни последици от евентуално допуснатите грешки. Поради това, концепцията насърчава командирите да действат решително в рамките на намерението на старшия началник.

Става ясно, че проявата на необходимата квалификация за ползване на мисийното командване е прекомерно и целенасочено. Българската армия инвестира в развитието на своите командни кадри въз основата на принципите на мисийното командване. Според книгата на автора Дими-

тров, свързана с историята на военното училище, военното обучение на курсантите от самото създаване на военноучебното заведение се развива посредством издигане на качества в обучаемите като правдивост, честност, мъжество и решителност. Проявяването на творческа инициативност, смело вземане на правилни решения, които да се налагат твърдо и неотклонно, са водещи мотиви във военнообразователната система (Dimitrov 1981, p. 68).

2. Исторически корени на мисийното командване в европейската военна практика

Според редица статии, засегнали тематиката, мисийното командване се разглежда като философия на командването, концепция, подход, аспект на маневрения подход, вид командване, команден метод и т.н.

Изследвайки историческите сведения извън българския опит в сферата на европейската военна наука, се доказва, че този тип командване се използва в тактическите действия още в Пруската война, но разглеждайки неговите принципи, се оказва прилаган от лидерите, военноначалниците и пълководците от древни времена.

Така например, началникът на Пруския генерален щаб Хелмут фон Молтке (1800 – 1891) използва метод, който буквално преведен на български език, означава тактика на мисията *(Auftragstaktik)*[17] и представлява децентрализирано изпълнение на подробното предварително планиране. Според него, след осъществяването на първия контакт с противника всяко едно планиране вече не отговаря на действителността.

Той вярва, че по време на една кампания командирите трябва да вземат решения въз основа на променлива ситуация. Неговите виждания са, че командирите трябва да вземат нови решения според постоянно променящата се обстановка. Динамичните промени в боя имат лавинообразен ефект, всяка нова ситуация поражда друга такава. Това от своя страна изисква проявата на гъвкавост от страна на командирите. Той вижда смисъл в делегирането на правомощия на подчинените командири, като всички те се съобразяват с намерението на старшия. Военният теоретик вижда ползите в това тактическите решения да се вземат на място и полага усилия в насърчаването на командирите на всички нива да започнат да го правят. Молтке продължава да развива концепцията си в това направление, че старшите командири трябва да дават общи инструкции, да издават най-важните заповеди. Според него успехът, който може да постигне един лидер

с постоянна намеса и контрол е илюзорен, дори се стига до момент, в който подчинените нямат реалната възможност да изпълнят редица заповеди на командира. Визията на Молтке е въведена в германския полеви регламент от 1888 г., след което стават част от практиката на германската армия.[18]

Заключение

От проведеното историческо изследване по темата се стига до основния извод, че принципите на мисийното командване не са непознати за българската и европейската военна теория и практика. Изследваните архивни документи и исторически свидетелства ни показват, че още през периода на Балканските войни българските командири прилагат успешно подходи, основани на инициативност, доверие, делегиране на правомощия и ориентиране към изпълнение на поставената цел. Макар концепцията за мисийното командване да придобива завършен теоретичен облик значително по-късно, нейните основни характеристики могат да бъдат открити в командната практика на редица български военноначалници.

Анализът сочи, че редица принципи на съвременната концепция имат своите корени в българската военна традиция и са успешно прилагани от нашите командири още в началото на XX век. Това създава благоприятни предпоставки за възприемането и развитието на мисийното командване в съвременните Сухопътни войски, като същевременно укрепва връзката между историческия опит и актуалните изисквания на оперативната среда.

През XXI век, мисийното командване продължава да бъде актуално, въпреки технологичния напредък. Макар, че иновациите позволяват централизация на командването, децентрализираните подходи, като мисийното командване, запазват предимството си. Бойната среда остава доста хаотична и непредсказуема, затова доверието, експертизата и широкият опит са нужни постулати за положителното провеждане на бойните действия. Ефективността на новите технологии все още зависи от добрата комуникация, координация и синхронизация, които са цел за въздействие на противостоящата страна.

БЕЛЕЖКИ

1. За нуждите на доклада е направено проучване в рамките на няколко дни в Държавния военноисторически архив със седалище в гр. Велико Търново. По време на историческото изследване са анализирани повече от 50 архивни единици от различни описи на няколко архивни фонда (дела).

2. ДВИА, ф. 317, оп. 7, а. е. 44, л. 65, 66; а. е. 78, л. 41, 42.

3. ДВИА, ф. 317, оп. 7, а. е. 46, л. 1, 2.

4. ДВИА, ф. 317, оп. 7, а. е. 46, л. 6.

5. ДВИА, ф. 317, оп. 7, а. е. 47 л. 1.

6. ДВИА, ф. 317, оп. 7, а. е. 44, л. 61; а. е. 78, л. 39.

7. ДВИА, ф. 317, оп. 7, а. е. 44, л. 70, 71; а. е. 78, л. 43, 44, 45, 46.

8. ДВИА, ф. 317, оп. 7, а. е. 78, л. 47.

9. Командване на сухопътните войски, 2023. Теоретични постановки (Концепция) за мисийното командване и стратегия за неговото прилагане в Сухопътните войски. София: Командване на сухопътните войски.

10. Пак там, с. 9.

11. Пак там, с. 12.

12. Пак там, с. 13.

13. Пак там, с. 17.

14. Командване на сухопътните войски, 2023. Теоретични постановки (Концепция) за мисийното командване и стратегия за неговото прилагане в Сухопътните войски. София: Командване на сухопътните войски, с. 18.

15. Пак там, с. 25.

16. Пак там, с. 31.

17. Auftragstaktik (на немски: auftrag – задача, taktik – тактика) е метод на командване и делегиране, при който командирът дава на подчинените си ясно определена цел, основни детайли като времева рамка и необходимите ресурси за изпълнение на задачата. Подчинените имат свобода да решават как да постигнат целта самостоятелно.

18. Командване на сухопътните войски, 2023. Теоретични постановки (Концепция) за мисийното командване и стратегия за неговото прилагане в Сухопътните войски. София: Командване на сухопътните войски, с. 3.

19. Mission Command: Command and Control of Army Forces. Army Doctrine Publication (ADP 6-0). Headquarters Department of the Army Washington, D.C., 31 July 2019.

ЛИТЕРАТУРА

ДИМИТРОВ, И., 1981. *ВНВУ „Васил Левски“ – страници из историята на училището.* София: Военно издателство.

ИЛИЕВ, Н., 2019. Влияние на ролята на информацията върху процеса по управлението на войските в боя. В: *Годишник на НВУ „Васил Левски“,* ч. II, с. 189 – 194. Велико Търново: НВУ „Васил Левски“. ISSN 1312-6148.

ИЛИЕВ, Н., 2011. Към проблема за вземането на решение при анализ на източниците и достоверността на информация. В: *Сборник доклади от годишната университетска научна конференция на НВУ „Васил Левски“*, [23 – 24 юни 2011], том 7, с. 184 – 191. Велико Търново: НВУ „Васил Левски“. ISSN 1314-1937.

REFERENCES

DIMITROV, I., 1981. *VNVU „Vasil Levski“ – stranitsi iz istoriyata na uchilishteto.* Sofia: Voenno izdatelstvo. [In Bulgarian].

ILIEV, N., 2019. Vliyanie na rolyata na informatsiyata varhu protsesa po upravlenieto na voyskite v boya. In: *Godishnik na NVU „Vasil Levski“,* part II, pp. 189 – 194. Veliko Tarnovo: NVU „Vasil Levski“. ISSN 1312-6148. [In Bulgarian].

ILIEV, N., 2011. Kam problema za vzemaneto na reshenie pri analiz na iztochnitsite i dostovernostta na informatsia. In: *Sbornik dokladi ot godishnata universitetska nauchna konferentsia na NVU „Vasil Levski“*, [23 – 24 yuni 2011], vol. 7, pp. 184 – 191. Veliko Tarnovo: NVU „Vasil Levski“. ISSN 1314-1937. [In Bulgarian].

HISTORICAL DEVELOPMENT OF THE MISSION COMMAND CONCEPT

Abstract. This report examines the historical development of the concept of mission command and the application of its core principles within the Bulgarian Army during the Balkan Wars and World War I. Through an analysis of archival documents, operational orders, diaries, and historical studies from the State Military Historical Archives (DVIA), the study traces examples of granting initiative, delegating authority, and the decentralized execution of tasks. The research demonstrates that, even prior to the formal definition of mission command as a modern military concept, Bulgarian commanders applied a number of its principles when planning and conducting combat operations. The study concludes that the Bulgarian Army's historical experience serves as a valuable resource for the development of modern command culture and the implementation of mission command within a dynamic operational environment.

Keywords: mission command; Auftragstaktik; Balkan Wars; Bulgarian Army

Veselin Georgiev, Assist. Prof.
Department of Military Science
Faculty of Security and Defence
Vasil Levski National Military University
76, Bulgaria Blvd.
5000 Veliko Tarnovo, Bulgaria
E-mail: vggeorgiev@nvu.bg

https://doi.org/10. 66334/annu26_geopolitsec

ГЕОПОЛИТИЧЕСКИ ИЗМЕРЕНИЯ НА СТРУКТУРНИТЕ ПРЕДИЗВИКАТЕЛСТВА ПРЕД СИГУРНОСТТА НА ЕВРОПЕЙСКИЯ СЪЮЗ

Виктория Вутова
Военна академия „Георги Стойков Раковски“

Абстракт. Европейският съюз все по-отчетливо губи позициите си на един от основните центрове на сила в променящата се геополитическа среда. Технологичното и ресурсното изоставане, превъоръжаването без собствена индустриална база и надпреварата в изкуствения интелект оставят Съюза зад САЩ и Китай и го поставят в двойна зависимост едновременно от двете сили. Брюксел отговаря с нови правила, общо финансиране и рекордни разходи за отбрана. Тези мерки обаче не премахват зависимостта, а често я заменят с нова. Това поставя под въпрос стремежа на ЕС към стратегическа автономност.

Ключови думи: геополитика; двойна зависимост; Европейски съюз; сигурност; стратегическа автономност; структурни предизвикателства

I. Увод

Методите на конфронтация между глобалните играчи се променят и придобиват нови измерения. Международните отношения и геополитическата значимост на новите актьори също се променят. Някои от промените следват дългогодишни тенденции, които претърпяват изместване на фокуса, докато други се раждат от разрушителни нови технологии, радикално променящо се поведение или разрушителните резултати от човешката дейност.[1]

Технологиите на Четвъртата индустриална революция все повече се използват за създаване на нови оръжия, някои от които променят правилата на бойното поле. Хибридните заплахи се увеличават, включително чрез използване на мигранти, фалшиви новини и тактики за намеса в изборите. Геоикономиката и геополитиката вече не могат да се разглеждат като отделни сфери, а Европа постепенно губи статуса си на един от основните центрове на сила във формиращия се многополюсен свят (Artamonova, Demchuk 2026, pp. 35 – 36).

Световната геополитика се променя. Традиционно ангажирани с ролята на гарант на геополитическия ред, Съединените щати сега са по-съсредоточени върху въпросите на вътрешната политика, отколкото върху външната политика.[2] Това оттегляне позволява възхода на други глобални сили, като Китай, който се конкурира и споделя ролята на световен лидер със САЩ. Сред тези промени ЕС започва да мисли за собствената си защита и да осъзнава значението на укрепването на общите отбранителни способности и геоикономическите инструменти.

Всички тези аспекти доказват промяна на парадигмата на сигурността, което изисква спешни действия от страна на ЕС. За да бъде конкурентоспособен в новата геополитическа среда, Съюзът се нуждае не само от нови правни и регулаторни рамки, но и от правилно отчитане на индустриалната си зависимост от чужди държави и от обединяване на ресурси за съвместно развитие на граждански и военни технологии с „двойна употреба“. На теория държавите членки могат да бъдат по-силен, по-сигурен и водещ глобален играч, като действат заедно. Глобализацията, миграцията, геополитическата динамика и променящата се природа на инструментите на силата обаче издигнаха уязвимостта до нови нива, което прави тази задача истинско предизвикателство за Съюза.

Целта на разработката е да анализира структурните предизвикателства пред сигурността на ЕС и да оцени доколко отговорите на Съюза намаляват неговата уязвимост като оценка на настоящото положение, а не

като прогноза. Защитаваната теза е, че тези предизвикателства поставят ЕС зад САЩ и Китай и го правят зависим едновременно и от двете страни. Тази двойна зависимост се проявява в технологиите, ресурсите, отбраната и изкуствения интелект. В стремежа си към самостоятелност Съюзът не премахва зависимостите си, а ги заменя с нови.

Обект на изследването е Европейският съюз като субект в областта на сигурността. Предмет са геополитическите измерения на структурните предизвикателства пред неговата сигурност. Под това се разбира как тези предизвикателства влияят на позицията на ЕС спрямо САЩ и Китай и на свободата му да действа самостоятелно.

Изследването се основава на анализ на официални документи на ЕС и НАТО, статистически данни, научни публикации и аналитични доклади, на съпоставяне на данни за ЕС, САЩ и Китай, както и на индукция и дедукция, обработка и обобщение на данни.

Ограниченията на изследването са свързани с времевия обхват и с обхвата на предмета. Анализът обхваща периода 2024 – 2026 г., а голяма част от разгледаните решения на ЕС са в начален етап на изпълнение, поради което оценката на ефекта им е предварителна.

II. Структурни предизвикателства пред сигурността на ЕС

Под структурни предизвикателства се разбират дълбоки и дългосрочни проблеми в икономическата, технологичната и отбранителната основа на ЕС, които не могат да бъдат преодолени бързо или с отделни мерки. Текстът разглежда три направления: технологичното и ресурсното изоставане; превъоръжаването и отбранителната зависимост; изкуствения интелект. Те са подбрани по критерия доколко засягат способността на ЕС да действа като самостоятелен субект в областта на сигурността.

2.1. Технологично и ресурсно изоставане

Един от най-устойчивите структурни дефицити на ЕС е изоставането в научноизследователската и развойната дейност. През 2024 г. Съюзът инвестира в нея 403 млрд. евро, но интензитетът остава 2,2% от БВП.[3] Това е далеч от целта от 3%. За сравнение САЩ отделят 3,45%[4], а Китай – 2,8%.[5] Едва четири от петдесетте водещи технологични компании в света са европейски (Draghi 2024, p. 14). Европа продължава да иновира в индустриите на XX век, но отсъства от тези, които ще определят баланса на силите през XXI век. Дори автомобилният сектор, традиционно най-силният в Европа, вече е под натиск. След като през 2024 г. ЕС въвежда допълнителни

изравнителни мита до 35,3% върху китайските електромобили, вносът се пренасочва към хибридните автомобили. Той нараства от около 3800 броя през октомври 2024 г. до 50 000 през юли 2026 г. През септември 2026 г. Съюзът моли Китай „доброволно“ да ограничи износа им до около 15% от европейския пазар, а европейски представител определя подхода като „управлявана търговия“.[6] Фактът, че ЕС трябва да моли, а не да определя условията дори в собствения си водещ отрасъл, е показателен за отслабването на неговите позиции.

Изоставането се превръща в зависимост от материалната основа на съвременната икономика. Между 75 и 90% от световния капацитет за производство на полупроводникови пластини е в Азия (Draghi 2024, p. 16), а делът на ЕС в световното производство на чипове ще нарасне едва от 9,8% до 11,7% вместо заложените 20%.[7] ЕС внася от Китай всичките си тежки редкоземни елементи и 98% от магнитите от редкоземни елементи.[8] Те са необходими едновременно за електромобилите, за вятърните турбини и за въоръжението.

Тази зависимост вече се използва като лост. През април и октомври 2025 г. Пекин въвежда лицензионен режим за износа на редкоземни елементи и магнити.[9] След като през септември 2025 г. нидерландското правителство поема временен контрол над производителя на чипове *Nexperia*, Китай забранява износа на произвежданите там компоненти. Европейската асоциация на автомобилните производители предупреждава за „критичен“ недостиг на основни микрочипове.[10]

Същата логика се наблюдава и в енергетиката. На 26 януари 2026 г. Съветът окончателно приема поетапна забрана за внос на руски газ. Тя важи за втечнения газ от началото на 2027 г., а за тръбопроводния – от есента на 2027 г.[11] Така зависимостта, използвана като инструмент за натиск през 2022 г., се премахва законодателно, но за сметка на нови зависимости. Европа вече зависи от вноса на втечнен газ от САЩ и от китайските технологии и суровини за възобновяемата енергия. Колко уязвима е тази позиция, показва есента на 2026 г. На 9 октомври 2026 г. президентът Тръмп обявява договореност с Путин за доставка на общо около 3 млн. тона руски дизел за американския и световния пазар, а Министерството на финансите на САЩ издава временно разрешение в отклонение от санкциите срещу Русия.[12] Докато ЕС законодателно се отказва от руските енергийни източници, неговият основен нов доставчик сам облекчава санкциите срещу Москва. Решението е взето без участието на Европа. Това поставя Съюза в парадоксална ситуация: следвайки собствените си принципи, той се отказ-

ва да купува пряко от Русия, но плаща по-висока цена за втечнения газ от американски доставчици, отколкото е плащал за доставките по тръбопровод, в момент, в който самите САЩ отварят пазара си за руско гориво. Така европейските бюджети се утежняват, без реално да намаляват приходите на Москва.

Оттук следва изводът, че технологичното и ресурсното изоставане на ЕС е проблем не само на конкурентоспособността, а и на сигурността. Европа се оказва в зависимост, която върви в две посоки и не е взаимна. Съюзът зависи от Китай за суровини, базови компоненти и технологии за възобновяемата енергия, а от САЩ за втечнен газ, както и за цифровите технологии, разгледани в т. 2.3. Нито една от двете сили обаче не зависи в същата степен от него, с изключение на отделни ниши като литографското оборудване. В условията на съперничество между Вашингтон и Пекин това излага Съюза на натиск и от двете страни, без да разполага със съпоставими собствени средства за противодействие.

2.2. Превъоръжаване и отбранителна зависимост

Епохата без големи междудържавни войни в Европа приключи. Успоредно с това се променят и трансатлантическите отношения. Стратегията за национална сигурност на САЩ от декември 2025 г. предупреждава за „цивилизационно заличаване“ на Европа, поставя под въпрос значението на трансатлантическата връзка за американската сигурност и изразява подкрепа за националистическите движения в Европа.[13] Американското изтегляне от Европа налага нова концепция за реформа на Съюза (Veselinov 2025). Въпросът дали европейската сигурност ще се изгражда със или без НАТО (Melnikova 2022) престава да бъде теоретичен.

Отговорът е безпрецедентно превъоръжаване. На срещата на върха в Хага през юни 2025 г. съюзниците от НАТО се ангажират до 2035 г. да отделят 5% от БВП. От тях 3,5% са за основни отбранителни нужди, а до 1,5% за устойчивост и инфраструктура.[14] ЕС приема плана „Превъоръжаване на Европа/Готовност 2030“ (*ReArm Europe/Readiness 2030*), който позволява до 800 млрд. евро допълнителни разходи, и инструмента „Действия за сигурността на Европа“ (*SAFE*) със заеми до 150 млрд. евро за съвместни поръчки, а разходите на държавите членки за отбрана нарастват от 343 млрд. евро през 2024 г. до около 381 млрд. евро през 2025 г.[15]

Превъоръжаването променя и отношенията между държавата и гражданите. Военната служба се завръща: в Германия от 1 януари 2026 г. всички мъже, родени след 2008 г., подлежат на задължителна регистрация

и медицински преглед, като целта е армията да достигне 460 000 души до средата на 2030-те години.[16] Френското министерство на здравеопазването нарежда на болниците да бъдат готови да приемат хиляди ранени военни при „голям ангажимент“[17], а Литва разработва план за евакуация на Вилнюс, в който един от основните маршрути води към Полша.[18] Това, което допреди няколко години беше немислимо за Европейския съюз като „проект за мир“, днес е част от обичайното държавно планиране.

Тази мобилизация протича преди всичко на национално равнище. Келемен и Макнамара обясняват това с факта, че ЕС е изграден чрез пазарите, а не чрез войни и затова разполага със силен регулаторен, но слаб фискален и принудителен капацитет (Kelemen, McNamara 2022). Инструменти като *SAFE* едва започват да запълват тази празнина. Концепцията за „стратегическа автономност“ се разглежда като път към „геополитическа Европа“ (Varma 2024), но примерът с превъоръжаването показва колко трудно е тя да бъде постигната на практика.

Тук се очертава своеобразен „парадокс на превъоръжаването“: стремежът към стратегическа автономност чрез *SAFE* и „Превъоръжаване на Европа“ не премахва зависимостта, а я възпроизвежда в нова форма. Между средата на 2022 г. и средата на 2023 г. 78% от разходите на държавите членки за отбранителни поръчки отиват при доставчици извън ЕС, от които 63% в САЩ (Draghi 2024, p. 8). САЩ осигуряват и 58% от вноса на основни оръжейни системи на европейските държави от НАТО през периода 2021 – 2025 г.[19] *SAFE* изисква поне 65% от стойността на финансираните системи да бъде произведена в ЕС, Европейското икономическо пространство или Украйна.[20] В най-технологично интензивните сегменти, като бойните самолети, противовъздушната отбрана, разузнаването и сателитната комуникация, европейска алтернатива в близък срок няма. Дори въоръжението, произведено в Европа, зависи от външни суровини: европейските ракети, сред които и ракетата „въздух – въздух“ *Meteor*, използват редкоземни елементи в системите за насочване и управление, а те се внасят почти изцяло от Китай.[21] Колкото по-бързо протича превъоръжаването при недостатъчен собствен производствен капацитет, толкова по-голяма става зависимостта от външни доставчици. На първо място това са САЩ, чиято ангажираност към европейската сигурност е все по-несигурна.[22]

Това има пряко стратегическо значение. Историческият опит показва, че изходът от продължителните конфликти между големи сили се определя не толкова от първоначалната военна мощ, колкото от способността за устойчиво военно-индустриално производство. Войната в Украйна

потвърждава, че в конфликт на изтощение решаващи са производството на боеприпаси, темпът на възстановяване на техниката и сигурността на доставките. Следователно при евентуален въоръжен конфликт стратегическо предимство ще има онзи, който контролира производството на въоръжение, а не онзи, който го закупува. Така и в отбраната ЕС е притиснат между двете сили: купува американско оръжие, а суровините за собственото си производство внася от Китай. В този смисъл в стремежа си към самостоятелност ЕС остава структурно зависим – без собствена отбранителна индустриална и технологична база превъоръжаването увеличава военните му възможности, но не и свободата му на действие.

2.3. Изкуствен интелект

Изкуственият интелект се превръща в една от основните области на съперничество между великите сили. Военните му приложения – от анализа на разузнавателни данни до автономните системи, ще определят баланса на силите в следващите десетилетия. В тази надпревара Европа изостава значително. През 2025 г. в САЩ са създадени 59 значими модела на изкуствен интелект, в Китай – 35, а дори Южна Корея има 8. Европа е представена едва с 2 модела – един френски и един английски.[23]

Китай показва, че е способен да навакса бързо. През януари 2025 г. китайската компания *DeepSeek* представя модел, чието разработване по нейни данни струва едва 5,6 млн. долара. В рамките на един ден пазарната стойност на американския производител на чипове *Nvidia* спада с близо 600 млрд. долара.[24] Така изкуственият интелект се развива в два центъра на сила, а Европа остава извън тях.

Изоставането се превръща в зависимост от САЩ. Три американски компании контролират над 65% от европейския пазар на облачни услуги, а около 70% от базовите модели на изкуствения интелект след 2017 г. са разработени в САЩ (Draghi 2024, p. 24). Тази зависимост също може да се използва като лост. През януари 2025 г. САЩ въвеждат правило за износа на усъвършенствани чипове за изкуствен интелект. Според него само десет държави членки получават неограничен достъп, а останалите седемнадесет попадат в категория с ограничения.[25] Макар правилото да е оттеглено през май 2025 г., то показва, че достъпът на европейските държави до ключова технология може да бъде определян едностранно във Вашингтон.

САЩ и Китай разглеждат изкуствения интелект като ключов елемент от националната си сигурност и са го включили в стратегиите си за отбрана. Зависимостта достига и до самата отбрана. През март 2025 г.

НАТО придобива системата *Maven Smart System* на американската компания *Palantir*. Тя дава на командващите инструменти с изкуствен интелект за обединяване на разузнавателни данни, определяне на цели и планиране на операциите.[26] Така дори ключови военни способности на Алианса в Европа разчитат на американски технологии.

Още в Бялата книга от 2020 г. Европейската комисия заявява целта ЕС да стане лидер едновременно в иновациите и в регулирането на изкуствения интелект.[27] Шест години по-късно Съюзът е постигнал второто, но не и първото. Отговорът му остава преди всичко регулаторен. Законът за изкуствения интелект (Регламент (ЕС) 2024/1689) въвежда подход, основан на степента на риска.[28] Съюзът обаче сам отстъпва от част от тази амбиция. С пакета „Цифров омнибус“ задълженията за високорисковите системи се отлагат до декември 2027 г., съответно – август 2028 г.[29] Това е косвено признание, че регулацията изпреварва възможностите на собствената индустрия. Планът „Континент на изкуствения интелект“ от април 2025 г. цели да мобилизира 200 млрд. евро, от които 20 млрд. за т.нар. гигафабрики.[30] Усилието е значимо, но остава далеч от мащаба на частните инвестиции в САЩ.

Дори в регулирането ЕС не е единственият, който определя правилата. Китай също регулира активно тази област и я подчинява на собствените си стратегически цели. Пречка са и различните интереси на държавите членки и фрагментираният процес на вземане на решения. Затова влиянието на ЕС в глобалното управление на изкуствения интелект остава ограничено в сравнение със САЩ и Китай. ЕС ще трябва да оцени доколко неговото управление на изкуствения интелект отговаря на нормативните му идеали и европейските ценности, без да изостава още повече в технологичната надпревара.

Следователно в областта на изкуствения интелект ЕС разполага със сила да създава правила, но не и със собствена технология. И тук Европа зависи от двете сили едновременно. Моделите, облачната инфраструктура и най-мощните чипове са американски, а суровините и компонентите, без които този хардуер не може да се произведе, идват от Китай и Азия. Така ЕС рискува да регулира технологии, от които все повече зависи и отбраната му, без да контролира тяхното създаване.

III. Заключение

Войната действа като ускорител на историята. Днес светът е изправен пред нарастващата опасност от разпространение на кризисни ситуации и ескалация в различни региони. През последните двадесет години в света

настъпиха мащабни промени, които преобърнаха реда за сигурност в Европа. В резултат на тях Европейският съюз се отказа от първенството на своята политика на „мека сила“ и започна активно да се преустройва на геополитическа основа.

Разгледаните предизвикателства не са нови, но през последното десетилетие придобиват ясно геополитическо измерение. Превъоръжаването на Европа се ускорява след украинската криза и достига безпрецедентни мащаби през 2025 г. Всяка нова криза кара ЕС да реагира, но отговорите му остават предимно нормативни и финансови, докато собственият му производствен и технологичен капацитет се изгражда бавно.

Геополитическите последици могат да бъдат обобщени в три посоки. Първо, ЕС губи позиция. От един от центровете на сила в многополюсния свят той все повече се превръща в пространство между САЩ и Китай и вече не може да определя условията дори в собствените си водещи отрасли. Второ, зависимостите му се превръщат в лостове за натиск. Пекин ги използва чрез ограниченията за редкоземни елементи и чипове, а Вашингтон чрез контрола върху технологиите и енергийните доставки. Решения, които пряко засягат европейската сигурност, все по-често се вземат без участието на Европа. Трето, стеснява се свободата на действие на Съюза. Който купува оръжието си отвън и зависи от чужди суровини и технологии, трудно може да води самостоятелна външна политика и политика за сигурност.

В стремежа си към самостоятелност ЕС не се освобождава от зависимостите си, а само ги пренасочва. Ако тази тенденция продължи, Съюзът рискува да се превърне от самостоятелен геополитически субект в обект на съперничеството между другите сили. Изходът зависи от това дали държавите членки ще успеят да превърнат общите средства в собствена индустриална и технологична база, преди следващата криза отново да покаже цената на зависимостта.

Използване на AI

Авторът декларира, че е използвал изкуствен интелект като помощно средство за проверка и подреждане на източниците и за сверяване на статистическите данни и фактите в текста.

БЕЛЕЖКИ

1. National Intelligence Council, 2021. *Global Trends 2040: A More Contested World*. Washington, D.C.: National Intelligence Council

2. RAPP, L., 2025. Trump’s new national security strategy: Cut deals, hammer Europe, and tread gently around autocrats. *Chatham House* [online]. Available from:

https://www.chathamhouse.org/2025/12/trumps-new-national-security-strategy-cut-deals-hammer-europe-and-tread-gently-around

3. Eurostat, 2025. *EU spending on R&D exceeded €403 billion in 2024*. News release, 4 December 2025

4. OECD, 2025. *Main Science and Technology Indicators*. Paris: OECD.

5. National Bureau of Statistics of China, 2026. China's R&D investment exceeded 3.92 trillion yuan in 2025. *The State Council of the PRC*, 5 March 2026

6. QUARTZ, 2026. E.U. asks China to voluntarily cap hybrid car exports. *Quartz* [online]. Available from: https://qz.com/eu-china-hybrid-car-export-cap-trade-war-091726

7. European Court of Auditors, 2025. *The EU's strategy for microchips.* Special report 12/2025. Luxembourg: European Court of Auditors

8. SZCZEPAŃSKI, M., 2025. *China's rare earth export restrictions*. EPRS At a Glance, 24 November 2025. Brussels: European Parliamentary Research Service.

9. SZCZEPAŃSKI, M., 2025. *China's rare earth export restrictions*. EPRS At a Glance, 24 November 2025. Brussels: European Parliamentary Research Service.

10. Euronews, 2025. European carmakers warn of supply shocks as Nexperia halts chip exports to China. *Euronews* [online]. Available from: https://www.euronews.com/business/2025/10/31/european-carmakers-warn-of-supply-shocks-as-nexperia-halts-chip-exports-to-china

11. Council of the European Union, 2026. *Russian gas imports: Council gives final green light to a stepwise ban.* Press release, 26 January 2026

12. RAVID, B., 2026. Trump announces major diesel deal with Putin, infuriating Ukraine. *Axios* [online]. Available from: https://www.axios.com/2026/10/09/trump-putin-diesel-agreement-ukraine-war

13. RAPP, L., 2025. Trump's new national security strategy: Cut deals, hammer Europe, and tread gently around autocrats. *Chatham House* [online]. Available from: https://www.chathamhouse.org/2025/12/trumps-new-national-security-strategy-cut-deals-hammer-europe-and-tread-gently-around

14. NATO, 2025. *Defence expenditures and NATO's 5% commitment*. Brussels: NATO.

15. Council of the European Union, 2025. *European defence readiness*. Brussels: Council of the European Union

16. Deutschland, 2026. Germany's new military service explained. *Deutschland* [online]. Available from: https://www.deutschland.de/en/topic/politics/new-military-service-bundeswehr

17. Euronews, 2025. France preparing hospitals to care for war-wounded soldiers by March 2026. *Euronews* [online]. Available from: https://www.euronews.com/video/2025/09/02/france-preparing-hospitals-to-care-for-war-wounded-soldiers-by-march-2026

18. KNews, 2026. Lithuania develops evacuation plan for possible war scenarios. *KNews* [online]. Available from: https://knews.media/2026/09/19/lithuania-develops-evacuation-plan-for-possible-war-scenarios

19. SIPRI, 2026. *Trends in International Arms Transfers, 2025.* SIPRI Fact Sheet, March 2026. Stockholm: Stockholm International Peace Research Institute

20. Euronews, 2025. Everything you need to know about SAFE, the EU's €150bn defence instrument. *Euronews* [online]. Available from: https://www.euronews.com/2025/05/21/everything-you-need-to-know-about-safe-the-eus-150bn-defence-instrument

21. HINTERMAYER, N.; HMAIDI, A., 2025. China's rare-earths export controls hit EU rearmament – but open a strategic window. *Merics* [online]. Available from: https://merics.org/de/comment/chinas-export-controls-hit-eu-rearmament-open-strategic-window

22. RAPP, L., 2025. Trump's new national security strategy: Cut deals, hammer Europe, and tread gently around autocrats. *Chatham House* [online]. Available from: https://www.chathamhouse.org/2025/12/trumps-new-national-security-strategy-cut-deals-hammer-europe-and-tread-gently-around

23. STANFORD HAI, 2026. *The 2026 AI Index Report.* Stanford: Institute for Human-Centered Artificial Intelligence, p. 17.

24. ABC7 NEWS, 2025. Bay Area-based Nvidia loses nearly $600B in market value following rise of Chinese AI app DeepSeek. *ABC7 News* [online]. Available from: https://abc7news.com/post/nvidia-news-chinese-artificial-intelligence-app-called-deepseek-sends-us-stocks-plunging/15841290

25. Law Society Gazette, 2025. Tougher US AI chip-export rules concern EU. *Law Society Gazette* [online]. Available from: https://www.lawsociety.ie/gazette/top-stories/2025/january/tougher-us-ai-chip-export-rules-concern-eu

26. NATO Communications and Information Agency, 2025. NATO acquires AI-enabled warfighting system. *NATO Communications and Information Agency* [online]. Available from: https://www.ncia.nato.int/newsroom/news/nato-acquires-aienabled-warfighting-system

27. European Commission, 2020. *White Paper on Artificial Intelligence: A European approach to excellence and trust*. COM(2020) 65 final. Brussels, 19 February 2020

28. European Parliament and Council, 2024. Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, L, 12.7.2024

29. LONG, William RM; RIGHINI, Elisabetta, BLYTHE, Francesca, 2026. EU lawmakers reach provisional agreement to delay key EU AI Act obligations. *Sidley* [online]. Available from: https://datamatters.sidley.com/2026/06/22/eu-lawmakers-reach-provisional-agreement-to-delay-key-eu-ai-act-obligations

30. European Commission, 2025. *AI Continent Action Plan*. COM(2025) 165 final. Brussels, 9 April 2025

ЛИТЕРАТУРА

АРТАМОНОВА, Ю.Д.; ДЕМЧУК, А.Л., 2026. Европа в контексте мегатенденций современного мирового развития. *Актуальные проблемы Европы*, № 1 (129), с. 21 – 40. DOI: 10.31249/ape/2026.01.02.

ВАРМА, Т., 2024. Европейската стратегическа автономия: Пътят към геополитическа Европа. *Геополитика*, год. XXI, бр. 4, с. 132 – 149.

ВЕСЕЛИНОВ, И., 2025. Тръмпизмът, путинизмът и новият световен ред. *Геополитика*, год. XXII, бр. 2, с. 110 – 114.

МЕЛНИКОВА, Ю., 2022. В търсене на оптималната архитектура на европейската сигурност: ЕС, с или без НАТО? *Геополитика*, год. XIX, № 2, с. 60 – 76.

DRAGHI, M., 2024. *The future of European competitiveness. Part A: A competitiveness strategy for Europe*. Brussels: European Commission.

KELEMEN, R.D.; McNAMARA, K.R., 2022. State-building and the European Union: Markets, War, and Europe's Uneven Political Development. *Comparative Political Studies*, vol. 55, no 6, pp. 963 – 991. Available from: https://doi.org/10.1177/00104140211047393.

REFERENCES

ARTAMONOVA, Yu.D.; DEMCHUK, A.L., 2026. Evropa v kontekste megatendentsiy sovremennogo mirovogo razvitia. *Aktualynie problemi Evropi*, no 1 (129), pp. 21 – 40. DOI: 10.31249/ape/2026.01.02 [in Russian].

DRAGHI, M., 2024. *The future of European competitiveness. Part A: A competitiveness strategy for Europe*. Brussels: European Commission.

KELEMEN, R.D.; McNAMARA, K.R., 2022. State-building and the European Union: Markets, War, and Europe's Uneven Political Development. *Comparative Political Studies*, vol. 55, no 6, pp. 963 – 991. Available from: https:/doi.org/10.1177/00104140211047393.

MELNIKOVA, Yu., 2022. V tarsene na optimalnata arhitektura na evropeyskata sigurnost: ES, s ili bez NATO? *Geopolitika*, vol. XIX, no 2, pp. 60 – 76 [in Bulgarian].

VARMA, T., 2024. Evropeyskata strategicheska avtonomia: Patyat kam geopoliticheska Evropa. *Geopolitika*, vol. XXI, no 4, pp. 132 – 149 [in Bulgarian].

VESELINOV, I., 2025. Trampizmat, putinizmat i noviyat svetoven red. *Geopolitika*, vol. XXII, no 2, pp. 110 – 114 [in Bulgarian].

GEOPOLITICAL DIMENSIONS OF THE STRUCTURAL CHALLENGES TO THE SECURITY OF THE EUROPEAN UNION

Abstract. The European Union is increasingly losing its position as one of the main centres of power in a changing geopolitical environment. Its technological and resource lag, rearmament without its own industrial base and the race in artificial intelligence leave the Union behind the United States and China and place it in a dual dependence on both powers at once. Brussels' responses – new rules, joint funding and record defence

spending – do not eliminate this dependence but often replace it with a new one, which calls into question the EU's pursuit of strategic autonomy.

Keywords: double dependence; European Union; geopolitics; security; strategic autonomy; structural challenges

Viktoriya Vutova, PhD Student
Rakovski National Defence College
82, Evlogi and Hristo Georgievi Blvd.
Sofia, Bulgaria
E-mail: v.g.hristova@rndc.bg

https://doi.org/10. 66334/annu26_vliizkecon

ВЛИЯНИЕ НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ ВЪРХУ ИКОНОМИКАТА И ОТБРАНАТА

д-р Владислав Василев
Медицински университет – Плевен

Абстракт. Изкуственият интелект се утвърждава като една от най-значимите и динамично развиващи се области на съвременните информационни технологии. Нарастването на достъпността му, особено на езиковите модели, постепенно го превръща от тясно специализирана технология в инструмент, който може да започне да влияе върху най-различни обществени и стратегически дейности и области. Икономиката и отбраната, като две основни области, са тясно преплетени да подпомагат способността на държавата да издържа и да противодейства на различни кризи. Влиянието, което изкуственият интелект, оказва върху тях, зависи от начина, по който те ще бъдат използвани и интегрирани, като същевременно се предоставят нови възможности и рискове.

Ключови думи: езикови модели; изкуствен интелект; икономика; киберсигурност; отбрана; човешки контрол

1. Увод

Изкуственият интелект се утвърждава като една от технологиите с най-съществено влияние върху развитието на съвременното общество. Той обхваща създаването на компютърни системи, способни да изпълняват задачи, традиционно свързвани с човешката интелигентност – обучение, разсъждение, разпознаване на закономерности, решаване на проблеми и използване на естествен език. В развитието на изкуствения интелект се разграничават различни подходи, сред които символният, основан на правила и логически зависимости, и конекционисткият, свързан с развитието и обучението на изкуствени невронни мрежи.[1]

Развитието на невронните мрежи, машинното обучение и обработката на естествен език създава предпоставки за появата на съвременните големи езикови модели. Те са способни да обработват значителни обеми текстова информация, да откриват зависимости в нея и да генерират съдържание в отговор на зададени инструкции. Техните възможности включват обобщаване и анализ на информация, превод, подготовка на документи, работа с програмен код и подпомагане на различни аналитични дейности.

Способността на езиковия модел да създава убедителен отговор обаче не означава непременно разбиране на съдържанието по начин, сравним с човешкия. Поради това резултатите от подобни системи следва да бъдат подлагани на критична оценка и проверка особено когато се използват в области, в които грешките могат да доведат до значими икономически, организационни или стратегически последствия.

Особено значение в този контекст имат икономиката и отбраната. Макар на пръв поглед да представляват различни области, между тях съществува пряка взаимозависимост. Икономическата устойчивост, технологичният капацитет, инвестициите, производствените възможности и наличието на квалифицирани специалисти определят в значителна степен способността на една държава да изгражда и поддържа съвременни отбранителни способности. От своя страна, отбранителните инвестиции, научноизследователската дейност и развитието на технологии с двойна употреба могат да оказват влияние върху икономическата активност, иновациите и развитието на нови технологични сектори.

Навлизането на изкуствения интелект допълнително засилва тази връзка. В икономиката изкуственият интелект може да подпомага анализа на данни, управлението на бизнес процеси, прогнозирането и автоматизирането на отделни дейности. В отбраната сходни технологични способ-

ности могат да бъдат използвани при обработката на информация, киберсигурността, логистиката, подготовката на документи и подпомагането на процесите по вземане на решения.

В този контекст особено значение придобива човешкият контрол. В рамките на настоящата разработка той се разбира като запазване на възможността и отговорността на компетентния специалист да проверява, оценява и при необходимост да отхвърля резултатите и препоръките, генерирани от система с изкуствен интелект. Ролята на изкуствения интелект се разглежда преди всичко като подпомагаща, а не като заместваща човешката преценка.

Целта на настоящия доклад е да се анализира влиянието на изкуствения интелект и по-конкретно на големите езикови модели върху икономиката и отбраната, като се разкрият както специфичните им приложения, така и взаимовръзките между двете области.

Основната теза е, че влиянието им върху икономиката и отбраната има взаимосвързан характер: икономическото и технологичното развитие създават условия за изграждане на съвременни отбранителни способности, докато внедряването на изкуствения интелект в отбраната стимулира технологични решения, компетентности и иновации с потенциално по-широко икономическо приложение.

2. Влияние на изкуствения интелект върху икономиката

Икономическото значение на изкуствения интелект се определя не само от възможността за автоматизиране на отделни задачи, но и от способността му да променя начина, по който организациите обработват информация, използват ресурсите си и вземат решения. В този смисъл изкуствения интелект може да бъде разглеждан едновременно като технологичен инструмент и като фактор, който влияе върху производителността, конкурентоспособността и структурата на икономическата дейност.

Авторите Challoumis и Eriotis разглеждат въздействието на изкуствения интелект върху икономическия растеж, заетостта, производителността и конкурентоспособността. Според техния анализ по-широкото внедряване на изкуствения интелект може да допринесе за повишаване на икономическата ефективност, но резултатите зависят от равнището на технологично развитие, инвестициите, инфраструктурата и готовността на икономическите сектори да възприемат новите технологии (Challoumis, Eriotis 2025).

Следователно самото наличие на тази технология не гарантира положителен икономически ефект. Необходими са цифрова инфраструктура, достъп до изчислителни ресурси, капитал и квалифицирани специалисти. Недостатъчната технологична готовност може да ограничи положителните резултати и да увеличи различията между организации и държави, които имат различен достъп до необходимите ресурси.

На равнището на отделното предприятие машинното обучение позволява анализиране на икономическата среда и подпомага управлението на ресурсите. Barati Bagherabad, Rivandi и Javid Mehr разглеждат приложения като прогнозиране на търсенето, оценяване на риска, управление на цените, анализиране на въздействието на икономически промени и оптимизиране на ресурсите (Barati Bagherabad, Rivandi, Mehr 2026).

Големите езикови модели разширяват тези възможности чрез способността си да обработват неструктурирана информация. Значителна част от икономическата дейност е свързана с договори, отчети, нормативни документи, кореспонденция, пазарни анализи и клиентски запитвания. Езиковите модели могат да подпомагат обобщаването и систематизирането на подобна информация и да ускоряват подготовката на документи и анализи.

Особено важен е въпросът доколко теоретичните възможности на езиковите модели вече се превръщат в реални икономически промени. Massenkoff и McCrory правят разграничение между това, което големите езикови модели технически могат да извършват, и действителното им използване в професионална среда. За целта те предлагат показател за „наблюдавана експозиция“, който съчетава теоретичната способност на езиков модел да подпомага дадена задача с реалните данни за неговото използване (Massenkoff, McCrory 2026).

Резултатите показват, че реалното приложение все още е значително по-малко от технически възможното. Сред професиите с висока експозиция са програмисти, служители в обслужването на клиенти и оператори за въвеждане на данни. За разлика от тях, професиите, свързани основно с физическа дейност, остават значително по-слабо засегнати. Това показва, че на настоящия етап езиковите модели влияят предимно върху отделни информационни и административни задачи, а не водят автоматично до цялостно заместване на професии.

Същото изследване не установява систематично увеличаване на безработицата сред работещите в професии с висока експозиция, но отчита ранни признаци за по-слабо наемане на млади служители в някои силно изложени професии (Massenkoff, McCrory 2026). Тези резултати следва

да бъдат интерпретирани предпазливо, но показват, че първоначалното въздействие на изкуствения интелект може да се прояви чрез промяна на съдържанието на длъжностите, необходимите умения и начина, по който работодателите организират работните процеси.

Основните икономически рискове са свързани с използването на непроверени резултати, възможни финансови загуби, защитата на фирмените данни и зависимостта от ограничен брой доставчици на модели, облачни услуги и специализиран хардуер.

Тук се отбелязва и връзката между икономиката и отбраната. Разработването на съвременни езикови модели изисква инвестиции, изчислителна инфраструктура, енергийни ресурси, научноизследователски капацитет и квалифицирани специалисти. Същите ресурси са необходими и за внедряването на ИИ в отбранителни системи. Следователно икономическата и технологичната база на държавата определя в значителна степен нейната способност да развива съвременни отбранителни технологии.

3. Влияние на изкуствения интелект върху отбраната

Връзката между икономическото развитие и отбранителните способности става все по-съществена с внедряването на изкуствения интелект. Технологичният потенциал, достъпът до данни, изчислителният капацитет и наличието на квалифицирани специалисти се превръщат едновременно в икономически и стратегически ресурси.

Black разглежда изкуствения интелект като група от технологии с общо предназначение, чието влияние върху отбраната не се определя единствено от техническите характеристики. Според автора резултатът от внедряването на езикови модели зависи от съчетаването на технологични, организационни, социални, културни и доктринални фактори (Black 2026).

Това означава, че една държава може да разполага с модерни системи, но да не успее да ги използва ефективно при липса на подходяща инфраструктура, квалифицирани специалисти и ясни организационни процедури. Достъпът до човешки капитал, данни и изчислителни ресурси постепенно се превръща във фактор за национална и военна конкурентоспособност.

Една от областите с най-пряко приложение на изкуствения интелект/езиковите модели в отбраната е киберсигурността. Съвременните военни, държавни и икономически системи генерират огромни количества информация, която трябва да бъде анализирана в кратки срокове. ИИ може да

подпомага откриването на аномалии, анализирането на зловреден софтуер, разпознаването на фишинг, управлението на уязвимости и реакцията при инциденти (Jadala 2026).

Големите езикови модели имат конкретна подпомагаща функция в този процес. Те могат да участват при анализ на системни дневници, подготовка на доклади, систематизиране на информация за заплахи и подпомагане на специалистите при разследването на инциденти.

Генеративният модел обаче има ясно изразен характер на технология с двойна употреба. Foley разглежда генеративните модели едновременно като средство за защита и като инструмент за осъществяване на атаки. Големите езикови модели могат да подпомагат създаването на персонализирано съдържание за фишинг и социално инженерство, докато защитната страна може да ги използва за откриване на заплахи и оценяване на уязвимости (Foley 2026).

Тази двойна употреба показва, че разпространението им не води автоматично до подобряване на сигурността. Същите технологични възможности могат едновременно да засилят защитата и да предоставят нови средства на нападателите.

Особен риск представлява манипулирането на самите системи, както и генерирането на неточни резултати. При киберсигурността фалшив положителен резултат може да доведе до блокиране на легитимна дейност, а фалшив отрицателен резултат – до пропускане на реална атака. В отбранителна среда подобни грешки могат да имат значителни оперативни последствия.

Поради това внедряването на изкуствен интелект в отбраната трябва да бъде съпроводено от ясни процедури за проверка, управление на риска и човешки контрол. Технологията следва да подпомага специалистите, а не да премахва тяхната отговорност.

4. Взаимовръзка между икономиката, отбраната и изкуствения интелект

Анализът показва, че икономическото и отбранителното приложение на изкуствения интелект не следва да се разглеждат изолирано. Между тях съществува двупосочна зависимост, при която икономическите ресурси и технологичният потенциал създават условия за развитие на отбранителни способности, а потребностите на отбраната стимулират инвестиции, научни изследвания и технологии с по-широко приложение.

Matthews разглежда отбранителната икономика в условията на глобализация и подчертава взаимната зависимост между икономическите възможности, отбранителната индустрия, международните производствени вериги и технологичното развитие (Matthews 2008).

Изкуственият интелект добавя ново измерение към тази връзка. Разработването и внедряването на такива системи изискват високопроизводителни изчислителни ресурси, специализиран хардуер, надеждна цифрова инфраструктура, данни и човешки капитал. Поради това икономическата и технологичната способност на една държава се превръща в предпоставка за нейния капацитет да използва ефективно изкуствения интелект и за целите на отбраната.

Влиянието действа и в обратна посока. Потребностите на отбраната създават търсене на нови технологични решения, киберсигурност, специализиран софтуер и квалифицирани специалисти. Подобни инвестиции могат да стимулират развитието на предприятия и научноизследователски организации, чиито технологии впоследствие намират приложение и извън военната сфера.

Особено значение имат технологиите с двойна употреба. Едно и също решение може да бъде използвано както в гражданската икономика, така и за нуждите на сигурността и отбраната. Това е особено характерно за ИИ, облачните технологии, киберсигурността и анализа на големи информационни масиви.

Тази взаимовръзка обаче не означава, че увеличаването на отбранителните разходи автоматично води до положителен икономически резултат. Tsitouras и Tsounis показват, че ефектът на военните разходи върху икономическия растеж може да бъде различен в краткосрочен и дългосрочен план и да зависи от структурата на самите разходи (Tsitouras, Tsounis 2026).

Когато средствата се насочват предимно към внос на готово оборудване, положителният ефект върху националната технологична база може да остане ограничен. Обратно, инвестициите в собствен научноизследователски капацитет, местно производство и подготовка на специалисти могат да създадат условия за разпространение на знания и технологии към други сектори.

При използването на изкуствения интелект този въпрос придобива особена актуалност. Държава, която разчита изцяло на външни доставчици на модели, облачна инфраструктура или специализиран хардуер, може да създаде едновременно икономическа и стратегическа зависимост. Следователно технологичната устойчивост и развитието на собствен експертен

капацитет придобиват значение както за конкурентоспособността, така и за националната сигурност.

Киберсигурността е един от най-ясните примери за синхронното влияние на изкуствения интелект върху икономиката и отбраната. Кибератаките могат едновременно да засегнат държавни институции, предприятия, финансови организации и критична инфраструктура. Следователно използването на изкуствения интелект за откриване на заплахи има едновременно икономическо и отбранително значение.

По този начин икономиката и отбраната образуват взаимосвързана система, в която икономическият и технологичният потенциал създават отбранителни способности, а потребностите на отбраната стимулират инвестиции, разработки и нови технологични решения.

5. Човешки контрол и подпомагане на процесите по вземане на решения

Разширяването на приложението на изкуствения интелект/езиковите модели поставя въпроса не само какви задачи могат да бъдат автоматизирани, но и каква трябва да бъде ролята на човека при използването на получените резултати.

В настоящия доклад под човешки контрол се разбира способността и отговорността да се наблюдава функционирането на такава система, да проверява резултатите, да оценява контекста и възможните последствия и при необходимост да коригира или отхвърля предложеното действие.

Tsamados, Floridi и Taddeo разграничават традиционния надзорен контрол от по-развитото взаимодействие между човека и езиковите модели. Възможни са загуба на ситуационна осведоменост, прекомерно доверие в автоматизацията и затруднения при намеса в непредвидени ситуации (Tsamados, Floridi, Taddeo 2025). Поради това ефективният контрол трябва да включва разбиране на ограниченията на системата. Потребителят трябва да знае кога резултатът може да бъде използван и кога е необходима допълнителна проверка.

Особено важно е разграничението между подпомагане на решението и автоматизирано вземане на решение. При първия подход изкуственият интелект обработва информация, идентифицира зависимости и предлага възможни варианти, но окончателната преценка остава при човека. При втория системата самостоятелно определя действието.

В икономиката човешкият контрол е необходим при използването на изкуствения интелект за прогнозиране, анализ на риска и управление

на ресурси. Неточен резултат може да доведе до финансови загуби и неправилни управленски решения. В отбраната необходимостта от човешки контрол е още по-голяма. Изкуственият интелект може да подпомага анализа, киберзащитата и логистиката, но грешен резултат може да засегне критична инфраструктура, националната сигурност или човешкия живот.

Човешкото участие само по себе си обаче не гарантира надеждност. Продължителното използване на автоматизирани системи може да доведе до ситуация, при която операторът приема резултатите без необходимата критична проверка.

Следователно човешкият контрол трябва да бъде осигурен чрез ясни организационни и технически механизми. Необходимо е да бъдат определени задачите, които могат да бъдат автоматизирани, ситуациите, които изискват човешко одобрение, и отговорността при неправилен резултат.

Най-подходящият модел е взаимодействие между тях. Системата предоставя бързина и възможност за обработка на големи информационни масиви, докато човекът запазва контекстуалната преценка, оценката на риска и отговорността за крайното решение.

6. Заключение

Развитието на изкуствения интелект и големите езикови модели постепенно променя начина, по който се обработва информация, анализират се данни и се подпомага вземането на решения. Въздействието върху икономиката и отбраната не следва да се разглежда като два независими процеса.

В икономиката се създават възможности за повишаване на производителността, прогнозиране, оптимизиране на ресурсите и автоматизиране на определени дейности. Реалният ефект обаче зависи от инфраструктурата, инвестициите, човешкия капитал и способността на организациите да интегрират технологията в своите процеси.

В отбраната изкуствения интелект може да подпомага обработването на информация, киберзащитата, логистиката и планирането. Същевременно технологията има характер на средство с двойна употреба и може да бъде използвана както за защита, така и за осъществяване на атаки.

Анализът показва, че синхронното влияние на изкуствения интелект върху икономиката и отбраната се проявява чрез зависимостта от общи ресурси: изчислителна инфраструктура, специализиран хардуер, данни, научноизследователски капацитет и човешки капитал.

От извършения анализ могат да бъдат формулирани следните основни изводи:

Влиянието на изкуствения интелект върху икономиката и отбраната има взаимосвързан характер.

Големите езикови модели имат предимно подпомагаща функция при обработване на информация и подготовка на решения.

Икономическият ефект от изкуствения интелект зависи от начина на внедряване, наличната инфраструктура, инвестициите и квалификацията на специалистите.

В отбраната изкуственият интелект има ясно изразен характер на технология с двойна употреба, която едновременно разширява защитните и нападателните възможности.

Човешкият контрол представлява основен механизъм за управление на риска и за запазване на ясна отговорност при използването на изкуствения интелект.

Технологичната независимост и устойчивост придобиват едновременно икономическо и стратегическо значение.

В заключение, изкуственият интелект следва да бъде разглеждан не само като средство за автоматизация, а като фактор, който постепенно променя взаимовръзката между икономическата мощ, технологичното развитие и отбранителния потенциал. Дългосрочната ефективност на неговото приложение ще зависи от способността технологичните възможности да бъдат съчетани с адекватно управление на риска, подготовка на специалисти, защита на критичната информация и ясно определена човешка отговорност.

БЕЛЕЖКИ

1. COPELAND, B. J., 2026. Artificial Intelligence: Methods and Goals in AI. *Encyclopaedia Britannica* [online] [last viewed 13.10.2026]. Available from: https://www.britannica.com/technology/artificial-intelligence/Methods-and-goals-in-AI

REFERENCES

BARATI BAGHERABAD, Mojtaba; RIVANDI, Elaheh; MEHR, Mahsa Javid, 2026. Machine Learning for Analyzing Effects of Various Factors on Business Economic. *Applied Decision Analytics*, vol. 2, no 1, pp. 41 – 54. DOI: 10.66972/ada2120269.

BLACK, James, 2026. Strategic Implications of Deploying Artificial Intelligence in Defence. – In: RANGELEY, Max; FAIRFAX, Nicholas (eds.) *The Artificial Intelligence Revolution*. Cham: Springer, pp. 299-320. DOI: 10.1007/978-3-032-11814-1_11.

CHALLOUMIS, Constantinos; ERIOTIS, Nikolaos, 2025. The Impact of Artificial Intelligence on the Greek Economy. *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 11, no 3, 100578. DOI: 10.1016/j.joitmc.2025.100578.

FOLEY, Joseph, 2026. The Impact of Generative AI on Cybersecurity: Attack Vectors, Defence Mechanisms, and Fair Representation Learning [Preprint]. *TechRxiv* [online]. DOI: 10.36227/techrxiv.177219990.05668652/v1.

JADALA, Santosh Kumar, 2026. How Artificial Intelligence is Revolutionising Cybersecurity: Challenges and the Future. *Indian Journal of Computer Science and Technology*, vol. 5, no 2, pp. 318 – 326. DOI: 10.59256/indjcst.20260502035.

MASSENKOFF, Maxim; McCRORY, Peter, 2026. Labor Market Impacts of AI: A New Measure and Early Evidence. *Anthropic* [online]. Available from: https://www.anthropic.com/research/labor-market-impacts [13.10.2026].

MATTHEWS, Ron, 2008. Defence and the Economy: An Introduction. – In: TILL, Geoffrey; CHEW, Emrys; HO, Joshua (eds.) *Globalisation and Defence in the Asia-Pacific: Arms Across Asia*. London: Routledge, pp. 133 – 147. DOI: 10.4324/9780203890530-16.

TSAMADOS, Andreas; FLORIDI, Luciano; TADDEO, Mariarosaria, 2025. Human Control of AI Systems: From Supervision to Teaming. *AI and Ethics*, vol. 5, no 2, pp. 1535-1548. DOI: 10.1007/s43681-024-00489-4.

TSITOURAS, Antonis; TSOUNIS, Nicholas, 2026. Guns versus Butter for Economic Growth: A Disaggregated Analysis of the Impact of Military Expenditure. *Humanities and Social Sciences Communications*, vol. 13, article 442. DOI: 10.1057/s41599-025-05580-7.

IMPACT OF ARTIFICIAL INTELLIGENCE ON THE ECONOMY AND DEFENCE

Abstract. Artificial intelligence is becoming one of the most significant and dynamically developing fields of modern information technology. Its increasing accessibility, particularly that of large language models, is gradually transforming it from a highly specialized technology into a tool capable of influencing a wide range of social and strategic activities and domains. The economy and defence, as two fundamental areas, are closely interconnected and contribute to a state's ability to withstand and respond to various crises. The impact of artificial intelligence on these areas depends on how it is used and integrated, while at the same time creating new opportunities as well as new risks.

Keywords: large language models; artificial intelligence; economy; defence; human oversight; cybersecurity

Dr. Vladislav Vasilev
ORCID iD: 0009-0005-4944-1610
Medical university – Pleven
1, Saint Kliment Ohridski St.
5800 Pleven, Bulgaria
E-mail: vladislav_vasilev_bz@outlook.com

https://doi.org/10. 66334/annu26_competintel

FROM COMPETITIVE INTELLIGENCE TO RISK INTELLIGENCE: REFRAMING INTELLIGENCE FOR DECISION ADVANTAGE UNDER UNCERTAINTY

Georgi Dimitrov
University of Agribusiness and Rural Development – Plovdiv (Bulgaria)

Abstract. Competitive Intelligence (CI) established intelligence as a structured organizational capability that transforms relevant information into decision support rather than mere data collection. Drawing on Bernhardt's formulation of intelligence as activity, knowledge, and organizational architecture, this article argues that contemporary conditions of systemic uncertainty, technological disruption, regulatory volatility, and geopolitical instability require an expansion of the paradigm. Competitive Intelligence remains essential, yet its traditional competitor-centric focus is insufficient. The article proposes Risk Intelligence as an integrative capability that links environmental sensing, intelligence analysis, risk interpretation, early warning, and anticipatory decision-making. The evolution from Competitive Intelligence to Risk Intelligence expands the intelligence domain from competitive actors to critical uncertainties and their consequences for organizational decisions. The ultimate objective is Decision Advantage under Uncertainty.

Keywords: competitive intelligence; risk intelligence; strategic intelligence; early warning; decision advantage; dynamic capabilities; organizational sensemaking; enterprise risk management

1. Introduction

Organizations today confront unprecedented volumes of data from digital platforms, open-source intelligence, regulatory systems, market analytics, and internal sensors. Information abundance, however, does not automatically produce better decisions. The central challenge is interpretive: distinguishing signal from noise, recognizing emerging patterns, assessing their implications, and acting before uncertainty crystallizes into irreversible events.

More than two decades ago, Bernhardt (2003) insisted that corporate intelligence must not be confused with market research or generic information services. He conceptualized intelligence as activity, knowledge, and organizational architecture, oriented directly toward strategic decision-making. This distinction remains foundational. The critical question is no longer whether an organization possesses information, but whether it can convert environmental information into understanding that improves the timing and quality of decisions.

This article examines the conceptual progression from Competitive Intelligence to Risk Intelligence. Competitive Intelligence provides the historical and theoretical foundation. Contemporary conditions, however, demand an architecture that encompasses uncertainty, weak signals, internal vulnerabilities, regulatory and technological disruption, and strategic opportunities. The proposed trajectory is:

Competitive Intelligence → Strategic Intelligence → Risk Intelligence → Decision Intelligence → Decision Advantage.

Each stage expands the organizational problem that intelligence is expected to solve without rendering earlier stages obsolete.

2. Competitive Intelligence as Organizational Capability

Bernhardt (2003) conceptualizes Competitive Intelligence through three interdependent dimensions: activity (the cycle of direction, collection, processing, analysis, and dissemination), knowledge (the resulting intelligence products), and organization (the formal architecture that sustains the capability). Intelligence is therefore simultaneously process, product, and organizational system.

Central to this model is the requirement that intelligence answer the managerial “so what?” question. Information acquires value only when it alters understanding; understanding acquires value only when it alters decisions. This principle directly anticipates the contemporary notion of Decision Advantage.

Equally important is the user-driven character of the intelligence process. Intelligence begins with the identification of management's critical information needs, which are then translated into collection and analysis priorities. Herring's Key Intelligence Topics (KIT) framework operationalized this logic by structuring interaction between decision-makers and intelligence professionals (Herring 1999; Francis & Herring 1999). The resulting reversal of the traditional information model is decisive:

Decision requirement → Intelligence requirement → Collection → Analysis → Intelligence product → Decision.

In an era of abundant machine-generated data, the bottleneck shifts from collection to question formulation, prioritization, interpretation, and action.

3. Strategic Early Warning and the Limits of Competitor-Centric Models

Bernhardt identified Strategic Early Warning Systems as a core component of competitive intelligence, designed to detect dynamic developments, construct scenarios, define indicators, and reduce strategic surprise. He explicitly linked early warning to a specialized form of risk assessment, thereby creating a conceptual bridge between intelligence and risk management.

Gilad (2003) further developed competitive early warning as a systematic process for identifying industry change drivers, prioritizing strategic risks, and overcoming managerial blind spots that produce "industry dissonance"—the gap between market realities and corporate strategy.

Yet the traditional competitor-centric focus of Competitive Intelligence is increasingly insufficient. Strategic disruptions now originate in regulatory decisions, geopolitical shifts, technological breakthroughs, cyber events, supply-chain interdependencies, internal control failures, reputational cascades, and unexpected interactions among risks. The central intelligence question therefore expands from "What are our competitors doing?" to "What is changing in the operating environment, what does the change imply for organizational exposure and strategic options, and how rapidly can the organization respond?"

This expanded question defines the domain of Risk Intelligence.

4. From Competitive Intelligence to Risk Intelligence

The distinction can be expressed as follows (table 1):

Table 1.

Dimension	*Competitive Intelligence*	*Risk Intelligence*
Primary object	Competitors and competitive environment	Critical uncertainty and organizational exposure
Core question	What are competitors and markets doing?	What is changing, what does it mean, and what could happen?
Main orientation	Competitive positioning	Anticipation and decision support
Time horizon	Present and near-future competitive developments	Continuous present–future assessment
Main mechanism	Intelligence cycle	Integrated intelligence–risk cycle
Early warning	Competitive threats and opportunities	Emerging risks, opportunities, vulnerabilities, disruptions
Organizational scope	Primarily external/competitive	External + internal + cross-functional
Output	Competitive intelligence product	Risk intelligence product and decision options
Ultimate objective	Competitive advantage	Decision Advantage under Uncertainty

Risk Intelligence does not replace Competitive Intelligence; it embeds it within a broader architecture in which risk becomes a primary interpretive lens. Information becomes strategically relevant only when its potential consequences for objectives, capabilities, assets, or options are understood. The resulting process can be summarized as:

Environmental sensing → Intelligence generation → Risk interpretation → Early warning → Decision options → Anticipatory action → Organizational learning.

5. Key Risk Intelligence Topics and the Problem of Interpretation

The KIT framework can be extended into Key Risk Intelligence Topics (KRITs). A KRIT is defined as a strategically significant uncertainty, development, vulnerability, or emerging condition whose evolution may materially affect organizational objectives, risk profile, strategic options, or decision-making.

Whereas a conventional KIT might ask "What is Competitor X planning?", a KRIT asks "What emerging technological, regulatory, geopolitical, operational, or competitive developments could materially alter our strategic risk profile over the next 12 – 24 months?"

The interpretive challenge intensifies with the volume and velocity of contemporary signals. A useful sequence is:

Indicator → Signal → Pattern → Interpretation → Risk significance → Decision relevance.

An isolated indicator is rarely meaningful. Patterns acquire significance only through contextual interpretation linked to organizational exposure. This process aligns closely with organizational sensemaking, understood as the ongoing construction of plausible images that rationalize experience and enable action (Weick 1995; Weick, Sutcliffe & Obstfeld 2005).

Information superiority, in this view, is not technological access to more data. It is the organizational capacity to understand relevant information faster and convert that understanding into timely action (Dimitrov 2026a).

6. Architecture, Dynamic Capabilities, and an Extended Intelligence Cycle

Risk Intelligence functions as an integration layer rather than a new isolated department. It connects Competitive Intelligence, Strategic Intelligence, Enterprise Risk Management, early warning, counterintelligence, compliance and security intelligence, and decision support.

The architecture can be conceptualized in five interconnected layers:

1. Environmental sensing and weak-signal detection (OSINT, market and regulatory monitoring, internal data, AI-enabled anomaly detection);

2. Intelligence integration and sensemaking;

3. Risk interpretation and early warning (assessment against objectives, vulnerabilities, and scenarios);

4. Decision acceleration and anticipatory action (protocols, escalation thresholds, response options);

5. Learning and reconfiguration.

This multi-layer structure resonates with the microfoundations of dynamic capabilities – sensing, seizing, and transforming – through which firms detect opportunities and threats, mobilize resources, and reconfigure assets under conditions of rapid change (Teece, Pisano & Shuen 1997; Teece 2007).

The classical intelligence cycle is correspondingly extended:

Decision Need → Environmental Sensing → Signal Detection → Intelligence Integration → Risk Interpretation → Scenario and Consequence Assessment → Early Warning →
Decision Options → Action → Feedback and Organizational Learning.

The objective shifts from producing intelligence products to generating adaptive decision capability.

7. Decision Advantage and the Role of Artificial Intelligence

Intelligence alone does not guarantee effective action. Decision-makers may discount, misinterpret, or ignore warnings that conflict with existing assumptions (Bernhardt 2003; Gilad 2003). The final performance variable is therefore Decision Advantage: the ability to detect relevant change, interpret it rapidly, understand implications, identify options, decide within the available time window, and execute before the decision environment shifts.

Artificial intelligence amplifies sensing, processing, pattern recognition, and scenario generation. It does not, however, eliminate the fundamental intelligence problem. Organizations now confront excess machine-generated information. The critical question remains which signals matter for this organization, at this moment, for this decision (Stanev 2026). Risk Intelligence is therefore best understood as a human–machine architecture in which machines expand capacity while humans retain responsibility for contextual interpretation, value judgments, strategic meaning, and decision accountability (Dimitrov 2026b).

8. Discussion and Conclusion

Modern organizations possess specialized functions – risk, compliance, security, intelligence, strategy, audit – each generating valuable information. Performance suffers when these streams remain fragmented. Risk Intelligence addresses this structural problem by functioning as an integration layer that converts distributed information into shared understanding, anticipatory risk interpretation, and decision advantage.

Bernhardt's core principles retain full validity: the distinction between information and intelligence, the primacy of decision requirements, the utility of Key Intelligence Topics, the strategic role of early warning, the necessity of organizational architecture, and the requirement that intelligence answer "so

what?". What has changed is the environment – information abundance, compressed decision windows, interconnected risks, and systemic uncertainty.

Competitive Intelligence remains necessary but is no longer sufficient as the overarching architecture. Risk Intelligence extends the paradigm from competitor awareness to uncertainty awareness, from monitoring to anticipation, from information products to decision options, and from risk reporting to strategic action. Its architecture may be summarized as:

Sensing → Intelligence → Risk Interpretation → Early Warning → Decision → Action → Learning.

The strategic value of intelligence is ultimately measured not by the volume of products generated, but by the Decision Advantage it creates. Competitive advantage increasingly depends less on possessing more information than competitors and more on converting uncertainty into superior decisions faster than alternatives allow.

Author Declaration

Use of Generative AI and AI-assisted technologies in the writing process: During the preparation of this work, the author used artificial intelligence (AI) tools solely to assist with language editing, stylistic refinement, and technical formatting. AI was not used to generate, develop, or structure the core scientific ideas, theoretical framework, methodology, original models, analysis, or conclusions. The author takes full responsibility for the originality, validity, and integrity of the content presented herein.

REFERENCES

BERNHARDT, D., 2003. *Competitive intelligence: How to acquire and use corporate intelligence and counter-intelligence*. FT Prentice Hall.

DIMITROV, G., 2026a. *Information superiority and risk management in modern business.* [Unpublished monograph].

DIMITROV, G., 2026b. Risk as strategic intelligence: From uncertainty mitigation to competitive advantage. In: *International Conference of Young Scientists* (ICYS).

FRANCIS, D. B. & HERRING, J. P., 1999. Key intelligence topics: A window on the corporate competitive psyche. *Competitive Intelligence Review*, vol. 1, no. 4, pp. 10 – 19.

GILAD, B., 2003. *Early warning: Using competitive intelligence to anticipate market shifts, control risk, and create powerful strategies*. AMACOM.

HERRING, J. P., 1999. Key intelligence topics: A process to identify and define intelligence needs. *Competitive Intelligence Review*, vol. 10, no. 2, pp. 4 – 14.

STANEV, S., 2026. Artificial Intelligence as a Risk Factor: Analysis of Security and Legal Consequences in System Breaches. In: *Proceedings of the Scientific Conference*

“Contemporary Security Issues”. May 7 – 8, 2026. Veliko Tarnovo: Publishing Complex of Vasil Levski National Military University, ISSN 2367-7473 (pdf), pp. 567 – 575.

TEECE, D. J., 2007. Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, vol. 28, no. 13, pp. 1319 – 1350.

TEECE, D. J.; PISANO, G. & SHUEN, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, vol. 18, no. 7, pp. 509 – 533.

WEICK, K. E., 1995. *Sensemaking in organizations*. Sage.

WEICK, K. E.; SUTCLIFFE, K. M. & OBSTFELD, D., 2005. Organizing and the process of sensemaking. *Organization Science*, vol. 16, no. 4, pp. 409 – 421.

Dr. Georgi Dimitrov
University of Agribusiness and Rural Development
78, Dunav Blvd.
Plovdiv, Bulgaria
E-mail: gdimitrov@uard.bg

https://doi.org/10. 66334/annu26_operleveldeci

OPERATIONAL-LEVEL DECISION MAKING: UNCERTAINTY DECREASING TOOLS

Colonel Dr. Daniel Roman, Assoc. Prof.
Lieutenant-colonel Assoc. Prof. Claudiu-Valer Nistorescu
National Defense University "CAROL I" – Bucharest (Romania)

Abstract. The emergence of novel challenges within the international security environment has necessitated that military organizations must demonstrate a capacity for constant adaptation. Moreover, the complexity of the contemporary operating environment necessitates a recalibration of the manner in which operations and campaigns are planned and conducted. Recent conflicts have demonstrated that the management of major operations and campaigns has become increasingly challenging, and that this responsibility no longer lies exclusively with the military. The recurring complexity of such operations necessitates inter-institutional and interagency collaboration. In this context, an increase in the level of uncertainty within the operational process can be discerned, with commanders and their staff encountering difficulties in managing the decision-making process. It is evident that the situation becomes increasingly complex at the operational level of military operations, primarily due to the substantial number of actors involved and the intricate nature of their relationships.

In this context, the study aims to identify critical points in the decision-making process at the operational level of military operations, while also offering solutions to reduce uncertainty - a prerequisite for improving the efficiency of the process. The research findings underscore the ongoing necessity to adapt the command-and-control system, the significance of inter-institutional collaboration and cooperation, and the fragility of

complex decision-making systems and mechanisms. The analysis has been developed for the use of scholars and practitioners in the military field, with the results obtained serving as guidelines for adapting doctrine and operational processes.

Keywords: operational level; decision-making process; uncertainty; commander's visualization; resilience; operational design

Introduction

Military operations are inherently dynamic and uncertain, a reality substantiated by the lessons of military conflicts. The sources of uncertainty are twofold: firstly, the nature of war is inherently unpredictable, and secondly, the character of war is in a constant state of flux. From the perspective of the nature of war, uncertainty is an inherent element alongside friction, chance, ambiguity, chaos, fear, and physical and psychological pressure. The perpetual mutability of warfare engenders a concomitant state of uncertainty, compelling military organizations to recalibrate their doctrine, technology, and leadership in accordance with the evolving dynamics of conflict (Barno and Bensahel 2020, p. 26 and Nistorescu 2024a, p. 204 – 205).

It is an established historical fact that military organizations have developed two approaches over time with the purpose of reducing uncertainty on the battlefield. The two approaches are as follows: firstly, a centralized approach, in which decision-making was concentrated at the highest level of military leadership; secondly, a decentralized approach, which facilitated decision-making at lower levels of command as well (Tuck 2023, p. 36). In the initial scenario, the decision was accompanied by the formulation of a campaign or operational plan, which was intended to be executed without modifications. This approach entailed a substantial curtailment of the initiative and calculated risk-taking capabilities of subordinate commanders. This approach continues to resonate in contemporary command-and-control systems and is known as detailed command. Despite the fact that the purpose of detailed command is to reduce ambiguity, reality has demonstrated that timely adjustments to the plan and the exercise of initiative in this regard are imperative in military operations. Conversely, the alternative approach – which sought centralized planning but decentralized execution – has proven to be significantly more feasible under conditions of uncertainty. This approach has been refined over time and gradually adopted by most modern military organizations. It forms

the basis of mission command, the command philosophy embraced by the North Atlantic Alliance.

In the contemporary operational environment, uncertainty is exacerbated by the proliferation of emerging and disruptive technologies, the abundance of information, multi-domain operations, the diversity of actors, and the vulnerability of command-and-control infrastructures. Recent studies on the effects of new weapons systems demonstrate that these systems can generate tactical and operational asymmetries that translate into advantages. Concurrently, the role of heavy capabilities is being recalibrated by the combination of sensors, precision strikes, mobility, and protection (Nistorescu 2024b, pp. 72 – 83). In such circumstances, the reduction of uncertainty cannot be regarded exclusively as a process of information collection, nor as a function confined to a singular decision-making factor. The operational level is characterized by the interaction of the commander with various elements of the organizational structure, including the staff, the components, intelligence structures, liaison elements, C2 systems, and assessment mechanisms. These interactions collectively inform and shape the decision-making process at this level (Nilsson 2023, pp. 48 – 58).[1]

A systemic perspective on this complexity demonstrates that the level of uncertainty is amplified by the interdependencies between different domains and by the possibility that effects may spread from one subsystem to others. In an operational environment where energy, transportation, communications, digital infrastructure, and public institutions are interdependent, a local disruption can have disproportionate consequences on freedom of action. It is therefore imperative that understanding of the operational environment moves beyond a domain-specific approach, in order to address the nodes, connections and ripple effects that can transform a localized malfunction into a widespread operational problem (Roman 2026, pp. 14 – 17).

In accordance with the aforementioned logic, operational design can be utilized to transform the complexity of the environment into a future-oriented framework for understanding. Consequently, planning does not commence solely with a description of the current situation, but also with the design of several possible future scenarios, constructed through perception, understanding, and projection. This perspective is pertinent to the operational decision-making process because it shifts the focus from merely reacting to events to preparing plausible options in advance, which can be adjusted as the operational reality becomes clearer (Ioniță and Roman 2024, pp. 14 – 16).

In light of this reality, the present study maintains uncertainty reduction as its practical goal, but situates it within a broader framework: the configuration

of a resilient operational decision-making architecture. The concept is employed to delineate an architectural framework that is able to sustain continuity in understanding, planning and decision-making processes, even in circumstances where one of its decision-making nodes is degraded, isolated or overloaded. The starting point for our analysis is the recognition that uncertainty cannot be eliminated. However, what can be designed and practiced is the organization's ability to maintain freedom of action in the face of uncertainty.[2,3]

In accordance with this line of reasoning, the resilience of a decision-making architecture should not be assessed solely based on the physical survival of command structures. The system must have the capability to prevent, absorb, and withstand disruption, to adapt its mode of operation, and to rapidly restore essential processes. When applied to the operational decision-making process, this perspective shifts the focus from protecting a single command centre to preserving the critical functions of the entire architecture, even when certain components become temporarily unavailable (Roman 2026, pp. 93 – 94).

Methodology and research directions

From a methodological standpoint, this research employs a qualitative approach based on documentary analysis and an interpretive analysis of the military phenomenon. The analysis of doctrinal guidelines and specialized literature is undertaken for two principal purposes. Firstly, it is used to identify sources of uncertainty and existing tools. Secondly, it is used to integrate these elements into an organizational framework that is oriented towards resilience, anticipation and adaptation. The study is of a conceptual-applied nature, building on established doctrinal concepts to formulate an analytical framework that can support the adaptation of operational processes.

The primary aim of the study is to examine how decision-making at the operational level can remain effective in an operational environment characterized by persistent uncertainty. This will be achieved through the distribution of critical functions, the maintenance of decision-making continuity, and the integration of operational design with mechanisms for anticipation and adaptation. To guide our research, we have formulated the following questions: *What are the key factors that generate and amplify uncertainty at the operational level of military operations? What structural, cognitive and procedural characteristics are required for a resilient operational decision-making architecture? In what ways can operational design and anticipation mechanisms support the transition from a predominantly reactive decision-making process to a proactive and adaptive one?*

The value of this study lies in its analysis of new security challenges, which are driven by the reconfiguration of international power relations and the proliferation of emerging and disruptive technologies. These challenges require military organizations to adapt, recalibrate their physical capabilities, and transform their doctrinal frameworks, including their philosophies and command and control systems. The analysis is organized along three lines: uncertainty as a structural property of the operational environment; resilient decision-making architecture; and the shift from reaction to anticipation through operational design (Barno and Bensahel 2020, pp. 231 – 247 and Nilsson 2023, pp. 48 – 58).

Uncertainty as a Structural Condition of Operational Decision-Making

As Clausewitz noted over two hundred years ago, uncertainty in war stems from several sources. Inaccurate and/or incomplete information can lead to situations that are often referred to as the "fog of war". Furthermore, the interactions among the campaign's various stakeholders generate nonlinear outcomes that are difficult to predict and understand. The geography of the battlefield, particularly dense and confined environments such as forests and urban areas, can amplify this condition. Uncertainty is also compounded by irregular forces, unconventional tactics, and efforts to conceal, deceive, and mislead (Clausewitz 1984; Tuck 2023, pp. 25 – 42).The human factor exerts a significant influence on conflict and military operations through non-physical multipliers of combat power, such as morale and the will to fight. The conflicts and contradictions inherent in the definition of the belligerents' objectives become additional sources of uncertainty. Information is selected, managed and interpreted by people, so uncertainty can also result from errors in judgment, cognitive biases, or an operational picture built on unverified assumptions (Jordan et al. 2016, p. 50).[4]

In the contemporary era, uncertainty remains a constant feature of military campaigns and operations. There are several sources of uncertainty that must be considered. Firstly, there is the question of the adversary, and also the local population and the actors involved. In addition to these, there are the PMESII operational variables to consider. The complexity of the entities involved in the conflict, the specific nature of the physical environment, and the dynamic interactions among actors make it difficult to anticipate outcomes. Chance and friction further increase the ambiguity during the conduct of operations and campaigns.[5] Chance is defined as unexpected events or changes in circumstances that cannot be fully controlled or anticipated. Friction is defined as obstacles that make it difficult to accomplish even the simplest tasks.

From an analytical perspective, these sources can be grouped into five interdependent categories: informational, adversarial, environmental, organizational, and cognitive uncertainty. The initial three factors pertain to external or inadequately observable unknowns; the subsequent two highlight the capacity of the military organization itself to engender or amplify uncertainty through the fragmentation of information, variations in procedures, lines of authority, information overload, and biases (Nilsson 2023, pp. 52 – 58).[6]

This perspective necessitates a shift in the criterion employed to evaluate the effectiveness of the decision-making process. A resilient architecture is not one that claims to eliminate uncertainties or produce an optimal, definitive plan; rather, it is one that can detect change, reassess assumptions, maintain the continuity of critical functions, and generate options before the situation necessitates a delayed response.[7]

Building a Resilient Operational Decision-Making Architecture

In this study, the concept of „resilient operational decision-making architecture“ is defined as a distributed organization of the functions of understanding, planning, decision-making, and evaluation, designed so that the failure of a single component does not paralyze the entire system. The commander’s role encompasses the provision of direction and intent, in addition to the decision-making process, within the boundaries of their responsibilities. However, the efficacy of this process is contingent upon a network of relationships, processes, and nodes that facilitate the development of situational awareness and options for resolution. Consequently, the resilience of the architecture can be analyzed along three complementary dimensions: structural, cognitive and procedural.

This architecture can also be understood as a system of relationships among multiple centers of knowledge and decision-making, positioned differently in relation to information flows and to what the authors call the „boundary of situational awareness.“ Within such a system, certain elements are responsible for generating the operational picture, while others act as filters or distributors of this information. Finally, there are elements that operate at the interface with operational reality. Consequently, the decision-making process should not be designed as a strictly vertical sequence, but rather as a network capable of maintaining a coherent understanding even when certain connections or nodes are compromised (Ioniță and Roman 2024, pp. 16 – 18).

Structural resilience: distributed nodes and decision continuity

Structural resilience involves the distribution of critical functions across multiple nodes that can support one another. The relationship between the main command post and the alternate command post is important for both physical survival and the continuity of the decision-making process. A backup command post that can only take over communications, without access to the same situational understanding, staff assessments, planning assumptions, and the rationale behind previous decisions, provides technical redundancy rather than decision-making resilience (. Consequently, redundancy must be designed at least on three levels: continuity of understanding, continuity of planning, and continuity of decision-making. It is imperative that the operational picture, functional estimates, CCIR, decision points, assumptions, and options can be reconstructed and utilized by alternative nodes without a significant loss of situational awareness. This capability is of the essence in a contested environment, where command posts, communications infrastructure and data nodes are all potential targets of high importance. From this perspective, the value of a backup command post depends not only on its ability to take over communications, but also on its role within the situational awareness system. If the alternate decision-maker does not have the same context, assumptions, relationships among actors, and anticipated developments, the transfer of command may preserve the technical infrastructure without also preserving the cognitive continuity of the operation. Therefore, structural resilience also entails maintaining access to the "operational pictures" that enable the rapid reconstruction of the logic of the plan and previous decisions (Ioniță and Roman 2024, pp. 16 – 18).

The application of dependency analysis provides an additional criterion for determining which functions should be distributed or duplicated. It is possible to distinguish between three categories of dependencies. The first category is that of upstream dependencies, which condition access to information, communications, and resources. The second category is that of internal dependencies, which are associated with the operation of the node itself. The third category is that of downstream dependencies, which reflect the effects generated on other components. When viewed from this perspective, decision continuity is not merely a matter of technical backup, but rather the maintenance of functional relationships between nodes. The loss of a critical link can degrade the system's overall capability even if the physical structures remain intact (Roman 2026, pp. 94 – 99).

The commander's physical presence in the joint area of operations has been demonstrated to contribute to enhanced situational awareness, effective

communication with subordinates and other relevant actors, and the fostering of trust. Nevertheless, it is imperative to acknowledge that this should be regarded as one of numerous mechanisms, rather than the exclusive determining factor of decision quality. In a distributed architecture, situational awareness and decision-making capacity must be maintained even when the physical presence of a particular leader or the operation of a specific command post is temporarily impossible.

Cognitive resilience: shared understanding and mission command

The contemporary concept of mission command is predicated on the idea that the ambiguity, uncertainty, complexity, and volatility of the battlefield preclude a single commander from being sufficiently well-informed at all times to make all important decisions, nor to keep up with the sheer number of them. Subordinate commanders may possess a more nuanced understanding of the local situation and are better positioned to capitalise on fleeting windows of opportunity when permitted to make prompt decisions (Nilsson 2023, p. 45). Theoretically, mission command incorporates a series of constants whose appropriate application is determinative of the success of the concept. These include mutual trust, a shared understanding of the situation, the commander's clear intent, disciplined initiative, mission-type orders, risk acceptance and professionalism.[9,10] The aforementioned principles do not merely distribute authority; they also distribute the organizations' ability to continue to understand and act in situations where the flow of information is incomplete or disrupted.

The basis for such a distribution is *mutual trust*. At the operational level, the establishment of a system of relationships based on trust is a more arduous task than at the tactical level. This is due to the fact that the interaction processes involve a greater number and wider variety of actors. The establishment of trust is an arduous process that necessitates a considerable investment of time, mutual respect, a congruence of values and objectives, a history of shared experiences, authentic interactions, and an awareness of interdependence (Balboni et al. 2020, p. 37). In the context of multinational and coalition operations, this challenge is further compounded.

The *commander's intent* continues to serve as a pivotal reference point. At the operational level, the objective of the operation or campaign is articulated, as well as the desired military end state. In this way, the planning effort is guided and a framework is provided for the actions of subordinate commanders, who are thus able to act without further orders when the situation no longer unfolds

according to plan.[11] As outlined in the proposed architecture, intent serves a vital role in ensuring coherence between nodes, rather than acting as a substitute for their initiative.

The *common shared understanding* is the result of collaboration throughout the entire operational process, including planning, preparation, execution and evaluation, both horizontally and vertically. Education, doctrine, standardized procedures and communication all contribute to this outcome, but shared understanding should not be interpreted as cognitive uniformity. Cognitive resilience also involves the ability to maintain alternative perspectives, challenge dominant assumptions, and early identification of changes. Situational awareness can provide an additional framework for understanding cognitive resilience. In this model, we have identified three levels that are interconnected: the perception of relevant elements, the understanding of their significance, and the projection of how the situation might unfold. In a distributed architecture, it is essential that these three functions are distributed across multiple individuals and command centers, with information exchange, collaboration and mutual verification being key elements in supporting them. Therefore, shared understanding is more about the collective capacity to construct and update operational meaning than the mere circulation of the same picture among participants (Ioniță and Roman 2024, p. 14–15).The cognitive dimension of resilience also requires a mindset broad enough to integrate perspectives from different fields and functions. This comprehensive approach does not seek to standardize interpretations, but rather to challenge them within a collaborative framework. This enables the testing of dominant hypotheses and the breakdown of ill-structured problems into manageable components. The value of this approach lies in its ability to maintain cognitive alternatives and to prevent organizational consensus from becoming a source of rigidity (Roman 2026, pp. 140 – 145).

In a similar manner, when lower-level commanders demonstrate a *disciplined initiative*, it enables adaptation within the parameters established by the higher echelon. When time permits, changes in the situation must be reported and coordinated; when time does not permit or communication with the higher echelon is interrupted, it must still be possible to adjust the plan, while adhering to the intent and reassessing risks. Redundant communication channels and contingency plans facilitate both vertical and horizontal collaboration. However, these channels only achieve their full potential when they are supported by an organizational culture that encourages initiative. In order to achieve effective adaptation, it is essential to first identify the drivers of change, followed by a thorough risk assessment. Utilizing performance and efficiency indicators

enables the rapid correction of identified issues (Nistorescu 2024a, pp. 204 – 205).

It should be noted that acceptance of risk remains an inherent part of operations. The commander and the JOPG are responsible for identifying and analyzing risks, assessing their severity, and developing mitigation strategies. They also assess the risk to their own forces and the risk to the mission. It is vital to strike a balance between the importance of the objective, the time available, and the anticipated cost, whilst also considering the obligation to protect the force, the local population, and partners. In a resilient architecture, risk management must allow the force to maintain the initiative, not hinder it.

The implementation of *professionalism* and standardized order processes is integral to this aspect. Competencies are developed through education and ongoing training, and the simplicity and standardization of orders facilitate a common understanding and more effective communication among units and partners. However, standardization should be implemented with the objective of reducing procedural friction without creating rigidity. It is vital that the process remains flexible enough to support adaptation.

Cognitive bias awareness and the protection of judgement

It is important to be aware of potential cognitive biases and to manage the factors that contribute to their emergence. This is a requirement of the operational process and supports decision-making in conditions of high uncertainty. The complexity of operations, the vast amount of information, the multitude of actors, and operational, behavioral and cultural constraints can lead to errors in assessing the situation, defining the end state and selecting an approach. The decision-making process is inherently human, and uncertainty can be compounded by errors of judgement and biases (Jordan et al. 2016, p.50).

The Army Design Methodology (ATP 5-0.1) identifies the following biases as relevant: confirmation bias, status quo bias, sunk cost bias, sample size bias and anchoring bias.[12] Confirmation bias is a phenomenon where senior staff or decision-makers primarily seek out information that confirms a conclusion or a prematurely formulated hypothesis, whilst ignoring evidence that contradicts it. Creating an organizational culture based on collaboration, dialogue and the questioning of assumptions can limit the effects of this bias. Status-quo bias refers to the tendency to maintain the current state of affairs and to attach disproportionate importance to information that justifies a lack of change. Sunk-cost bias occurs when the costs already incurred lead to the

continuation of a course of action after its assumptions have been disproved. It is important to note that sample-size bias can lead to generalizations based on insufficient or unrepresentative samples. Similarly, anchoring bias can result in the retention of initial estimates or information as a reference point, even when new data contradicts them. In all these cases, the issue is not a lack of information, but rather the architecture's inability to reinterpret it effectively. In addition to cognitive biases, logical fallacies, groupthink, inconsistent analogies and the overvaluation of certain sources can affect the decision-making process. In a resilient architecture, safeguarding judgement involves institutionalized mechanisms such as red teaming, challenge functions, the review of assumptions and access to independent perspectives, so that consensus is the result of testing arguments rather than organizational pressure.

Procedural resilience: planning assumptions, risk and adaptive options

The development of planning assumptions is an indispensable tool when there is insufficient validated information to continue with planning. A planning assumption is defined as a supposition regarding the current situation or the future course of events, temporarily accepted as true in order to enable the process to continue. Assumptions are vital in addressing the gaps in knowledge, however, they must be necessary, logical and realistic, and their validation must be continuously monitored by the JOPG through requests for information, data received from subordinates and the allocation of data-collection resources.[13]

The commander and the JOPG must evaluate the assumptions in order to avoid biases, erroneous historical analogies, and individual or group thinking that is prematurely oriented in a particular direction. The formulation of excessive assumptions can increase the plan's vulnerability. It is imperative that assumptions regarding the adversary's capabilities and intentions are not made in a manner that understates these capabilities and intentions. Furthermore, each critical assumption must be associated with the associated risk and alternative courses of action in the event of its inaccuracy.

The manner in which assumptions are managed exerts a direct influence on the decision-making capability. In practice, an assumption can be linked to a decision point and to one of the commander's critical information requirements – CCIR. Consequently, the unknown is not 'eliminated', but transformed into a targeted condition, for which options are prepared. This finding is of particular significance in the context of understanding the relationship between procedural resilience and anticipation.

The correlation between assumptions and decision-making becomes evident when these elements are integrated with decision points. Consequently, assumptions play a crucial role in facilitating ongoing planning in the absence of complete information. However, it is imperative to maintain these assumptions to the minimum necessary, subject them to periodic review, and, where feasible, replace them with confirmed information. Concurrently, the junctures that necessitate decision-making should be synchronized with the instances when a choice becomes imperative and the risks associated with delaying or accelerating them unduly. This relationship endows procedural resilience with a temporal dimension: the organization must be cognizant not only of its decision-making capabilities, but also of the temporal parameters that delineate the optimal window for decision-making (Ioniță and Roman 2024, pp. 26 – 28). The transition in combat operations can be analyzed using the same logic. It has been determined that change is more manageable when the triggers and indicators are identified in a timely manner. This reduces the risk of a transition being imposed belatedly as a result of developments in the situation (Nistorescu 2024c, pp. 98 – 100). The application of procedural logic is rendered more robust when linked to an inter-institutional workflow. The application of scenario planning, early warning systems, standardized communication protocols, exercises, and the periodic revision of procedures facilitates the collective management of unknowns, transforming them into issues that can be addressed collectively. This approach facilitates the establishment of continuity in decision-making processes prior to the onset of a crisis. Furthermore, it enables the transition from a reactive to a proactive stance by integrating data, expertise and responsibilities from multiple organizations into a systematic process of analysis, planning, execution and evaluation (Roman 2026, pp. 124 – 129).

From Reactive Decision-Making to Anticipatory Operational Design

At an operational level, the complexity of the problem arising from the discrepancy between the current unsatisfactory situation and the desired end state necessitates the utilisation of a tool that facilitates comprehension and adaptation in conditions of uncertainty. Operational design fulfils this function by facilitating understanding and definition of the problem, and by supporting the application of operational expertise. The integration of the end-ways-means framework, a comprehensive approach and an analysis of the actors' behaviour is pivotal to the design. This approach involves defining the current state, describing the desired end state, formulating the problem and establishing an approach to resolve it.[14]

In its classical form, the OODA cycle (Observe, Orient, Decide, Act) describes an iterative logic of the decision-making process. For the purposes of this study, this logic can be applied in an expanded analytical form: The process is initiated with observation, followed by orientation, anticipation, decision-making, action, and assessment. The explicit introduction of anticipation is not intended to alter the OODA doctrine; rather, it is intended to highlight a function which, in the contemporary environment, must be deliberately cultivated between orientation and decision-making. In a similar manner, the concept of assessment is rendered explicit in order to underscore the notion that the outcome of an action must promptly be integrated into the understanding and re-framing of the problem. In this context, it is imperative to distinguish between anticipation and deterministic prediction. In an adaptive and adversarial system, the future cannot be known with certainty. Anticipation involves exploring plausible developments, identifying indicators and early warning signs, linking these to decision points, and preparing options before change necessitates a reaction. In this sense, the process does not aim to 'guess' the future, but rather to reduce the time between the recognition of change and the adaptation of the organization (Boyd 1995).

This forward-looking approach can be supported by distinguishing between feedback and feed-forward. Feedback corrects action on the basis of results that have already been produced, whereas feed-forward seeks to incorporate information about possible developments into planning before they materialize. Consequently, combining this logic with the practicality of operational design demonstrates that it can compensate for the inherent delays in reacting to rapid changes in the operational environment. In the context of the decision-making architecture examined in this study, the value of feed-forward lies not in its capacity to make specific predictions, but rather in its ability to proactively prepare the options, capabilities and transitions necessary for plausible scenarios.

The enhancement of forward-looking capability can be facilitated through the utilization of predictive platforms, simulation and digital twin tools, provided that these are regarded as aids rather than substitutes for professional judgement. The integration of ISR, sensors, geospatial data and open-source intelligence has the capacity to highlight weak signals, patterns and plausible trajectories prior to their manifestation. In this configuration, technological advancement has the potential to expedite observation and enhance situational awareness. It can facilitate a feed-forward logic that prepares options in accordance with probable developments, thereby circumventing the transformation of prediction into an artificial certainty. Operational design must therefore be regarded not as an activity confined to the initial stages of planning, but as an ongoing cognitive process of framing and

reframing. Continuous assessments, war games, the refinement of options and the reassessment of assumptions enable adaptation as the situation changes. Within the design process, the identification of decision points and their linkage to the CCIR, in addition to the identification of alternatives, critical points, culmination point, and opportunities that can be exploited.

A significant contribution of artificial intelligence to this anticipatory logic is the support it provides for design and planning in environments characterized by large volumes of data and complex decision-making requirements. Research conducted on the utilization of design engineering assistant tools in the context of space applications has indicated that such tools can facilitate access to prior knowledge, support the estimation of initial data, and generate additional options for experts (Russo and Lax 2022).

A second useful element is the shift from descriptive monitoring to the early identification of anomalies and to autonomous or semi-autonomous replanning. In the context of space applications, artificial intelligence (AI) systems are utilized for the purpose of monitoring the status of platforms, detecting deviations, and, in select circumstances, adjusting the plan without awaiting the completion of the entire ground intervention cycle. For a resilient operational decision-making architecture, this principle is relevant because it suggests that informational resilience does not merely mean data retention, but also the ability of nodes to identify degradation, signal deviations and prepare options before the loss of connectivity or information delays lead to a decision-making deadlock (Russo and Lax 2022).

A third area of concern pertains to the integration of data sources and the transformation of data into actionable alerts. A review of the specialist literature on “Earth observation” and “disaster management” applications indicates that the value of AI lies not only in its processing speed, but also in its capacity to filter large volumes of information, identify relevant patterns, and generate useful decision-making outputs in high-pressure situations. Within the operational process, this logic reinforces the relationship between Observe, Orient and Anticipate: the advantage lies not in the uncontrolled accumulation of data, but in reducing the time required to transform it into indicators, early warnings and options for action, whilst maintaining human control over interpretation and the final decision (Russo and Lax 2022).

The establishment and monitoring of measures of performance (MOP) and measures of effectiveness (MOE) are instrumental in identifying the necessity for decision-making and in evaluating the achieved effects. Sequencing is integral to the orchestration of the campaign or operation, ensuring the coherence of the actions and effects that contribute to the creation of the necessary conditions

for the achievement of objectives. The interrelationship among assumptions, indicators, CCIR, decision points, MOP/MOE, branches and sequels thus establishes a pragmatic apparatus for anticipation.

This logic can be summarized in a simplified conceptual model: *Understand – Anticipate – Decide – Adapt*. "Understand" refers to building and maintaining a shared understanding of the situation. "Anticipate" involves exploring plausible developments and preparing options before they materialize. "Decide" involves selecting a course of action in relation to intent, risk and the time available. "Adapt" means implementing the change, assessing its effects and, where necessary, reframing the problem. The model is not proposed as a doctrinal replacement for OODA or existing processes, but as an analytical framework for integrating them into the logic of a resilient architecture. The model can be strengthened by treating operational design as a process of continuous learning. To this end, focusing on systemic design and soft systems methodologies shows that, in complex conditions, the problem does not remain static throughout the planning phase, and the solution cannot be separated from the process through which the organization revises its understanding. Re-framing, iterative learning and adaptation thus become ongoing functions, rather than exceptional activities triggered only when the plan fails. In this context, the sequence *Understand – Anticipate – Decide – Adapt* can be interpreted as an operational learning loop in which each adaptation alters the basis for the next stage of understanding and anticipation.

In order to achieve a more profound understanding of the model, it is necessary to consider the distinction between structured and unstructured problems. The former allows for the application of relatively stable procedures, algorithms or solutions, whilst complex operational problems remain open-ended, ambiguous and context-dependent. Consequently, adaptation should not be interpreted as the final stage of a linear sequence, but rather as the mechanism through which the problem is continually reframed, broken down and re-analyzed. The model posits that *Understand – Anticipate – Decide – Adapt* is a paradigm for a cycle of learning and reconfiguration rather than a rigid sequence of steps within an operational analysis and planning process.

From this standpoint, the notion of operational advantage does not derive from the endeavor to eradicate uncertainty; rather, it is derived from the capacity to maintain freedom of action in the face of it. An organization becomes less reactive when it can detect change at an early stage, prepare alternatives, delegate sufficient authority and understanding to the relevant nodes, and continue to make decisions even when the C2 architecture is compromised (Nilsson 2023, pp. 52 – 58).

Conclusions

Our analysis highlights the fact that uncertainty is a structural feature of military operations and cannot be eliminated by centralizing decision-making or by indefinitely increasing the volume of information. While additional information can sometimes help to clarify certain issues, it can also result in information overload, delays and new vulnerabilities. The decision-making process must therefore be realistic in its approach, with the goal being to manage uncertainty through an architecture capable of maintaining critical functions and freedom of action.

The initial finding of the research indicates that decision-making resilience is distributed in nature. It is imperative to consider the main command post, alternate command post, components, intelligence structures, liaison elements, and assessment mechanisms as nodes of a unified architecture. True continuity requires more than technical redundancy; continuity of understanding, continuity of planning and continuity of decision-making must be prepared for, practiced and supported procedurally.

The second conclusion is that resilience has structural, cognitive and procedural dimensions. In the absence of cognitive redundancy, physical redundancy merely creates the illusion of continuity. Similarly, standardized procedures that do not allow for initiative or the challenging of assumptions can transform organizational stability into rigidity. Mission command leadership, professionalism, shared understanding, risk management and bias control are all relevant because they support the system's overall ability to continue functioning under less-than-ideal conditions.

The third conclusion drawn from this research is that operational design can function as a mechanism for integrating anticipatory thinking. It is evident that assumptions, indicators, CCIRs, decision points, running estimates, MOP/MOE, branches and sequels, and war gaming are instrumental in enabling the organization to transform unknowns into monitored conditions and to prepare options before they become urgent. In this sense, anticipation does not eliminate uncertainty; rather, it reduces reliance on delayed reaction.

It is evident that commanders continue to make decisions based on a combination of expertise, experience, intuition and judgement. The possession of professional competence, a strong sense of ethics and an understanding of one's own capabilities and those of the adversary remain fundamental. However, in a complex operational environment, the quality of a decision cannot be explained solely by the commander's individual attributes. This is achieved through an architectural framework in which the general staff, the components,

the information systems, the planning processes and the assessment mechanisms all contribute to the continuous development and updating of options.

The *Understand – Anticipate – Decide – Adapt* conceptual model encapsulates this approach and suggests that a decision-making advantage stems from an organizations' ability to understand change early enough, to anticipate plausible developments, to make timely decisions and to adapt more quickly than its adversary. It can thus be concluded that the effectiveness of the operational process is contingent not on the ability to eliminate uncertainty, but rather on the projection of a resilient operational decision-making architecture. The purpose of this architecture is to maintain freedom of action in conditions of deterioration, surprise and change.

NOTES

1. Mission Command Training Program. 2024. *FY23 Mission Command Training in Large-Scale Combat Operations: Key Observations*. Fort Leavenworth, KS: Center for Army Lessons Learned.

2. Department of the Army. 2019. *ADP 6-0, Mission Command: Command and Control of Army Forces*. Washington, DC: Headquarters, Department of the Army.

3. Mission Command Training Program. 2024.

4. Department of the Army. 2015. *ATP 5-0.1, Army Design Methodology*. Washington, DC: Headquarters, Department of the Army.

5. Department of the Army 2024…

6. Department of the Army 2015…

7. Department of the Army 2015…

8. Mission Command Training Program 2024

9. NATO Standardization Office. 2016. *ATP-3.2.2, Command and Control of Allied Land Forces*. Brussels: NATO Standardization Office.

10. Department of the Army. 2019…

11. Joint Chiefs of Staff. 2017. *JP 3-0, Joint Operations*. Washington, DC: Joint Chiefs of Staff.

12. Department of the Army 2015…

13. NATO Standardization Office. 2019. *AJP-5, Allied Joint Doctrine for the Planning of Operations*. Edition A, Version 2. Brussels: NATO Standardization Office.

14. NATO Standardization Office. 2019.

15. CLAUSEWITZ, C., 1984. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press.

16. Department of the Army. 2024. *FM 5-0, Planning and Orders Production*. Washington, DC: Headquarters, Department of the Army.

REFERENCES

BALBONI, M.; BONIN, J.A.; MUNDELL, R.; ORSI, D, 2020. *Mission Command of Multi-Domain Operations*. Carlisle Barracks, PA: U.S. Army War College Press.

BARNO, D.; BENSAHEL. N. 2020. *Adaptation under Fire: How Militaries Change in Wartime*. New York: Oxford University Press.

BOYD, J.R., 1995. *The Essence of Winning and Losing*. Briefing, 28 June 1995.

IONIȚĂ, C.-C.; ROMAN, D., 2024. *Designul operațional: Aplicarea artei operative în procesul de planificare a operațiilor*. București: Editura Universității Naționale de Apărare „Carol I”.

JORDAN, D.; KIRAS, J.D.; LONSDALE D.J.; SPELLER, I.; TUCK, C.; WALTON, C.D., 2016. *Understanding Modern Warfare*. 2nd ed. Cambridge: Cambridge University Press.

NILSSON, N., 2023. Commanding Contemporary and Future Land Operations: What Role for Mission Command? In: *Advanced Land Warfare: Tactics and Operations*, edited by Mikael Weissmann and Niklas Nilsson, pp. 43 – 62. Oxford: Oxford University Press.

NISTORESCU, C.V., 2024a. Adaptation of the Military Organization – An Essential Condition for Obtaining Success on the Battlefield. *Romanian Military Thinking*, no. 3, pp. 194 – 209. DOI: 10.55535/RMT.2024.3.10.

NISTORESCU, C.V., 2024b. The Asymmetries Generated by New Weapon Systems and Their Role in Achieving Success on the Battlefield. The Impact of HIMARS on the Conflict in Ukraine. *Buletinul Universității Naționale de Apărare "Carol I"*, vol. 13, no. 3, pp. 72 – 83. Available from: DOI: 10.53477/2065-8281-24-23. https://www.ceeol.com/search/article-detail?id=1280186.

NISTORESCU, C.V., 2024c. The Role of Heavy Armour in Modern Warfare. *Romanian Military Thinking*. 2024, vol. 3, pp. 42 – 59. Available from: DOI: 10.55535/RMT.2024.3.3; https://www.ceeol.com/search/article-detail?id=1333236

ROMAN, D., 2026. *Conceptualizarea protecției infrastructurilor critice prin aplicarea artei operative*. București: Editura Militară. ISBN 978-973-32-1446-5.

RUSSO, A.; LAX, G., 2022. Using Artificial Intelligence for Space Challenges: A Survey. *Applied Sciences,* vol. 12, no. 10, p. 5106. available from: DOI: 10.3390/app12105106.

TUCK, C., 2023. The Future of Manoeuvre Warfare. In: *Advanced Land Warfare: Tactics and Operations*, edited by Mikael Weissmann and Niklas Nilsson, pp. 25 – 42. Oxford: Oxford University Press.

Colonel Dr. Daniel Roman, Assoc. Prof.
National Defense University "Carol I"
68 – 72, Șoseaua Panduri
Bucharest, Romania
E-mail: roman.daniel@unap.ro

Lieutenant-colonel Claudiu-Valer Nistorescu, Assoc. Prof.
National Defense University "Carol I"
68 – 72, Șoseaua Panduri
Bucharest, Romania
E-mail: nistorescu.claudiu@unap.ro

https://doi.org/10. 66334/annu26_stratpredcri

СТРАТЕГИЧЕСКО ПРЕДВИЖДАНЕ ЗА КРИЗИСНА ГОТОВНОСТ ПО ИЗТОЧНИЯ ФЛАНГ НА НАТО: ИЗМЕРЕНИЯ НА НАЦИОНАЛНА УСТОЙЧИВОСТ НА БЪЛГАРИЯ В РИСКОВА СРЕДА ЗА СИГУРНОСТ

гл. ас. д-р Деница Хинкова
Софийски университет „Св. Климент Охридски“

Абстракт. Статията изследва стратегическото предвиждане, кризисната готовност и националната устойчивост като взаимосвързани компоненти на сигурността по Източния фланг на НАТО в условията на продължителна стратегическа несигурност, комплексни рискове и нарастваща взаимозависимост между гражданската и военната сфера. Изходна позиция е разбирането за стратегическото предвиждане като систематично изследване на множество възможни бъдещи развития, което подпомага подготовката и адаптацията на публичните политики, а не като прогнозиране на едно предварително определено бъдеще. Основната теза е, че способността на държавите да предвиждат рискове, да поддържат непрекъснатост на управлението и жизненоважните обществени функции и да осигуряват гражданска подкрепа за отбранителните операции представлява съществен компонент на националната и колективната сигурност. В теоретичен план изследването свързва концепциите за стратегическо прогнозиране или стратегиче-

ско предвиждане (*foresight*), с изпреварващо управление (*anticipatory governance*), кризисна готовност, национална устойчивост и колективна отбрана. Надграждайки подходите на OECD към стратегическото предвиждане и изграждането на антиципативен капацитет, статията разглежда *foresight* като механизъм за идентифициране на потенциални прекъсвания, разработване на сценарии, стрес-тестиране на политики и превръщане на знанията за възможни бъдещи рискове в действия в настоящето. На тази основа се предлага аналитична рамка, в която кризисната готовност се разглежда не само като способност за реакция след настъпването на кризата, а като предварително изградена институционална, инфраструктурна, технологична и обществена способност за предвиждане, подготовка, функциониране и адаптация. Моделът предлага рамка за анализ чрез *Integrated Anticipatory Governance Framework* (*IAGF*), като адаптира измеренията на предвиждане, институционален капацитет, устойчивост и уязвимост към контекста на националната и колективната сигурност. Подходът е съобразен и с актуализираните през 2026 г. изисквания на НАТО за устойчивост, акцентиращи върху непрекъснатостта на управлението, устойчивото предоставяне на основни услуги, гражданската подкрепа за военните операции, критичната инфраструктура, транспорта, енергетиката, комуникациите и координацията между институциите и обществото. Емпиричната част представя сравнителен анализ на държавите от Източния фланг на НАТО, основан на комбинация от международни сравнителни индикатори и документален анализ на национални стратегии, политики и институционални механизми. За оценяване на различните измерения на устойчивостта и кризисната готовност се използват данни за военни разходи от *SIPRI Military Expenditure Database*, предоставяща съпоставими времеви серии за военните разходи на държавите от 1949 г. насам. Като допълващ индикатор за военни способности се използва *Global Firepower PowerIndex*, включващ повече от 60 фактора, свързани с личен състав, въоръжение, финансови ресурси, логистични способности и география. Показателят се използва предпазливо и само като един от компонентите на анализа предвид различията между измерването на конвенционален военен потенциал и по-широката концепция за национална устойчивост. За оценяване на структурната уязвимост и рисковата експозиция се използват данни и аналитични ресурси на *European Commission Joint Research Centre (JRC) / Disaster Risk Management Knowledge Centre – Risk Data Hub. Risk Data Hub* интегрира данни за опасности,

експозиция, уязвимост и последици от бедствия и предоставя европейски съпоставими инструменти за анализ на риска. Особено релевантен е подходът на *JRC* към многорисковата среда, при който взаимодействието между природни, технологични, обществени и геополитически рискове може да поражда кумулативни и каскадни ефекти. Анализът на *JRC* от 2025 г. идентифицира 47 риска и подчертава необходимостта от по-систематично използване на *foresight*, сценарийно планиране и антиципативно управление при подготовката за бъдещи рискове.

Ключови думи: България; военна мобилност; гражданско-военно взаимодействие; изпреварващо управление; Източен фланг; кризисна готовност; критична инфраструктура; НАТО; национална сигурност; стратегическа несигурност; стратегическо предвиждане; устойчивост

Увод

Бъдещето не е просто продължение на настоящето. То представлява пространство от възможности, рискове и решения, чрез които действията в настоящето постепенно оформят условията, в които институциите и обществата ще функционират. Способността на публичните институции да разбират възможните бъдещи развития, да се подготвят за тях и да адаптират своите действия се превръща във все по-значим компонент на съвременното управление. Този проблем придобива особено значение в сферата на сигурността, където геополитическата нестабилност, технологичната трансформация, климатичните рискове, киберзаплахите, прекъсванията на критичната инфраструктура, трансграничните кризи и военните конфликти се наслагват и взаимодействат. Съвременните кризи рядко възникват в изолирана форма. Те се развиват в среда на взаимозависими системи, в която нарушаването на една критична функция може да предизвика каскадни последици за множество други. Прекъсването на енергийни доставки може да засегне транспорта и комуникациите; нарушаването на цифровата инфраструктура може да затрудни функционирането на публичните институции; ограничаването на транспортната свързаност може да възпрепятства както гражданското функциониране, така и военната мобилност. Поради това способността на държавата да поддържа основните си функции при продължителна криза се превръща в съществено измерение на националната сигурност. Традиционните подходи към сигурността дълго време поставят

основен акцент върху военната мощ, отбранителните способности и способността за непосредствена реакция. Тези измерения остават фундаментални, но сами по себе си не обхващат цялата способност на държавата да функционира при мащабна или продължителна криза. Военните способности зависят от транспорт, енергия, комуникации, медицинска инфраструктура, логистика, функционираща администрация и способност на гражданските институции да осигурят необходимата подкрепа. Следователно националната сигурност трябва да бъде разглеждана и през способността на институциите и обществото да поддържат своето функциониране, да се адаптират и да възстановяват основни функции при нарушаване на нормалния ред. Този въпрос е особено релевантен за държавите от Източния фланг на НАТО. След 2014 г., а още по-ясно след 2022 г. регионалната среда за сигурност се развива в условията на продължителна стратегическа несигурност, нарастващи изисквания към отбранителните способности и необходимост от по-висока степен на гражданска и институционална готовност. Военната готовност, предното присъствие, оперативната съвместимост и военната мобилност са тясно свързани с устойчивостта на гражданските системи, които осигуряват инфраструктура, енергия, транспорт, комуникации, медицинска подкрепа и непрекъснатост на управлението.

Настоящото изследване разглежда именно тази връзка между стратегическото предвиждане, кризисната готовност и националната устойчивост. Основният изследователски въпрос е как тези три измерения могат да бъдат интегрирани в сравнителна аналитична рамка за държавите от Източния фланг на НАТО и какви специфични характеристики на тази рамка се открояват в случая на България. Сравнителният анализ обхваща ключови измерения на националната устойчивост и кризисната готовност, включително непрекъснатост на управлението и основните обществени функции, енергийна и транспортна устойчивост, критична инфраструктура, здравна и обществена готовност, устойчиви комуникации и киберсигурност, военна мобилност, гражданско-военно взаимодействие, институционален капацитет и структурна уязвимост. Тези измерения се съпоставят с актуалната рамка на НАТО за национална устойчивост и гражданска готовност, включително седемте базови изисквания за устойчивост и способността на съюзниците да подготвят, противодействат, реагират и възстановяват основни функции при стратегически шокове и прекъсвания. На основата на сравнителните резултати се идентифицират сходства, различия и модели на кризисна готовност и национална устойчивост по Източния фланг. Втората аналитична линия поставя България

като фокусиран казус в сравнителната рамка. Анализират се специфичните характеристики на българската кризисна готовност и устойчивост с акцент върху стратегическото положение на страната по Югоизточния и Черноморския сегмент на Източния фланг, ролята на страната домакин, военната мобилност, критичната инфраструктура и взаимодействието между граждански и военни структури. Въз основа на сравнителните резултати се предлага модел за стратегическо предвиждане и управление на националната устойчивост на България, който свързва ранното идентифициране на рискове, оценката на уязвимостите, сценарийното планиране, институционалната готовност, способността за адаптация и гражданско-военното взаимодействие. Изследването аргументира, че националната устойчивост не следва да се разглежда единствено като способност за противодействие и възстановяване след настъпването на криза, а като динамичен капацитет за предвиждане, подготовка, адаптация, непрекъснатост и координирана реакция, който допълва военните способности и укрепва способността на държавата да изпълнява своите национални и съюзни функции. Анализът на националната устойчивост не се свежда до един количествен показател, а я операционализира като многомерна конструкция, в която военните способности, структурната уязвимост, институционалният капацитет за предвиждане и кризисната готовност се разглеждат като взаимосвързани, но аналитично разграничени измерения. От него произтичат три допълнителни въпроса: Кои институционални, инфраструктурни, обществени, технологични и отбранителни способности формират националната кризисна готовност? Какви сходства, различия и модели на национална устойчивост се открояват между държавите от сравнителната група? Как сравнителните резултати могат да бъдат използвани за разработване на модел за стратегическо предвиждане и управление на националната устойчивост на България? Статията не цели да измерва пряко ефективността на възпирането или да прави оценка на военната мощ на отделните държави. Вместо това тя изследва системните условия, които подпомагат способността на държавата да поддържа основните си функции при криза и по този начин създават институционална, инфраструктурна и обществена основа за функционирането на колективната сигурност.

От стратегическо предвиждане към изпреварващо управление

Стратегическото предвиждане се развива като отговор на ограниченията на традиционното прогнозиране. Докато прогнозата обикновено се

стреми да оцени вероятното бъдещо развитие въз основа на налични данни и установени тенденции, *strategic foresight* разглежда бъдещето като множество възможни траектории. Тази разлика е особено важна в среда на висока несигурност, в която историческите тенденции невинаги са достатъчни за идентифициране на нововъзникващи рискове. Риел Милър (Miller 2018) и Роберто Поли (Poli 2010) разглеждат *anticipation* като когнитивна и организационна способност, която позволява на институциите да работят с множество възможни бъдещи развития. Fuerth (2009) свързва *foresight* с управленския капацитет и подчертава необходимостта бъдещо-ориентираната информация да бъде интегрирана в текущото вземане на решения. В същата посока OECD разглежда стратегическото предвиждане като публичносекторен капацитет, който трябва да бъде свързан с разработването на политики, бюджетиране, регулации, инвестиционни решения и организационни промени.[1] В този смисъл стратегическото предвиждане не представлява опит да се предскаже едно конкретно бъдеще. То разширява способността на институциите да разбират възможните развития, да разпознават слаби сигнали, да изследват алтернативни сценарии и да подобряват настоящите решения с оглед на потенциалните бъдещи последствия. Особено значение имат *horizon scanning*, сценарийното планиране, анализът на *emerging risks*, стрес-тестирането и системното използване на *lessons learned*. Тази перспектива позволява да се направи следващата концептуална стъпка – от *strategic foresight* към *anticipatory governance*. Изпреварващото управление предполага, че институциите не само разпознават потенциални рискове, но разполагат с механизми за превръщане на знанието за тях в решения, ресурси и конкретни способности. Следователно между предвиждането и резултата стои институционалният капацитет.

Логиката може да бъде представена като последователност от взаимосвързани процеси: стратегическото предвиждане идентифицира възможните бъдещи развития; изпреварващото управление интегрира това знание в процеса на вземане на решения; кризисната подготовка превръща решенията в конкретни способности; а устойчивостта определя доколко системата може да поддържа основните си функции, да се адаптира и да се възстановява при настъпването на кризата. Така се формира основната концептуална връзка на изследването: стратегическо предвиждане → изпреварващо управление → кризисна готовност → устойчивост → адаптивен капацитет.

Кризисна готовност и национална устойчивост

Кризисната готовност не следва да бъде ограничавана до способността за непосредствено реагиране. Тя включва предварително изградени институционални, инфраструктурни, технологични и обществени способности, които позволяват на държавата да функционира при нарушаване на нормалните условия. В настоящото изследване терминът *кризисна готовност (crisis prereparedness)* се разбира като предварителна способност за подготовка и действие, *отговор при кризи (response)* – като непосредствено действие при настъпването на кризата, а *устойчивост (resilience)* като способност за поддържане на основните функции, адаптиране и възстановяване. Това разграничение е важно, защото една държава може да притежава значителен военен потенциал и едновременно с това да бъде уязвима при продължително прекъсване на енергийни доставки, транспортни коридори, комуникации или критични цифрови системи. *Националната устойчивост (national resilience)* в този смисъл включва способността на институциите и обществото да поддържат непрекъснатост на управлението и основните обществени услуги, да защитават критичната инфраструктура, да осигуряват устойчиви комуникационни и цифрови системи, да поддържат медицински и хуманитарни способности, да осигуряват транспорт и логистика, да координират граждански и военни структури, да мобилизират ресурси и да се адаптират към променящите се условия. Тези способности не заместват военната отбрана. Те създават част от условията, при които отбранителните способности могат да бъдат поддържани при продължителна криза. В този смисъл устойчивостта функционира като връзка между гражданската готовност, националната сигурност и способността на държавата да изпълнява своите съюзнически ангажименти.

Инегриран модел за кризисна готовност и устойчивост

За целите на настоящото изследване се предлага Интегриран модел за кризисна готовност и устойчивост (*Integrated Anticipatory Crisis Resilience Framework – IACRF*) като рамка за изпреварващо управление към конкретния с пет взаимосвързани измерения.

1) Стратегическо предвиждане, което обхваща сканиране на хоризонта (на англ. *horizon scanning*), сценарийно планиране, ранно предупреждение, идентифициране на нововъзникващи рискове (на англ. *emerging risks*) и използване на стратегически анализ при разработването на политики.

2) Институционална готовност – способността на институциите да превръщат знанието за възможните рискове в предварителна подготовка чрез механизми за непрекъснатост на управлението, координация, кризисно планиране, процедури за вземане на решения, управление на ресурси и междуинституционално взаимодействие.

3) Устойчивост на критичната инфраструктура, включваща енергетика, транспорт, комуникации, цифрова инфраструктура, водоснабдяване, хранителни системи и здравна инфраструктура. Критичната инфраструктура се разглежда не само като икономически ресурс, а като част от способността на държавата и обществото да поддържат своите функции при криза.

4) Обществена и гражданската готовност, включваща гражданска защита, медицинска готовност, способност за управление на масови инциденти, готовност на населението, кризисна комуникация и механизмите за обществена и доброволческа мобилизация.

5) Сигурност и адаптивен капацитет, който свързва гражданската устойчивост с националната и колективната сигурност. То включва киберустойчивост, гражданско-военно взаимодействие, военна мобилност, оперативна съвместимост и способност за институционално учене и адаптация след учения и кризи. Към тези измерения се добавя структурната уязвимост като напречен фактор, който може да ограничава всички останали способности. Уязвимостта може да произтича от географска експозиция, енергийна зависимост, инфраструктурни дефицити, демографски и социално-икономически ограничения, климатични рискове, зависимост от външни системи и киберрискове. По този начин моделът (*IACRF*) очертава способността на държавата да предвижда, да се подготвя, да функционира и да се адаптира при комплексна криза.

Методология и изследователски дизайн

Изследването използва смесен сравнителен дизайн, който съчетава количествени международни индикатори с качествен анализ на национални стратегически документи, политики и институционални механизми. Основната сравнителна група включва държавите от Източния фланг на НАТО, за които са налични достатъчно съпоставими данни: България, Румъния, Полша, Естония, Латвия, Литва, Словакия, Унгария и Финландия. Периодът 2016 – 2026 г. позволява да се проследят промените в институционалната и кризисната готовност в контекста на трансформацията на

европейската среда за сигурност през последното десетилетие. Изборът на периода позволява едновременно да бъдат обхванати развитието на политиките за устойчивост след 2014 г. и последвалите промени в условията на сигурност след 2022 г.

Емпиричният анализ се основава на няколко групи данни. Показателите на SIPRI за военните разходи се използват за характеризиране на ресурсното измерение на отбранителната политика, без да се приемат като самостоятелна мярка за национална сигурност. Данните на *Global Firepower* могат да бъдат използвани като допълнителен, ориентировъчен показател за конвенционалния военен потенциал, като се отчита методологичната специфика на този индекс. Данните и аналитичните ресурси на *European Commission Joint Research Centre* и *Risk Data Hub* се използват за оценяване на рисковата експозиция, уязвимостта и потенциалните последици от различни опасности. *OECD* предоставя основата за измерване и концептуализиране на стратегическото предвиждане и изпреварващия институционален капацитет. Тези международни източници се допълват от данни на НАТО, *UNDRR*, *Eurostat*, *World Bank* и други релевантни международни бази данни, както и от национални стратегии и документи за сигурност, управление на кризи, гражданска защита, критична инфраструктура, киберсигурност, военна мобилност и гражданско-военно взаимодействие. Методологическият подход не предполага предварително зададен съставен индекс. Първо се оценяват наличността, съпоставимостта и статистическите характеристики на отделните показатели. След това се анализират техните взаимовръзки и възможността за агрегиране. При недостатъчна съпоставимост отделните измерения се запазват като многомерна аналитична система вместо да бъдат редуцирани до една числова стойност. Този подход е особено важен при сравнителна група с ограничен брой държави. Корелационният анализ може да покаже асоциации между отделни измерения на *preparedness*, *resilience*, *institutional capacity*, *vulnerability* и *military expenditure*, но резултатите не следва да бъдат интерпретирани като доказателство за причинно-следствени зависимости.

Сравнителна аналитична рамка

Сравнителният анализ разглежда националната устойчивост като многомерна конструкция. Стратегическото предвиждане показва доколко институциите развиват способност да идентифицират бъдещи рискове и да работят със сценарии. Институционалната готовност показва доколко това

знание може да бъде превърнато в координирани решения и предварителна подготовка. Устойчивостта на критичната инфраструктура характеризира способността на ключовите системи да продължат да функционират при прекъсвания. Обществената и гражданската готовност отразяват способността на обществото и публичните услуги да реагират при мащабна криза. Сигурността и адаптивният капацитет свързват тези измерения с отбранителните и съюзническите функции. Тази рамка позволява да се направи важно разграничение между военна способност, кризисна готовност и устойчивост. Военната способност се отнася до наличните сили, средства и отбранителен потенциал. Кризисната готовност разглежда способността на държавата да се подготви и да реагира при сериозен системен шок. Устойчивостта се отнася до способността да се поддържа функционирането, да се адаптира системата и да се възстановят основните функции. *Трите измерения са взаимосвързани, но не са взаимозаменяеми* и тази разлика е особено важна за Източния фланг на НАТО, където националните системи трябва да функционират не само самостоятелно, но и като част от обща архитектура на колективната отбрана. Прекъсването на национална транспортна, енергийна или комуникационна система може да има последици за способността на съюзническите сили да се придвижват, комуникират и поддържат своите операции.

Сравнителният анализ на Източния фланг

Източният фланг представлява особено подходяща среда за изследване на кризисната готовност поради съчетаването на различни институционални, икономически, инфраструктурни и геостратегически характеристики. Държавите от сравнителната група имат различен административен и ресурсен капацитет, различна степен на експозиция към геополитически, енергийни, кибернетични и климатични рискове и различни национални модели за организация на гражданската и военната готовност. Същевременно те участват в обща система на колективна отбрана и са включени в европейска и евроатлантическа нормативна и институционална среда. Това създава възможност да бъдат разграничени общите структурни изисквания от националните специфики. Особено значение има способността на държавите да функционират като приемащи страни и да осигуряват необходимата инфраструктурна, транспортна, комуникационна, медицинска и логистична подкрепа за съюзнически сили. Следователно националната устойчивост придобива не само вътрешно, но и съюзническо измерение.

Целта на сравнителния анализ не е да подреди държавите в йерархия на *устойчиви /неустойчиви,* а да идентифицира различията в техните модели, комбинации от способности и структурни ограничения. Това позволява да се изследва дали съществуват различими подходи към кризисната готовност и кои измерения се оказват най-тясно свързани в различните национални контексти.

България като фокусиран емпиричен случай

В рамките на сравнителния анализ България е разгледана като фокусиран емпиричен случай, чрез който се изследва как общите измерения на националната устойчивост се проявяват в конкретния институционален, инфраструктурен и геостратегически контекст на Югоизточния и Черноморския сегмент на Източния фланг.Особено внимание се отделя на транспортната и логистичната свързаност, военната мобилност, енергийната устойчивост, критичната инфраструктура, комуникационната и цифровата устойчивост, гражданската защита, медицинската готовност и институционалната координация. Значим аспект е и способността на България да функционира като *Host Nation* и да осигурява необходимата подкрепа за съюзническите сили, без това да компрометира собствените ѝ основни обществени функции. Тук стратегическото предвиждане има особено практическо значение. Ако потенциалните рискове и зависимости бъдат идентифицирани предварително, подготовката може да бъде интегрирана в инвестиционни решения, инфраструктурно планиране, учения, кризисни процедури и междуинституционална координация. Поради това въпросът за България не се свежда до това какви отбранителни способности притежава страната. По-широкият въпрос е доколко националната система може да поддържа критичните функции, необходими както за гражданското общество, така и за функционирането на колективната отбрана при продължителна и многомерна криза.

От военна мощ към системна готовност

Сравнителната перспектива позволява да бъде преосмислена ролята на военната мощ в по-широката система на националната сигурност. Военните показатели могат да дадат информация за наличието на персонал, техника, финансови ресурси, инфраструктура и оперативен потенциал, но не измерват изцяло способността на държавата да поддържа тези способности при продължителна криза. Функционирането на военната мобил-

ност например зависи от състоянието на транспортната инфраструктура, мостове, железопътни линии, пристанища, енергийни системи, комуникации и административни процедури. По същия начин устойчивостта на критичната инфраструктура има пряко значение за способността на обществото да поддържа нормално функциониране в условията на криза. Това позволява да се формулира основната системна връзка на изследването: военните способности осигуряват средствата за отбрана, докато кризисната готовност и устойчивостта създават част от условията, при които тези способности могат да бъдат поддържани и използвани при продължителен системен шок. Следователно устойчивостта не трябва да бъде разбирана като алтернатива на отбраната. Тя представлява допълващо измерение на сигурността, което намалява уязвимостите и подпомага продължителното функциониране на националните и съюзническите способности.

Стратегическото предвиждане като механизъм за изпреварваща готовност

Основният принос на стратегическото предвиждане към кризисната готовност е промяната на времевата логика на управлението. Реактивният модел може да бъде представен като последователност от криза, реакция и възстановяване. Изпреварващият модел добавя към тази логика ранното разпознаване на сигнали, анализ, сценарии, предварителна подготовка, адаптация и институционално учене. Тази промяна не означава, че кризите могат да бъдат предвидени или предотвратени с точност. Тя означава, че институциите могат да бъдат по-добре подготвени за множество възможни развития. Практическата стойност на стратегическото предвиждане (*foresight*) се проявява тогава, когато то води до промени в реалната готовност. Това включва национални оценки на риска, сценарийни упражнения, сканиране на хоризонта (*horizon scanning*), стрес-тестове, учения за гражданска защита, гражданско-военни учения, тестове на критичната инфраструктура и киберсистемите и систематично използване на уроци, изведени от опита (*lessons learned*). По този начин стратегическото предвиждане се превръща от аналитичен инструмент в институционална способност за подготовка.

Дискусия

Предложената рамка показва необходимостта сигурността да бъде разглеждана като многосистемна способност. Традиционните показате-

ли за военна мощ не могат да обхванат всички фактори, които определят способността на държавата да функционира при продължителна криза. Те следва да бъдат допълнени от показатели за институционална, инфраструктурна, цифрова и обществена устойчивост. Същевременно съюзническата интеграция променя значението на националната готовност. В рамките на НАТО националната устойчивост има колективно измерение, защото способността на отделните държави да осигуряват транспорт, енергия, комуникации, медицинска подкрепа и *Host Nation Support* е свързана с функционирането на съюзническите способности.

Стратегическото предвиждане предоставя възможност да се премине от управление на вече настъпила криза към подготовка за множество възможни сценарии. В този смисъл устойчивостта може да бъде разглеждана като фактор, който подпомага поддържането на отбранителните способности при нарушаване на нормалния режим. Необходимо е обаче да се направи важно методологично разграничение. Настоящото изследване не твърди, че по-високата устойчивост автоматично води до по-висока ефективност на възпирането или до по-висока военна ефективност. Подобна причинна връзка изисква отделно изследване и различна емпирична стратегия. Аргументът е по-ограничен: устойчивостта представлява част от системните условия, при които националната и колективната отбрана могат да бъдат поддържани при продължителни и комплексни кризи.

Към модел за стратегическо предвиждане и национална устойчивост на България

Сравнителните резултати могат да бъдат използвани за разработването на модел за стратегическо предвиждане и управление на националната устойчивост на България. Моделът не следва да представлява механично копиране на практиките на друга държава, а адаптиране на идентифицираните сравнителни модели към българския институционален, инфраструктурен и геостратегически контекст. В основата му стои последователността от ранно идентифициране на рискове, оценка на уязвимостите, сценарийно планиране, институционална подготовка, изграждане на инфраструктурни и обществени способности, гражданско-военно взаимодействие, адаптация и институционално учене. Така предложената логика позволява стратегическото предвиждане да бъде свързано не само с разработването на стратегии, но и с конкретни решения относно инфраструктурата, ресурсите, ученията, кризисните процедури и координацията между институциите.

Заключение

Съвременната среда за сигурност поставя пред държавите задача, която надхвърля традиционната способност за непосредствена военна реакция. Кризите все по-често възникват като комплексни и взаимосвързани процеси, които засягат едновременно институции, инфраструктура, икономика, технологии, общество и сигурност. В тази среда стратегическото предвиждане придобива значение не като средство за предсказване на едно конкретно бъдеще, а като институционална способност за работа с множество възможни развития. Предвиждането придобива практическа стойност, когато е свързано с решения, подготовка, инвестиции, учения и институционално учене. Предложеният модел на Интегрирана рамка за кризисна готовност и устойчивост (*Integrated Anticipatory Crisis Resilience Framework*) развива тази логика, като свързва стратегическото предвиждане, институционалната готовност, устойчивостта на критичната инфраструктура, обществената и гражданската готовност, сигурността и адаптивния капацитет, като едновременно с това отчита структурната уязвимост като напречен ограничител.

Основното теоретично предложение в този контекст е, че кризисната готовност следва да бъде разглеждана като системна способност, а не като изолирана функция на управлението при извънредни ситуации. Тя включва способността на държавата да поддържа управлението, основните обществени услуги, критичната инфраструктура и взаимодействието между граждански и военни структури. За държавите от Източния фланг на НАТО този въпрос придобива допълнително значение поради необходимостта националните системи да функционират в рамките на обща архитектура на колективната отбрана. Националната устойчивост има съюзническо измерение, доколкото способността на една държава да осигурява транспорт, енергия, комуникации, медицинска помощ и помощ при преминаване от държавата домакин (*Host Nation Support*) може да влияе върху функционирането на съюзническите способности. В тази сравнителна перспектива България представлява фокусиран случай за изследване на взаимодействието между националната устойчивост и колективната сигурност. Географското положение на страната, Черноморското измерение, транспортната и логистичната свързаност и ролята ѝ в системата на съюзническата мобилност поставят специфични изисквания към кризисната готовност. Предложеният подход позволява преход от въпроса „*Колко военна мощ притежава държавата*?“ към по-комплексния въпрос: Доколко

ко държавата е способна да предвиди, да се подготви, да функционира и да се адаптира при продължителна и многомерна криза? Този въпрос не намалява значението на военната способност. Напротив, той я поставя в по-широка системна среда. Военната готовност изисква функциониращa държава, инфраструктура, логистика, комуникации и общество, способни да поддържат отбранителните способности при нарушаване на нормалния ред. Следователно стратегическото предвиждане, кризисната готовност и националната устойчивост могат да бъдат разглеждани като взаимосвързани компоненти на съвременната национална и колективна сигурност. Преходът от реактивно управление на кризите към изпреварваща готовност не означава отказ от реакцията, а промяна на времевата логика на управлението – от подготовка след появата на риска към системна подготовка за възможния риск. Именно в тази връзка стратегическото предвиждане може да се превърне от аналитичен инструмент в практическа способност за национална устойчивост.

БЕЛЕЖКИ

1. OECD, 2025. *Building Anticipatory Capacity with Strategic Foresight in Government: Lessons from Lithuania, Italy, and Malta.* OECD Public Governance Reviews. OECD Publishing. Available from: https://doi.org/10.1787/d7eb0bb6-en

2. ТАГАРЕВ, Т., 2024. От гражданско-военни отношения към устойчивост: Петата вълна на укрепване на демокрацията чрез изследвания и образование. – В *Сборник с научни доклади по сигурност и устойчивост*.

3. ФОТЕВ, Г., 2001. *Граници на политиката*. Изток–Запад

4. ШАЛАМАНОВ, В., 2019. Възпиране и отбрана на източния фланг на НАТО и ЕС: Готовност и оперативна съвместимост в контекста на предното присъствие. *Информационни процеси и системи за сигурност, № 2*, с. 12 – 25

5. Air University, 2025. *Enhancing deterrence on NATO's eastern flank: Nuclear integration and U.S. strategic posture*. Wild Blue Yonder

6. Allied Command Transformation, 2024. *Navigating the Future: Key Findings from Allied Command Transformation's 2023 Strategic Foresight Analysis*. NATO

7. Allied Command Transformation, 2024. *NATO Strategic Foresight Analysis: Future Capabilities & Security*. NATO

8. BRESSAN, S., 2025. *What foresight does NATO need?* NATO Defense College, NDC Outlook 09-2025

9. Center for Strategic and International Studies, 2024. *The Future of NATO's Eastern Flank*. CSIS

10. Centre for Eastern Studies, 2022. *NATO after Madrid: How much deterrence and defence on the eastern flank?* OSW Commentary

11. Council on Foreign Relations, 2023. *NATO's Deterrence Problem: An Analog Strategy in a Digital Age*. CFR

12. European Council on Foreign Relations, 2024. *The Ticking Clock: Why NATO's Deterrence Against Russia Is Under Pressure*. ECFR

13. FREEDMAN, L., 2021. Introduction-The evolution of deterrence strategy and research. – In: OSINGA, F.; SWEIJS, T. (eds.). *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century – Insights from Theory and Practice.* T.M.C. Asser Press, pp. 1-10. Available from: https://doi.org/10.1007/978-94-6265-419-8_1

14. GLOBSEC. *GLOBSEC Vulnerability Index: Bulgaria*. GLOBSEC

15. MAHNKEN, T. G.; MAZARR, M. J.; HEATH, T.; CEVALLOS, A. S., 2018. *Countering Comprehensive Coercion: Competitive Strategies Against Authoritarian Political Warfare*. Center for Strategic and Budgetary Assessments

16. MINKKINEN, M., 2019. The anatomy of plausible futures in policy processes: Comparing the cases of data protection and comprehensive security. *Technological Forecasting and Social Change,* vol. 143, pp. 172-180. Available from: https://doi.org/10.1016/j.techfore.2019.03.007

17. NATO Parliamentary Assembly, 2025. *Deterring aggression: Poland takes bold steps on NATO's eastern border.* NATO Parliamentary Assembly

18. NATO, 2021. *Strengthened Resilience Commitment*. NATO

19. NATO, 2025. *NATO launches Eastern Sentry to bolster posture along eastern flank*. NATO

20. Nuclear Threat Initiative, 2022. *NATO's New Strategic Concept: What It Is and Why It Matters*. NTI

21. OECD, 2024. *Framework for anticipatory governance of emerging technologies*. OECD Publishing. Available from: https://doi.org/10.1787/0248ead5-en

22. OECD, 2024. *Strategic Foresight Toolkit for Resilient Public Policy*. OECD Publishing

23. OSINGA, F.; SWEIJS, T. (eds.), 2021. *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century – Insights from Theory and Practice*. T.M.C. Asser Press. Available from: https://doi.org/10.1007/978-94-6265-419-8

24. PECO-YESTE, M., 2024. *How to do strategic foresight*. NATO Defense College, NDC Insight 04-2024

25. QUAY, R., 2010. Anticipatory governance: A tool for climate change adaptation. *Journal of the American Planning Association,* vol. 76, no 4, pp. 496-511. Available from: https://doi.org/10.1080/01944363.2010.508428

26. SHALAMANOV, V.; ANASTASOV, P.; TSVETKOV, G., 2019. Deterrence and defense at the eastern flank of NATO and the EU: Readiness and interoperability in the context of forward presence. *Connections: The Quarterly Journal,* vol. 18, no 1-2, pp. 11-25. Available from: https://doi.org/10.11610/Connections.18.1-2.02

27. SHLAPAK, D. A.; JOHNSON, M. W., 2016. *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics*. RAND Corporation

28. Stockholm International Peace Research Institute, 2026. *SIPRI Yearbook 2026: Armaments, Disarmament and International Security.* SIPRI

29. TAGAREV, T., 2019. Theory and current practice of deterrence in international security. *Connections: The Quarterly Journal,* vol. 18, no 1-2, pp. 5-10. Available from: https://doi.org/10.11610/Connections.18.1-2.01

30. TÕNURIST, P.; HANSON, A., 2020. Anticipatory innovation governance: Shaping the future through proactive policy making. – In: *OECD Working Papers on Public Governance*, No. 44. OECD Publishing. Available from: https://doi.org/10.1787/cce14d80-en

31. TREVERTON, G., et al., 2018. *Addressing Hybrid Threats*. Swedish Defence University

32. World Economic Forum & OECD, 2025. *AI in Strategic Foresight: Reshaping Anticipatory Governance*. OECD Publishing. Available from: https://doi.org/10.1787/aa573076-en

REFERENCES

FUERTH, L. S., 2009. Foresight and anticipatory governance. *Foresight,* vol. 11, no 4, pp. 14-32. Available from: https://doi.org/10.1108/14636680910982412.

MILLER, R. ed., 2018. Transforming the Future: Anticipation in the 21st Century. Paris/London: UNESCO Publishing/Routledge.

POLI, R., 2010. The many aspects of anticipation. Foresight, vol 12, no 3, pp. 7–17.

STRATEGIC FORESIGHT FOR CRISIS PREPAREDNESS AND DETERRENCE ON NATO'S EASTERN FLANK: COMPARATIVE MODELS AND DIMENSIONS OF BULGARIA'S NATIONAL RESILIENCE

Abstract. The changing security environment on NATO's Eastern Flank requires a shift from predominantly reactive approaches to security and defence towards greater preparedness, resilience and strategic foresight. This article examines the relationship between strategic foresight, crisis preparedness, deterrence and national resilience, focusing on the experience of NATO member states on the Eastern Flank and the position of Bulgaria within the evolving security architecture. The analysis combines conceptual perspectives on deterrence and defence with comparative examination of selected national approaches to preparedness, resilience, forward defence, defence investment and civil preparedness. Particular attention is paid to the interaction between military capabilities and broader societal, institutional and infrastructural capacities that contribute to credible deterrence and the ability to withstand and recover from crises. The article argues that strategic foresight can complement traditional deterrence approaches by strengthening the capacity of states and alliances to identify emerging risks, anticipate alternative scenarios and prepare adaptive responses before a crisis materialises. The Bulgarian case

is considered in the context of NATO's strengthened deterrence and defence posture, including developments on the Eastern Flank and the increasing importance of resilience, integrated air and missile defence, logistics, interoperability and defence-industrial capacity. The analysis highlights the importance of linking foresight with concrete preparedness measures and institutional capacity rather than treating it solely as a forecasting exercise. In this perspective, national resilience becomes an integral component of credible deterrence and collective defence.

Keywords: Bulgaria; military mobility; civil-military interaction; proactive management; Eastern Flank; crisis preparedness; critical infrastructure; NATO; national security; strategic uncertainty; strategic foresight; resilience

Dr. Denitsa Hinkova, Assist. Prof.
ORCID iD: 0000-0001-6565-9330
Web of Science ResearcherID: K-5525-20
Department of Public Administration
Faculty of Philosophy
Sofia University "St. Kliment Ohridski"
Sofia, Bulgaria
E-mail: dihinkova@phls.uni-sofia.bg

https://doi.org/10. 66334/annu26_civustcogn

ГРАЖДАНСКАТА УСТОЙЧИВОСТ В КОНТЕКСТА НА КОГНИТИВНИТЕ ВЪЗДЕЙСТВИЯ ВЪРХУ ОБЩЕСТВЕНОТО СЪЗНАНИЕ НА БЪЛГАРИТЕ ОТ ЗАПАДНИТЕ БАЛКАНИ

Деница Китанова, докторант
Военна академия „Георги Стойков Раковски“

Абстракт. Българските граждани извън страната са под под закрила на българската държава. Същевременно съхраняването на националната идентичност е въпрос от национален интерес. Настоящото изследване има за цел да анализира когнитивните въздействия върху гражданската устойчивост на българските общности в Западните Балкани – по-конкретно на българите в Северна Македония, Сърбия и Албания.

Ключови думи: гражданска устойчивост; когнитивни въздействия; Западни Балкани

Българските общности извън страната са се образували в резултат на различни фактори и процеси. Част от тях възникват вследствие на миграция. Други се появяват назад в историята. След участието на България във войните за национално обединение и произтеклите от тях мирни договори цели територии с българско население остават окончателно извън страната, т.е. това не е станало по желание на българите там. Така възникват българските исторически диаспори в

страните от Западните Балкани, които са предмет на настоящата разработка.

От една страна те могат да послужат като пример за обществена устойчивост, защото са запазили българското си самосъзнание десетилетия наред, но върху тях се забелязват определени когнитивни въздействия – именно те са обект на настоящия труд.

Целта, която авторът си поставя е да изследва когнитивните въздействия върху общественото българско самосъзнание в Албания, Северна Македония и Сърбия на лица, които притежават българско гражданство, и как тези въздействия влияят на тяхната гражданска устойчивост – като граждани на съответната държава, в която живеят. Като такива те разполагат с всички граждански права, свободи и задължения, които изхождат от съответните закони в разглежданите държави. С други думи – когнитивните въздействия върху тяхното българско обществено съзнание едновременно ги касае като български граждани, но и като отделни граждани на трите разглеждани държави в Западните Балкани.

Основната хипотеза е, че начинът, по който българите в Северна Македония, Сърбия и Албания са подложени на когнитивни въздействия се отразява пряко на тяхната гражданска устойчивост.

Докато понятието национална идентичност не се нуждае от допълнителни пояснения, е редно да се уточни в какъв контекст и какво значение влага авторът в разбирането за гражданска устойчивост. Това се налага, тъй като научните дефиниции са ограничени като брой и в голямата си част не са релевантни към изследването.

Прокопиев разглежда устойчивостта като „способност за устояване и справяне с рискове и предизвикателства“ (Prokopiev 2026, p. 312). Тук трябва изрично да се уточни, че той не разглежда гражданската устойчивост, а устойчивостта като цяло. В контекста на настоящото изследване обаче понятието устойчивост би могло да се обвърже с гражданите, ако се приеме, че гражданската устойчивост все пак е вид устойчивост. Тогава логично е устойчивостта на гражданите да бъде способността им за справяне с рискове и предизвикателства, които в настоящата разработка представляват когнитивните въздействия върху тяхното съзнание.

Изразът *гражданска устойчивост* може да бъде открит в различни стратегически документи. Те са съставени в последните години и изхождат от разбирането, че демократичният ред, вкл. пълноправното участие на гражданите в него, е подложен на различни заплахи, най-общо свързани с манипулиране на информацията; заплахи, които въздействат когнитивно

върху общественото съзнание. Такъв пример е пътната карта „Изграждане на гражданска устойчивост на глобалното предизвикателство за манипулиране на цифрова информация“ на Бюрото за киберпространство и цифрова политика (CDP) към Държавния департамент на САЩ. Този документ не си поставя за цел да даде изчерпателна дефиниция за гражданска устойчивост, но ясно говори за нейния практически смисъл и приложение – в САЩ обвързват повишаването на гражданската устойчивост с демокрацията и резистентността на гражданите към дезинформация и фалшиви новини.[1] За хипотезата на настоящия текст привличането на подобно разбиране е от съществено значение, понеже в хода на проучванията авторът непрекъснато се натъкваше на убедителни примери за това как конкретни дезинформационни потоци спрямо българите в чужбина оказват негативно влияние върху тяхната гражданска устойчивост и интегритет в държавите, в които живеят.

Гражданската устойчивост се употребява още веднъж, в друго изследване, в по-различен смисъл. Според авторите Tian et al. (2025) гражданската, или както я наричат общностната устойчивост, се обвързва с идентичността, но от гледна точка на националната държава. Два вида употреба на този израз – от една страна, гражданската устойчивост се свързва с демократичния ред и интеграцията на гражданите в него; а от друга, разглеждането му предполага поглед върху националната идентичност и нейното съхранение.

Настоящото изследване ще направи опит да използва това разминаване продуктивно, и да изработи от напрежението между двете разбирания собствен изследователски маршрут. Защото българите в чужбина и когнитивните въздействия спрямо тяхното съзнание попадат по особен начин и в двете тълкувания на *гражданската устойчивост* – и като елемент на националната идентичност, и като собственото битие на българите зад граница именно като граждани на държавите, в които живеят.

Въпросът е от значение за България, защото, от една страна, Конституцията на страната дава задължения на българската държава да закриля българските граждани в чужбина.[2] Наред с това според Актуализираната стратегия за национална сигурност опазването на националната идентичност е национален интерес за България.[3]

В настоящия труд се използват дескриптивен метод и сравнителен анализ. Използвани са мненията на представители на българската общност в Албания, Северна Македония и Сърбия – в лицето на Софика Мале от Глобочани (Мала Преспа), Люпчо Георгиевски, председател на закрития

клуб „Иван Михайлов“ в Битоля, и Иван Николов, председател на Културно-информационен център – Босилеград. Те са събрани под формата на интервюта, осъществени от автора в рамките на работата по дисертация на тема „Гражданската устойчивост в контекста на когнитивните въздействия върху общественото съзнание и възпитание“. Всички те са лидери в общността и притежават български паспорти. Събраните мнения нямат характер на социологическо изследване.

Авторът се ограничава с българите в Северна Македония, Албания и Сърбия в изследването си и не обхваща всички страни от Западните Балкани, не използва класифицирана информация и подчертава, че уважава правото на самоопределение на всеки един гражданин.

Когнитивните въздействия върху българите от Западните Балкани в контекста на тяхната гражданска устойчивост

Когнитивните въздействия върху общественото съзнание на българите от Западните Балкани са вид информационно въздействие, което в по-широк контекст е инструмент на хибридната война.

Информационното въздействие представлява преднамерено създаване и разпространение на специфична информация, оказваща непосредствено влияние върху функционирането и развитието на обществените информационни средства, психиката и поведението на политическия елит и населението на страната (Zhelev 2018, p. 54). Психологическото и пропагандното въздействие са съставен елемент на информационното въздействие. Това въздействие според автора на монографията се осъществява чрез инфологеми, известни още като „психична инфекция“ или идея-вирус, като за целта въвеждат правдоподобни конструкции (Zhelev 2018, p. 60)

Правдоподобни конструкции в контекста на настоящото изследване могат да бъдат датата 2 август, която е празник в Република Северна Македония, както и наименованието на различни организации с името „Илинден“. На датата 2 август по стар стил се отбелязва избухването на Илинденско-Преображенското въстание.

Това е и датата на първото заседание на Антифашисткото събрание за народно освобождение на Македония (АСНОМ) през 1944 г., чиято основна задача е да узакони югославския македонизъм, който е антибългарски (Stoyanov 2023, p. 44).

Предвид горното твърдение, се вижда как върху спомена за освободителните борби на българите в историко-географската област Македония,

се наслагва събитието, свързано с насаждане на омраза срещу българите, което дава на датата 2 август всички характеристики на инфологема.

Подобни наслагвания има и върху името Илинден, каквото носи организацията не македонците в Албания „Илинден – Тирана“, която в своя официален вестник със същото наименование отрича съществуването на българите в Албания и пише за тях като „така наречени“[4].

Според събраните мнения на формални и неформални лидери на общностите в Албания и Северна Македония[5] – те отговарят какво е за тях Илинден, като във въпроса не се уточнява какво се има предвид. За всички то е символ на борбата за национално обединение на българите и символ на жертвоготовност. С други думи те отнасят понятието към Илинденско-Преображенското въстание, но от друга страна българската общност в Албания например е отричана от организация с това име.

Тук се забелязва когнитивно-информационно въздействие върху българите, а както по-горе беше споменато, това е вид атака върху тях като отделни граждани. Макар и тя да е насочена към общественото съзнание на българската общност, тя ги касае и като граждани на Албания, а въпросът доколко те са устойчиви на това предизвикателство е пряко свързан с тяхната гражданска устойчивост. Казано по друг начин, тук се наблюдава класически пример за офанзива срещу националната идентичност, която прераства в подронване на гражданската устойчивост – това, че българите са „така наречени“ най-напред отрича тяхната идентичност, свежда я буквално до нереално определение, измислица, а после по този начин ерозира и самата им устойчивост като граждани на Албания – те са непълноценни, „така наречени“.

Сходен наратив за отричане на българската идентичност, което влияе на гражданската устойчивост, се забелязва и в Сърбия, където има българско малцинство. Сръбската медия Telegraf.rs публикува статия през 2018 г., според която шопите винаги са били смятани за племе в рамките на сръбския народ.[6] БАН отрича шопите да са вид архаични сърби в свое становище през 2025 г.[7]

Шопите обаче са известна етнографска група в България, имат специфични говори, като тази статия в сръбска медия представлява опит те да бъдат превърнати в инфологема и отново да се отрече тяхната българска идентичност, като под шопи изглежда се определят според статията и българите от Западните покрайнини, т.е. българското малцинство в Сърбия.

Иван Николов от КИЦ – Босилеград заявява в полуструктурирано интервю, че тезата за така наречената сръбско-шопска нация винаги е при-

съствала в медийното пространство на Сърбия и се засилва по време на отбелязването на годишнини, събития от българо-сръбската история.[8]

Същевременно, ако в Сърбия българите загубят своята идентичност, те ще се лишат от правото да имат свой Национален съвет, който да ги представлява пред сръбската държава, т.е. ще ги лиши от граждански права, макар и те да са формални.

На следващо място българите в Република Северна Македония са определяни в македонските средства за масова информация като татари, фашистки окупатори, или само окупатори. Например през 2026 г., вестник „Нова Македония“ публикува заглавие: „Нацистка Германия и българските окупатори в Треблинка отнеха душата на Скопие, Битоля, Щип...“.[9] В доклада на Европейската комисия срещу расизма и нетолерантността (ECRI) се дава пример с ефира на македонската телевизия „Канал 5“, където често българките са наричани с обидни квалификации.[10]

Тези примери от средствата за масова информация в Република Северна Македония могат да бъдат дефинирани като форма на манипулация, „защото лепенето на етикети с цел налагане на нарицателно име за някого са сред основните манипулативни техники“ (Zhelev 2018, p. 63), а според ECRI това представлява реч на омразата – в този случай срещу българите.

В този смисъл чрез медиите в Република Северна Македония на българите се лепят етикети – може да се допусне, че целта е те да бъдат стигматизирани и дори дискриминирани, тъй като те са принудени да потискат своята национална идентичност в обществото.

В Северна Македония има партии на етническите албанци, на бошняците, но не и на българите, което, от една страна, може да е резултат от тази стигма, от друга страна, рядко се срещат мнения на българите в македонските медии, което може да означава, че тяхното право на изразяване също не е достатъчно добре защитено, което пак е свързано с тяхната гражданска устойчивост от гледна точка на демокрацията. Това е така, защото от признаването на националната идентичност следват и конкретни политически права, както и медийна гласност – фундаменти на едно гражданско общество. Но ако същата национална идентичност бъде етикетирана и заклеймявана, тези права така и няма да бъдат придобити, а българите в Северна Македония не биха могли да постигнат онези нива на гражданска устойчивост, с които разполагат всички останали граждани на същата страна.

Същевременно интервюираните лица от българските общности твърдят, че манипулативният език, лепенето на етикети не се забелязва

само в медиите, а той е толериран и от съответната държава, и се използва от държавни лица. Изключение прави единствено Албания[11].

Ако се разгледат нивата на демокрацията в съответните страни – според доклада на американската неправителствена организация Freedom House – Сърбия е частично свободна, с най-малко точки от трите държави (53 точки), следвана от Република Северна Македония (67 точки) и Албания е с най-добър резултат (69 точки)[12]. Неслучайно и тя е най-напреднала в своята европейска интеграция, чрез която се гарантират основни човешки права и свободи.

В този смисъл, макар и да не са представителна извадка – мненията на лидерите на български общности съответстват на нивата на демокрация в разглежданите страни.

Изводи

Предвид гореизложеното може да се направят следните изводи:

Сравнителният анализ и мненията на представители на общността, както и разгледаните примери показват, че когнитивните въздействия върху българите от Западните Балкани са насочени срещу тяхната идентичност, което потвърждава първоначалната хипотеза на изследването.

Забелязва се сходен наратив и методи за когнитивни въздействия срещу българите от Албания, Северна Македония и Сърбия.

Всичко сякаш е в синхрон с нивата на демокрация в трите държави. Пример за това е Албания, в която нивото на демокрация е най-високо, а там според мнението на лидер на общността няма данни когнитивните въздействия да се насърчават от държавата, въпреки че все пак съществуват.

Когнитивните въздействия са предизвикателство пред гражданите на Албания, Северна Македония и Сърбия, които притежават и българско гражданство. То се изразява чрез манипулации и информационни въздействия, които обаче са насочени към тяхната българска идентичност. С други думи тяхната гражданска устойчивост е пряко свързана със запазването на тяхното българско самосъзнание, което е и ангажимент на българската държава.

БЕЛЕЖКИ

1. U.S. DEPARTMENT OF STATE, 2024. *Democratic Roadmap: Building Civic Resilience to the Global Digital Information Manipulation Challenge.* Bureau of Cyberspace and Digital Policy. [online]. Available from:

https://2021-2025.state.gov/roadmap-info-integrity/. [last viewed: 29 September 2026].

2. НАРОДНО СЪБРАНИЕ, 1991. Конституция на Република България. *Държавен вестник*, бр. 56 от 13 юли 1991 г.

3. МИНИСТЕРСКИ СЪВЕТ, 2018. Актуализирана стратегия за национална сигурност на Република България, [приета с Решение на НС от 14.03.2018 г.]. *Държавен вестник*, бр. 26 от 23.03.2018 г.

4. Публицистичен материал „Вистината за Македонците во Албанија паника кај бугарите“, публикуван на уебсайта на Македонско друштво „Илинден“ – Тирана на 17.02.2026 г. [онлайн]. Достъпно на: https://ilindentirana.com/vistinata-za-makedonczite-vo-albanija-panika-kaj-bugarite/.

5. Полуструктурирани интервюта, осъществени от автора със Софика Мале от Глобочани (Мала Преспа), Люпчо Георгиевски, председател на закрития клуб „Иван Михайлов“ в Битоля, и Иван Николов, председател на Културно-информационен център – Босилеград. Те са осъществени в периода март – юли 2026 г., като част от работата по дисертационен труд на тема „Гражданската устойчивост в контекста на когнитивните въздействия върху общественото съзнание и възпитание“.

6. Публикация „Šopsku salatu jedemo i volimo svi, a malo ko zna kako je nastala i ko su Šopski Srbi po kojima je i dobila ime“, публикувана в портала *Telegraf.rs* на 23.08.2018 г. [онлайн]. Достъпно на: https://www.telegraf.rs/zanimljivosti/zabavnik/2985496-sopsku-salatu-jedemo-i-volimo-svi-a-malo-ko-zna-kako-je-nastala-i-ko-su-sopski-srbi-po-kojima-je-i-dobila-ime.

7. ИНСТИТУТ ЗА ИСТОРИЧЕСКИ ИЗСЛЕДВАНИЯ – БАН, 2025. *Становище от 28 януари 2025 г.* София: Институт за исторически изследвания при БАН, 28 януари 2025 г. [онлайн]. Достъпно на: https://ihist.bas.bg/становище-28012025/. [Последно видян: 29 септември 2026].

8. Полуструктурирани интервюта, осъществени от автора със Софика Мале от Глобочани (Мала Преспа), Люпчо Георгиевски, председател на закрития клуб „Иван Михайлов“ в Битоля, и Иван Николов, председател на Културно-информационен център – Босилеград. Те са осъществени в периода март – юли 2026 г., като част от работата по дисертационен труд на тема „Гражданската устойчивост в контекста на когнитивните въздействия върху общественото съзнание и възпитание“.

9. Публикация „Нацистичка Германија и бугарските окупатори во Треблинка ја однесоа душата на Скопје, на Битола, на Штип“, публикувана в *Нова Македонија* на 11 март 2024 г. [онлайн]. Достъпно на: https://novamakedonija.com.mk/makedonija/politika/nacistichka-germanija-i-

bugarskite-okupatori-vo-treblinka-ja-odnesoa-dushata-na-skopje-na-bitola-na-shtip-2/.

10. COUNCIL OF EUROPE & EUROPEAN COMMISSION AGAINST RACISM AND INTOLERANCE (ECRI), 2023. *ECRI Report on North Macedonia (sixth monitoring cycle)*, [ECRI(2023)28, 20 September 2023], p. 13 . Strasbourg: Council of Europe. [online]. Available from: https://rm.coe.int/sixth-ecri-report-on-north-macedonia/1680ac8c47. [last viewed: 29 September 2026].

11. Полуструктурирани интервюта, осъществени от автора със Софика Мале от Глобочани (Мала Преспа), Люпчо Георгиевски, председател на закрития клуб „Иван Михайлов“ в Битоля, и Иван Николов, председател на Културно-информационен център – Босилеград. Те са осъществени в периода март – юли 2026 г., като част от работата по дисертационен труд на тема „Гражданската устойчивост в контекста на когнитивните въздействия върху общественото съзнание и възпитание“.

12. FREEDOM HOUSE, 2026. *Freedom in the World 2026: Country and Territory Reports* [online]. Washington, DC: Freedom House. [online]. Availa ble from: https://freedomhouse.org/country/scores. [last viewed: 29 September 2026].

ЛИТЕРАТУРА

ЖЕЛЕВ, Ж., 2018. *Информационни операции и информационно въздействие*. София: Военна академия „Г. С. Раковски“. ISBN 978-619-7478-01-3.

ПРОКОПИЕВ, С., 2026. Стратегически инструменти на устойчивостта в Европейския съюз. *Военен журнал*, т. 133, бр. 3, с. 311 – 322. София: ВА „Г. С. Раковски“. ISSN 0861-7392.

СТОЯНОВ, Л., 2023. Автономизъм и македонизъм – видове и начини на употреба. В: МАРКОВ, Г., ред. *България и Македония. История и политика. Втора част*, с. 9 – 52. София: Тангра ИК. ISBN 978-619-91801-2-9.

TIAN, S.; NING, S.; LI, H.; CHEN, L.; ZHU, H. & GAO, G., 2025. Relationship of social capital, community identity, and perceived safety resilience during public emergencies in Shanghai. *Scientific Reports*, vol. 15, no. 1, art. no. 6608. [online]. Available from: https://doi.org/10.1038/s41598-025-86990-0. [last viewed: 29 September 2026].

REFERENCES

PROKOPIEV, S., 2026. Strategicheski instrumenti na ustoychivostta v Evropeyskia sayuz. *Voenen zhurnal,* vol. 133, no. 3, pp. 311 – 322. Sofia: VA „G. S. Rakovski“. ISSN 0861-7392. [in Bulgarian].

STOYANOV, L., 2023. Avtonomizam i makedonizam – vidove i nachini na upotreba. In: MARKOV, G., ed. *Balgariya i Makedoniya. Istoriya i politika. Vtora chast*, pp. 9 – 52. Sofia: Tangra IK. ISBN 978-619-91801-2-9. [in Bulgarian].

TIAN, S.; NING, S.; LI, H.; CHEN, L.; ZHU, H. & GAO, G., 2025. Relationship of social capital, community identity, and perceived safety resilience during public emergencies in Shanghai. *Scientific Reports*, vol. 15, no. 1, art. no. 6608. [online]. Available from: https://doi.org/10.1038/s41598-025-86990-0. [last viewed: 29 September 2026].

ZHELEV, ZH., 2018. *Informatsionni operatsii i informatsionno vazdeystvie*. Sofia: Rakovski National Defence College. ISBN 978-619-7478-01-3. [in Bulgarian].

CIVIC RESILIENCE IN THE CONTEXT OF COGNITIVE IMPACTS ON THE PUBLIC CONSCIOUSNESS OF BULGARIANS IN THE WESTERN BALKANS

Abstract. Bulgarian citizens abroad are under the protection of the Bulgarian state. At the same time, preserving national identity is a matter of national interest. This study aims to analyze the cognitive impacts on the civic resilience of Bulgarian communities in the Western Balkans – specifically, Bulgarians in North Macedonia, Serbia, and Albania.

Keywords: Civic resilience; cognitive impacts; Western Balkans

Denitsa Kitanova, PhD Student
ORCID iD: 0009-0003-5639-810X
Faculty of National Security and Defence
Rakovski National Defence College
82, Evlogi i Hristo Georgievi Blvd.
E-mail: d.s.kitanova@rndc.bg

https://doi.org/10. 66334/annu26_artintsystsupp

ИЗКУСТВЕНИЯТ ИНТЕЛЕКТ В СИСТЕМАТА ЗА ПОДДРЪЖКА НА ВЗЕМАНЕТО НА РЕШЕНИЯ В СИСТЕМАТА ЗА СИГУРНОСТ И ОТБРАНА

д-р Деян Иванов
Сухопътно командване на НАТО

Абстракт. Докладът разглежда ролята и приложението на изкуствения интелект в системите за поддръжка на вземането на решения (Decision Support Systems – DSS) в системата за сигурност и отбрана. Интегрирането на изкуствен интелект в DSS има потенциал да повиши ефективността, точността и навременността в процеса на вземане на решение, като същевременно поставя нови изисквания към компетентностите на специалистите и към управлението на риска.

Ключови думи: изкуствен интелект; поддръжка на решения; сигурност; отбрана; човешки контрол

I. Увод

Вземането на решения е сред основните дейности в управлението на всяка организация. В условията на нарастваща сложност на средата, увеличаващи се обеми информация и съкращаващо се време за реакция, качеството на решенията придобива критично значение. Именно за подпомагане на този процес са създадени системите за поддръжка на вземането на ре-

шения (Decision Support Systems – DSS). Това са информационни системи, които предоставят на вземащия решение аналитична информация, модели и инструменти (Power 2002; Turban et al. 2005). Класическите DSS съчетават бази данни с аналитични модели, за да подпомогнат структурирането и анализа на управленски проблеми. С развитието на информационните технологии тези системи стават все по-мощни, като през последните години навлизането на изкуствения интелект открива нови възможности за тяхното усъвършенстване (Turban et al. 2005; Sauter 2010).

Изкуственият интелект представлява съвкупност от технологии, способни да изпълняват задачи, изискващи човешки интелект, като разпознаване на образи, анализ на данни, прогнозиране, обработка на естествен език. Интегрирането на тези технологии в системите за поддръжка на вземането на решения ги трансформира от пасивни инструменти за анализ в активни партньори, способни да откриват закономерности, да генерират варианти и да предоставят препоръки (Sauter 2010; Duan et al. 2019). Организациите във всички сектори, от бизнеса и публичната администрация до сигурността и отбраната, все по-често прибягват до системи, подпомагани от изкуствен интелект, за подкрепа на своите решения. Разбирането на възможностите, ограниченията и рисковете на тези системи е предпоставка за тяхното отговорно и ефективно използване (Duan et al. 2019; Tagarev 2007).

II. Изкуственият интелект в системата за поддръжка на решения

Системата за поддръжка на вземането на решения представлява интерактивна информационна система, предназначена да подпомогне вземащите решения при решаването на слабо структурирани и неструктурирани проблеми. За разлика от системите за автоматизирано управление, които вземат решения самостоятелно, DSS подпомагат човека, като му предоставят информация, анализ и варианти, оставяйки окончателното решение на неговата преценка (Power 2002; Turban et al. 2005). В системата за сигурност и отбрана тази концепция може да бъде разширена до система, която интегрира данни, модели, разузнавателна информация и експертни знания, за да подпомага командния и управленския състав при оценка на обстановката, разработване на варианти за действие и избор на решение.

Класическата структура на DSS обхваща няколко основни компонента, представени на фигура 1. Базата данни осигурява съхранението и достъпа до данните, необходими за анализа. Базата модели съдържа аналитични и прогнозни модели, чрез които данните се обработват. Потребителският

интерфейс осигурява взаимодействието между системата и вземащия решение. При по-развитите системи се добавя и база знания, съдържаща правила и експертни знания (Turban et al. 2005; Arnott & Pervan 2005).



Фигура 1. Компоненти на системата за поддръжка на вземането на решения

Интегрирането на изкуствен интелект добавя нов компонент към тази структура – модул, който прилага технологии като машинно обучение, анализ на данни и прогнозиране. Този модул не замества останалите компоненти, а ги обогатява, като повишава способностите на системата за анализ, откриване на закономерности и генериране на препоръки. По този начин изкуственият интелект трансформира DSS от инструмент за представяне на информация в система, способна да извлича знание от данните (Sauter 2010; Arnott & Pervan 2005).

Изкуственият интелект намира приложение в системите за поддръжка на вземането на решения по няколко основни направления (Duan et al. 2019; Provost & Fawcett 2013). Първото направление е анализът на данни. Изкуственият интелект позволява обработката на огромни обеми данни, недостъпни за ръчен анализ. Технологиите за машинно обучение откриват закономерности, тенденции и аномалии в данните, предоставяйки на вземащия решение информация, която иначе би останала скрита. Тази способност е особено ценна в условия на нарастващи обеми данни (Provost & Fawcett 2013; Duan et al. 2019). Второто направление е прогнозирането. Въз основа на исторически данни системите с изкуствен интелект изграждат модели, които прогнозират бъдещи събития и тенденции. Тези прогнози подпомагат планирането и предвиждането на последствията от различните варианти за действие. Прогнозната способност на изкуствения инте-

лект превръща DSS от инструмент за анализ на миналото в инструмент за предвиждане на бъдещето (Provost & Fawcett 2013; Phillips-Wren 2012). Третото направление е генерирането на варианти и препоръки. Изкуственият интелект може да генерира и оценява различни варианти за решение, като предоставя на вземащия решение структуриран набор от алтернативи с техните вероятни последствия. Това подпомага разглеждането на по-широк спектър от възможности, отколкото човекът би могъл да обхване самостоятелно (Duan et al. 2019; Phillips-Wren 2012). Четвъртото направление е взаимодействието на естествен език. Съвременните системи с генеративен изкуствен интелект позволяват на вземащия решение да формулира запитвания и да получава отговори на естествен език, което прави системите по-достъпни и по-лесни за използване. Това взаимодействие намалява бариерата пред използването на сложни аналитични инструменти[1] (Brynjolfsson & McAfee 2017).

2.1. Процес на вземане на решение с подкрепа от изкуствен интелект

Интегрирането на изкуствен интелект в процеса на вземане на решения не променя основната роля на човека, а обогатява отделните етапи на процеса. Фигура 2 представя този процес (Phillips-Wren 2012; Tagarev & Shalamanov 2019).



Фигура 2. Процес на вземане на решение с подкрепа от изкуствен интелект

Разглеждането на процеса на вземане на решение с подкрепа от изкуствен интелект налага по-подробен анализ на отделните му етапи. В теорията на вземането на решения се разграничават няколко последователни фази: идентифициране на проблема, събиране и анализ на информация, генериране на алтернативи, оценка на вариантите, избор и прилагане на решението. Изкуственият интелект намира приложение в почти всяка от тези фази: той разпознава аномалии и тенденции, сигнализиращи за възникващ проблем; обработва обеми данни, недостъпни за

ръчен анализ; предлага варианти за решение, които вземащият решение би могъл да пропусне и моделира вероятните последствия от всяка алтернатива (Provost & Fawcett 2013; Phillips-Wren 2012; Tagarev & Shalamanov 2019). Съществено е разбирането, че приносът на изкуствения интелект варира според характера на решението. При структурираните решения, които следват ясни правила и разполагат с достатъчно данни, изкуственият интелект може да предостави значителна подкрепа, доближаваща се до автоматизация. При слабо структурираните и неструктурираните решения, които изискват преценка и отчитане на уникален контекст, ролята на изкуствения интелект остава подчинена на човешката преценка (Turban et al. 2005; Tagarev & Shalamanov 2019).

Взаимодействието между човека и изкуствения интелект може да приеме различни форми, разположени в спектър според степента на автономност на системата. В единия край стои консултативният модел, при който изкуственият интелект предоставя препоръки, а човекът взема всички решения самостоятелно, в другия – автоматизираният модел, при който системата взема определени решения, а човекът упражнява надзор. Между тях се разполагат смесени модели, при които разпределението на функциите зависи от характера на задачата и от нивото на риска: при решения с висок залог човекът запазва пълен контрол, докато при рутинни решения е допустима по-висока степен на автоматизация[2] (Tagarev & Shalamanov 2019; Parasuraman & Manzey 2010). Оптималното взаимодействие се основава на принципа на взимното допълване – изкуственият интелект превъзхожда човека в обработката на големи обеми данни и в бързината на изчисленията, докато човекът превъзхожда системата в разбирането на контекста, в ценностната преценка и в поемането на отговорност. Добре проектираната система използва силните страни на всяка страна, като компенсира нейните ограничения (Tagarev & Shalamanov 2019; Jarrahi 2018).

2.2. Ползи и рискове от интегрирането на изкуствен интелект

Интегрирането на изкуствен интелект в системите за поддръжка на вземането на решения носи съществени ползи, които обосновават нарастващото му приложение. Фигура 3 обобщава основните ползи и рискове (Duan et al. 2019; Davenport & Harris 2007).

Основна полза от интегрирането на ИИ е повишаването на ефективността. Изкуственият интелект автоматизира трудоемки задачи по обработка и анализ на данни, което освобождава време и ресурси и ускорява процеса на вземане на решения. В условия на нарастваща сложност това

повишаване на ефективността е съществено предимство (Duan et al. 2019; Davenport & Harris 2007). Също така, чрез анализ на големи обеми данни и откриване на закономерности и модели изкуственият интелект може да предостави по-точна информация и по-надеждни прогнози, отколкото би било възможно при ръчен анализ. Тази точност подобрява качеството на основата, върху която се вземат решенията (Provost & Fawcett 2013; Davenport & Harris 2007). Не на последно място голямо предимство е навременността. Способността на изкуствения интелект да обработва информация бързо позволява вземането на решения в реално време или почти в реално време. В ситуации, изискващи бърза реакция, тази навременност може да бъде решаваща. Заедно тези предимства обосновават стойността на интегрирането на изкуствен интелект в системите за поддръжка на вземането на решения (Phillips-Wren 2012; Davenport & Harris 2007).



Фигура 3. Ползи и рискове от интегрирането на изкуствен интелект в DSS

Наред с ползите, интегрирането на изкуствен интелект в системите за поддръжка на вземането на решения поражда и съществени рискове и предизвикателства, чието разбиране е предпоставка за отговорно използване[3] (Parasuraman & Manzey 2010). Първият риск е прекомерното доверие в системата. Когато системата работи надеждно продължително време, вземащите решения могат да започнат да ѝ се доверяват безусловно, намалявайки собствената си проверка. Това явление, известно като автоматизирано пристрастие (automation bias), превръща надеждната система в източник на грешки, когато тя допусне пропуск, който остава непроверен[4] (Parasuraman & Manzey 2010). Друг риск е непрозрачността. Много съвременни системи с изкуствен интелект функционират като черна кутия, т.е. те произвеждат резултати, но начинът, по който достигат до тях, е труден

за разбиране. Тази непрозрачност затруднява проверката на препоръките и поемането на отговорност за решенията, основани на тях[5] (Mittelstadt et al. 2016). Третият риск е свързан с алгоритмичните предубеждения, а именно ако данните съдържат предубеждения, системата ги възпроизвежда с привидната обективност на технологията. Четвъртият риск засяга уязвимости към нови и специфични атаки, а петият риск е загубата на умения от човека поради прекомерно разчитане на системите[6] (Mittelstadt et al. 2016).

2.3. Изкуственият интелект в системата за командване и управление

Системите за поддръжка на вземането на решения, подпомогнати от изкуствен интелект, намират особено значимо приложение в областта на сигурността и отбраната. В тази област решенията често се вземат в условия на несигурност, натиск на времето и висок залог, което прави подкрепата от изкуствен интелект особено ценна (Tagarev & Shalamanov 2019; Scharre 2023). Военните приложения обхващат подпомагането на командването и управлението, оперативното планиране, анализа на разузнавателна информация и логистиката. В тези области изкуственият интелект обработва големи обеми данни, предоставя аналитична подкрепа и подпомага планирането, като ускорява и обогатява процеса на вземане на решения (Shim et al. 2002; Turban et al. 2005).

Едно от най-съществените приложения на ИИ е изграждането на единна и актуална картина на оперативната обстановка. В системите за командване и управление постъпват данни от радиолокационни средства, сензори, безпилотни платформи, комуникационни системи, разузнавателни структури, киберсензори и информационни системи на съюзни формирования. Чрез методи за машинно обучение и обработка на естествен език ИИ може да извлича съществени сведения от големи масиви структурирани и неструктурирани данни. Прилагането на алгоритми за многосензорно сливане подпомага съпоставянето на информацията, отстраняването на дублиранията и установяването на несъответствия между отделните източници. По този начин се създават условия за по-пълна, своевременна и контекстуализирана оперативна картина. Необходимо е обаче да се отчита, че автоматичното обединяване на данни не гарантира тяхната достоверност. При наличие на неточни сензори, преднамерена дезинформация или кибернетично компрометирани източници алгоритмите могат да формират неправилни оценки. Поради това системите следва да използват механизми за оценка на надеждността, проследимост на произхода на данните и представяне на степента на неопределеност.

ИИ може да подпомага щабовете и при идентифициране на тенденции, откриване на аномалии и оценяване на вероятни сценарии. Например чрез анализ на пространствени зависимости могат да бъдат откривани промени в активността на определени обекти, необичайни модели на движение или признаци за подготовка на действия. В разузнавателния процес ИИ е приложим при автоматизирана обработка на изображения, разпознаване на обекти, анализ на комуникационни потоци и извличане на събития от текстови източници. Това позволява на анализаторите да насочат усилията си към интерпретация, проверка и оценка, вместо да изразходват основната част от времето си за първична обработка на данни. Същевременно резултатите от алгоритмите не трябва да се приемат като окончателна истина. Оперативната оценка включва политически, правни, културни, морални и контекстуални фактори, които не могат да бъдат надеждно сведени единствено до статистически зависимости. Поради това ИИ следва да предоставя аргументирани предложения, а не да замества професионалната преценка на командния състав.

В процеса на оперативното планиране ИИ може да подпомага разработването и сравнението на варианти за действие. Системите могат да моделират различни комбинации от сили и средства, ограничения на времето и ресурсите, вероятни реакции на противника и възможни последствия от предприетите действия. Особено значение имат инструментите за подпомагане вземането на решения, които представят на командира няколко алтернативи, придружени от оценка на рисковете, необходимите ресурси и очакваните резултати. Това създава възможност за по-бързо сравнение на варианти и за идентифициране на критични зависимости, които могат да останат незабелязани при ръчен анализ. Практическата приложимост на подобен подход се потвърждава от изследователски дейности на НАТО, при които AI-базиран прототип е използван за автоматизирано извличане и обработка на критична информация и за подпомагане на процеса по формулиране на командирските информационни изисквания. Въпреки това използването на ИИ при планиране изисква повишено внимание. Моделите се обучават върху определени данни и допускания, поради което могат да се окажат недостатъчно надеждни при нестандартна или коренно променена обстановка. Следователно всяко автоматично генерирано предложение трябва да бъде проверявано спрямо намерението на командира, действащите правила за употреба на сила, наличните разузнавателни сведения и изискванията на международното хуманитарно право.

Интегрирането на изкуствен интелект в системите за поддръжка на вземането на решения поставя нови изисквания към компетентностите на личния състав, които ги използват. Съвременният специалист трябва да притежава разбиране, надхвърлящо традиционните управленски умения (Tagarev 2007; Jarrahi 2018). Първо, необходимо е технологично разбиране. Специалистът не е нужно да бъде експерт по изкуствен интелект, но трябва да разбира основните принципи на технологията, а именно как работят системите, какви са техните възможности и ограничения. Без такова разбиране специалистът не може да оцени критично препоръките на системата, нито да разпознае ситуации, в които тя може да греши (Tagarev 2007; Jarrahi 2018). Също така е необходимо критично отношение. Командирите трябва да поддържат критична преценка спрямо препоръките на системата, като ги разглеждат като подкрепа за решението, а не като готов отговор. Това критично отношение е противодействие на автоматизираното пристрастие и предпоставка за отговорно използване (Parasuraman & Manzey 2010; Jarrahi 2018). В допълнение е необходимо разбиране на данните. Тъй като качеството на препоръките зависи от качеството на данните, личният състав трябва да разбира произхода, ограниченията и възможните предубеждения на данните, върху които се основава системата. Не на последно място, необходимо е етично и правно разбиране на отговорностите, свързани с използването на изкуствен интелект при вземането на решения. Формирането на тези компетентности е задача на образованието и професионалната подготовка[7] (Jarrahi 2018).

III. Заключение

Настоящият доклад разгледа ролята и приложението на изкуствения интелект в системите за поддръжка на вземането на решения. Анализът показа, че интегрирането на изкуствен интелект трансформира тези системи, като разширява значително техните възможности за анализ, прогнозиране и генериране на препоръки. Интегрирането на изкуствен интелект в системите за поддръжка на вземането на решения има съществен потенциал да повиши ефективността, точността и навременността на процеса на вземане на решения. Изкуственият интелект обработва обеми данни, недостъпни за човека, открива скрити закономерности, прогнозира бъдещи тенденции и генерира варианти за решение. Тези способности обогатяват процеса на вземане на решения и предоставят на вземащите решения по-добра основа за техните избори.

Същевременно докладът подчертава, че този потенциал е съпроводен с нови изисквания и рискове. Прекомерното доверие, непрозрачността, алгоритмичните предубеждения и новите уязвимости са рискове, които изискват внимателно управление. Реализирането на ползите от технологията, при овладяване на нейните рискове, зависи от запазването на смисления човешки контрол, от прозрачността на системите и от систематичното управление на риска.

В заключение, изкуственият интелект е мощен инструмент за подпомагане на вземането на решения, но той не замества човешката преценка, контрол и отговорност. Добре проектираната и отговорно използвана система за поддръжка на вземането на решения усилва човешките възможности, вместо да ги замества. Именно в това единство на технологичните възможности и човешката преценка се крие потенциалът на изкуствения интелект да служи за по-доброто вземане на решения.

БЕЛЕЖКИ

1. БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ, 2020. *Изкуствен интелект за интелигентен растеж: предложение за Национална стратегия за развитие на изкуствения интелект в България до 2030 г.* [онлайн]. Достъпно на: https://www.strategy.bg/strategicdocuments/View.aspx?Id=1338. София: БАН. [Последно видян: 17.09.2026].

2. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), 2023. *Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100*-1 [online]. Available from: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf. Gaithersburg, MD: U.S. Department of Commerce. DOI: 10.6028/NIST.AI.100-1. [last viewed: 17.09.2026].

3. Пак там.

4. Пак там.

5. Пак там.

6. Пак там.

7. EUROPEAN COMMISSION, HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, 2019. *Ethics Guidelines for Trustworthy AI.* Brussels: European Commission [online]. Available from: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai. [last viewed: 17.09.2026].

8. МИНИСТЕРСКИ СЪВЕТ НА РЕПУБЛИКА БЪЛГАРИЯ, 2026. *Концепция за развитие на изкуствения интелект в България до 2030 г.* 2020 [онлайн]. Достъпно на: https://www.strategy.bg/strategicdocuments/View.aspx?Id=1338. София: Министерски съвет. [Последно видян: 17.09.2026].

9. DIGNUM, V., 2019. *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way.* Cham: Springer.

REFERENCES

ARNOTT, D. & PERVAN, G., 2005. Critical Analysis of Decision Support Systems *Research. Journal of Information Technology*, vol. 20, no. 2, pp. 67 – 87. London: SAGE Publishing. ISSN 1815-7432.

BRYNJOLFSSON, E. & McAFEE, A., 2017. The Business of Artificial Intelligence. *Harvard Business Review*, vol. 7, pp. 3 – 11. Boston, MA: Harvard Business School Publishing Corporation. ISSN 0017-8012.

DAVENPORT, T. & HARRIS, J., 2007. *Competing on Analytics: The New Science of Winning.* Boston, MA: Harvard Business School Press.

DUAN, Y.; EDWARDS, J. & DWIVEDI, Y., 2019. Artificial Intelligence for Decision Making in the Era of Big Data: Evolution, Challenges and Research Agenda. *International Journal of Information Management,* vol. 48, pp. 63 – 71. DOI: 10.1016/j. ijinfomgt.2019.01.021.

JARRAHI, M., 2018. Artificial Intelligence and the Future of Work: Human-AI Symbiosis in Organizational Decision Making. *Business Horizons*, vol. 61, no 4, pp. 577 – 586. ISSN 0007-6813.

MITTELSTADT, B.; ALLO, P.; TADDEO, M.; WACHTER, S. & FLORIDI, L., 2016. The Ethics of Algorithms: Mapping the Debate. *Big Data & Society*, vol. 3, no 2, pp. 1 – 21. ISSN 2053-9517.

PARASURAMAN, R. & MANZEY, D., 2010. Complacency and Bias in Human Use of Automation: An Attentional Integration. *Human Factors*, vol. 52, no 3, pp. 381 – 410. DOI: 10.1177/0018720810376055.

PHILLIPS-WREN, G., 2012. AI Tools in Decision Making Support Systems: A Review. *International Journal on Artificial Intelligence Tools*, vol. 21, no 2. ISSN 0218-2130.

POWER, D., 2002. *Decision Support Systems: Concepts and Resources for Managers.* Westport, CT: Quorum Books. ISBN 156720497X.

PROVOST, F. & FAWCETT, T., 2013. *Data Science for Business: What You Need to Know about Data Mining and Data-Analytic Thinking.* Sebastopol, CA: O'Reilly Media.

SAUTER, V., 2010. *Decision Support Systems for Business Intelligence*, 2nd ed. Hoboken, NJ: John Wiley & Sons.

SCHARRE, P., 2023. *Four Battlegrounds: Power in the Age of Artificial Intelligence*. New York: W. W. Norton & Company.

SHIM, J.; WARKENTIN, M.; COURTNEY, J.; POWER, D.; SHARDA, R. & CARLSSON, CH., 2002. Past, Present, and Future of Decision Support Technology. *Decision Support Systems*, vol. 33, no 2, pp. 111 – 126. ISSN 1873-5797.

TAGAREV, T., 2007. *Metodologiya i situatsionni stsenarii za planirane na otbranata i vaorazhenite sili*. Sofia: Voenno izdatelstvo. [in Bulgarian].

TAGAREV, T. & SHALAMANOV, V., 2019. *Upravlenie na resursite za otbrana i izgrazhdane na sposobnosti: metodologiya i prilozheniya*. Sofia: Institut po otbrana „Profesor Tsvetan Lazarov". [in Bulgarian].

TURBAN, E.; ARONSON, J. & LIANG, T.-P, 2005. *Decision Support Systems and Intelligent Systems*, 7th ed. Upper Saddle River, NJ: Pearson Prentice Hall. ISBN 9780130461063.

ARTIFICIAL INTELLIGENCE IN THE DECISION-MAKING SUPPORT SYSTEM WITHIN THE SECURITY AND DEFENCE SYSTEM

Abstract. The paper examines the role and application of artificial intelligence in Decision Support Systems (DSS) within the security and defence system. The integration of artificial intelligence into DSS has the potential to enhance the efficiency, accuracy, and timeliness of the decision-making process, while simultaneously creating new requirements regarding the competencies of specialists and risk management.

Keywords: artificial intelligence; decision support; security; defence; human-in the-loop

Dr. Deyan Ivanov
NATO LANDCOM HQ
General Vecihi Akin Garrison
35380 Izmir, Türkiye
E-mail: deyan_ivanov@abv.bg

https://doi.org/10. 66334/annu26_suvrpro

СЪВРЕМЕННИ ПРОЕКЦИИ НА АРМЕНСКО-АЗЕРБАЙДЖАНСКИТЕ ОТНОШЕНИЯ И ЕВРОПЕЙСКАТА СИГУРНОСТ

гл. ас. д-р Димитър Дринков
Военна академия „Георги Стойков Раковски“

Абстракт. Южен Кавказ все по-отчетливо се превръща в ключов за европейската сигурност регион. Важността му от гледна точка на енергетиката, инвестиционния, транспортния и логистичния потенциал е сред основните причини за извеждането на тази част от света като особено значима за Брюксел в новата стратегия на Европейския съюз за Черноморския регион от май 2025 г. Реализацията на европейските приоритети обаче в голяма степен е обвързана с бъдещите проекции на отношенията между историческите противници Армения и Азербайджан.

Ключови думи: Южен Кавказ; енергетика; коридори; европейска сигурност; Армения; Азербайджан

Въведение

През XXI век структурната конфигурация на системата на регионална сигурност в Южен Кавказ се оформя като един от основните стълбове във външната политика и политика за сигурност на Европейския съюз

(ЕС). Транспортният, логистичният и енергийният потенциал на региона, свързващ Източна Европа и Западна Азия, Черно и Каспийско море, повишават значително геостратегическата му тежест за Брюксел и същевременно го превръщат в пресечна точка на интересите на глобални и регионални сили. Уникалността на тази част от света се допълва от богатата палитра от етнически и религиозни общности, която, от една страна, оставя след себе си забележително културно-историческо наследство, но от друга, се превръща в предпоставка за етнически конфликти, водещи до външна намеса и ендемична нестабилност. За дълги години именно втората тенденция се превръща в своеобразна визитна картичка на Южен Кавказ. Понастоящем обаче е налице безпрецедентна възможност за установяването на стабилността като основна характеристика на средата за сигурност в региона. Макар и сепаратистките конфликти в Южна Осетия и Абхазия все още да запазват „замразения“ си статут, мирът между историческите противници Армения и Азербайджан, чиито антагонистични отношения са основен катализатор на регионална несигурност за повече от три десетилетия, изглежда все по възможен сценарий, който има перспектива да „отключи“ потенциала на Южен Кавказ в разнообразни геоикономически направления. От тази гледна точка детайлният анализ на съвременните проекции на отношенията по оста Баку – Ереван е задължителна предпоставка за ефективна външна политика на всяка страна, международна организация или интеграционна общност, имаща амбиции за активно участие в процесите на сигурност и сътрудничество в региона.

Изложение

Настоящите измерения на арменско-азербайджанските отношения са пряко обвързани с дългогодишната история на конфликтност по оста Баку – Ереван. Напрежението между арменци и мюсюлмани е налице още през първата половина на XIX век, но именно през следващото столетие двата кавказки народа се изправят един срещу друг в няколко кървави конфликта. Разпадът на Руската империя води до краткотрайно съществуване на Армения и Азербайджан като независими републики и още в този период започват да се отличават непреодолимите противоречия между двете страни. Утвърждаването на болшевиките в Южен Кавказ през 20-те години и сформирането впоследствие на Съюза на социалистическите съветски републики (СССР) – с Азербайджан и Армения като съставни републики, оставя за дълги години националните противоречия на заден план,

особено на фона на усилията за формирането на съветска нация. Въпреки това националните каузи и стремежи на арменци и азербайджанци не са изкоренени и казусът, свързан със статута на новосформираната Нагорно-карабахска автономна област (НКАО), е доказателство за това. Макар и областта да има явен арменски облик в демографски план, тя официално е присъединена като автономна административна единица в рамките на Азербайджанската ССР през 1923 г.

В следващите десетилетия видни арменски комунисти многократно повдигат въпроса за присъединяването на НКАО към Арменската ССР пред централните власти в Москва, но исканията им така и не се увенчават с успех (Coyle 2018, p. 212). Проникването на идеите на национализма в СССР през 80-те години и възраждането на стремежите за независимост на населяващите най-голямата страна в света народи извеждат отново на преден план дълго потискани етнорелигиозни противоречия. Особено сериозни са те именно между арменци и азербайджанци. Кулминацията на множеството кървави сблъсъци между двете общности е Сумгаитският погром срещу арменците от февруари 1988 г., който явно показва, че пътят на конфронтация е неизбежен. Впоследствие Първата Нагорнокарабахска война, приключила с подписването на Протокола от Бишкек през 1994 г., не само не довежда до мирно съвместно съществуване между двете съседни страни, но създава предпоставки за нова ескалация вследствие на създаването на квазидържавния субект Нагорно-Карабахска република и своеобразното „замразяване“ на конфликта.

Коренно нова насока на отношенията между Армения и Азербайджан дават две събития от настоящото десетилетие – Втората Нагорнокарабахска война от есента на 2020 г. и цялостното овладяване на Нагорни Карабах от Азербайджан три години по-късно. Именно окончателното разрешаване на конфликта, макар и постигнато не посредством инструментите на дипломацията, а чрез използването на военна сила, отваря напълно нова страница в отношенията между Баку и Ереван. Кардинално променениият баланс във военен план, изолацията на древната християнска държава от значими регионални проекти в сферата на икономиката, транспорта и енергетиката, от една страна, и постигането на азербайджанската първостепенна цел за установяване на пълен контрол върху международно признатите си граници, от друга, създават ситуация, в която конфликтът не изглежда желан и от двете републики. Така настоящият исторически и геополитически контекст създава възможности за утвърждаването на мира и сътрудничеството като основна характеристика на съвременните арменско-азербайджански отношения.

Периодът след 2023 г. поставя основите на историческа трансформация на отношенията между двете бивши съветски републики и преминаването към директен дипломатически диалог. Кулминацията на този процес е подписаното на 8 август 2025 г. във Вашингтон споразумение. Макар, и вероятно прибързано, то да е наречено от определени политически фигури и анализатори мирен договор, тъй като ратификация на документа към септември 2026 г. все още не е налице, то несъмнено е особено значима пътна карта към постигането на такава цел. В споразумението могат да се отличат няколко важни пункта, които недвусмислено трасират прехода към мир между Баку и Ереван. На първо място, страните се договарят взаимно да зачитат териториалната си цялост на базата на установените административни граници между тях от съветския период – тоест границите на Арменската ССР и Азербайджанската ССР[1]. Освен това Армения и Азербайджан се задължават да се въздържат от употреба на сила или заплаха срещу териториалната цялост или политическата независимост на другата страна[2], както и да установят дипломатически отношения след ратификацията на документа и от двете републики[3]

Внимание привлича и ангажиментът да не се разполагат по общата граница сили на трети страни. По този пункт противоречия възникват най-вече от гледна точка на присъствието на мисията на ЕС в Армения (EUMA), чиято основна цел е да наблюдава и докладва за ситуацията на място (по арменската страна на границата), да допринася за сигурността на хората в засегнатите от конфликта райони и да подпомага изграждането на доверие между Армения и Азербайджан[4]. Докато Армения изтъква аргумента, че мисията има строго цивилен характер, тъй като европейските наблюдатели не носят оръжие и не изпълняват отбранителни функции, Азербайджан поддържа тезата, че присъствието на EUMA нарушава чл. 7 от Вашингтонското споразумение, настоявайки сигурността в региона да се крепи единствено на двустранни механизми за изграждане на доверие. Всичко това прави присъствието на мисията несигурно (макар и мандатът ѝ да е до 2027 г.), тъй като е вероятно Армения да поиска постепенното ѝ изтегляне с цел да не се застрашава окончателното подписване на мирен договор. Значимо от гледна точка на международното публично право е и фиксираното в чл. 15 задължение на страните да оттеглят всички междудържавни искове, жалби, протести, възражения, производства и спорове, свързани с въпросите, съществували помежду им преди подписването на споразумението[5]. Реализацията на ангажиментите по този пункт на практика все още не е факт, тъй като към септември 2026 г. продължават да

се разглеждат няколко знакови дела, заведени от двете страни – исковете на Армения и Азербайджан в Международния съд на Организацията на обединените нации (ООН), обвиняващи насрещната страна в етническо прочистване, жалби в Европейския съд по правата на човека по казуси, касаещи изчезнали хора, изтезания на военнопленници, незаконни съдебни процеси срещу задържани лица, умишлено разрушаване на цивилно имущество, както и дела към Постоянния арбитражен съд в Хага срещу Армения по обвинения в причиняване на мащабни екологични щети и незаконно експлоатиране на енергийни ресурси в Нагорни Карабах.

Макар и горепосочените двустранни въпроси да са от особено значение за бъдещите проекции на арменско-азербайджанските отношения, то несъмнено на срещата на върха във Вашингтон от 8 август 2025 г. друга тема привлича в най-голяма степен вниманието на международната общност – Зангезурският коридор или „Пътят на Тръмп за международен мир и просперитет“ (TRIPP). Трасето представлява стратегически транспортен проект с дължина от малко над 40 км, който свързва територията на Азербайджан с екслава ѝ (Нахичеванска автономна република) през арменската Сюникска област. Събитията след Втората Нагорнокарабахска война и явната промяна в баланса на силите в полза на Азербайджан будят сериозни опасения в Ереван, че Баку би потърсил всякакъв начин да си осигури контрол върху трасето – дали чрез своеобразен екстериториален статут, тоест извън юрисдикцията на Армения, или чрез директно използване на военна сила. Във Вашингтон обаче е дадено началото на проекта TRIPP, разглеждан като изгоден и за двете кавказки страни. Постигнати са договорености за икономическо развитие на коридора под американско попечителство, като за целта се създава компанията TRIPP Development Company, която да има основна роля в изграждането на железопътна инфраструктура (железопътни линии, терминали, гари), пътна инфраструктура (магистрали, пътища, мостове, тунели), енергийна инфраструктура (електропреносни мрежи, нефтопроводи, газопроводи), цифрова инфраструктура (оптични мрежи) и спомагателна инфраструктура (административни съоръжения, комунални услуги, системи за безопасност и сигурност) в съответствие с арменското законодателство[6]. Правото за развитие на коридора от страна на САЩ е за срок от 99 години. Ползите са налице и за трите замесени държави – Вашингтон си гарантира значимо логистично и геополитическо присъствие в Южен Кавказ (по границата с Иран), Азербайджан слага край на своеобразната изолация на Нахичеванската автономна република, а за Армения се създават надеждни предпоставки за икономическа интеграция

в Южен Кавказ вследствие на евентуално нормализиране на отношенията със съседните Турция и Азербайджан. От своя страна, Турция също подкрепя инициативата, тъй като подобен проект би улеснил достъпа ѝ до близкия съюзник Азербайджан (единствената сухопътна граница между двете страни е именно на територията на Нахичеванската автономна република), а оттам и до Каспийско море и Централна Азия където Анкара се стреми да се позиционира като значим геополитически играч. Въпреки че са налице сериозни инженерни предизвикателства за реализирането на проекта – като например географските специфики на местността, характеризиращи се голямата надморска височина и планински релеф, реализирането му вече е в ход. Изграждането на нови железопътни и пътни проекти на азербайджанска територия напредва с бързи темпове, като очакванията са двата проекта да достигнат арменската граница до началото на 2027 г.[7]. От арменска страна инфраструктурата трябва да започне да се изгражда до края на настоящата 2026 г.

В последната година са налице няколко безпрецедентни момента на сътрудничество между Армения и Азербайджан, даващи сериозни поводи за оптимизъм за неизбежност на процеса на нормализация в отношенията им. Сериозен напредък е постигнат в хода на делимитацията и демаркацията на границите, макар и понастоящем да се наблюдава период на застой по този въпрос поради липса на консенсус по отношение на определянето на следващите участъци за демаркация. Същевременно още преди подписването на Вашингтонското споразумение са осъществени няколко кръга на размяна на военнослужещи и задържани лица. В края на 2023 г. пък Армения оттегля кандидатура си за домакинство на глобалната климатична конференция COP29 в полза на източната си съседка, а от своя страна, Баку се застъпва за членство на Ереван в Бюрото на Източноевропейската група за същата климатична рамка под егидата на ООН. В рамките на последната година – след срещата на върха във Вашингтон, Азербайджан едностранно отменя всички ограничения за транзита по отношение на Армения, като през територията на мюсюлманската република са превозени близо 60 000 тона стоки от и към Армения[8]. Азербайджан също така доставя 20 000 тона нефтопродукти на Армения, а Баку и Ереван продължават да работят за увеличаване на двустранната търговия[9]. Междувременно националните оператори на двете държави – AzerTelecom и Telecom Armenia, подписват през юни 2026 г. споразумение за транзит на интернет през териториите си, с което да се разнообразят маршрутите за регионална свързаност, да се повиши надеждността и устойчивостта в Южен Кавказ и да се подкре-

пи развитието на инфраструктурата в евразийските телекомуникационни мрежи[10]. Въпреки всички тези примери за сътрудничество, все още остава една сериозна пречка пред окончателното финализиране на мирния процес – азербайджанското настояване за промяна на арменската конституция. Искането е насочено към преамбюла на действащата конституция, който съдържа директна препратка към Декларацията за независимост на Армения от 1990 г. Проблемът се състои в частта на декларацията, цитираща съвместно решение от 1989 г. на Върховния съвет на Арменската ССР и Националния съвет на Арцах (Нагорни Карабах) относно „Обединението на Арменската ССР и планинския район Карабах“[12]. Макар и Армения да няма военния потенциал и политически амбиции за подобни действия, Баку разглежда този въпрос като скрита законово заложена териториална претенция към Азербайджан. Понастоящем управляващата партия в Армения „Граждански договор“ няма необходимото мнозинство за осъществяване на конституционни промени. Налице е необходимост от провеждането на национален референдум, като премиерът Пашинян се стреми да подготви проект за целта до края на годината, но същевременно е необходимо да се има предвид поляризацията на общественото мнение в бившата съветска република, поставяща под сериозен риск евентуален успех на националното допитване.

Заключение

Позитивните тенденции в арменско-азербайджанските отношения в последните три години несъмнено са безпрецедентна стъпка към завършване на мирния процес между историческите южнокавказки противници Армения и Азербайджан. Подобен сценарий би позволил значително задълбочаване на процесите на сигурност и сътрудничество в Европа, като същевременно би създал и предпоставки за все по-значима роля на ЕС в ключовия за съвременната архитектура на глобална сигурност Южен Кавказ. Интензивното сътрудничество с Азербайджан в енергийната сфера и близките политически връзки с арменското правителство, особено след разрешаването на казуса Нагорни Карабах, и все по-явната мултивекторна политика на Ереван, отдалечаваща го от Москва, извежда тази част от света като стратегически важна за външната политика и политика за сигурност на Брюксел. Свидетелство за това е мястото на Южен Кавказ в Стратегията на ЕС за Черноморския регион от май 2025 г. Бъдещето на тези позитивни за европейската сигурност тенденции обаче е пряко обвързано

с утвърждаването на мира в исторически размирния регион. Въпреки несъмнените стъпки напред от последните години, не трябва да се подценяват историческата вражда и подозрения, които все още съществуват между двата народа. Белезите от миналото обикновено битуват дълги години в паметта на един народ, но най-големият показател за зрелостта на дадена нация винаги е способността да прощава. Именно такива са надеждите и по отношение на един от най-кървавите конфликти от изминалите десетилетия, защото, както пише британският философ Бъртранд Ръсел, „войната не решава кой е прав, а само кой остава“.

БЕЛЕЖКИ

1. Ministry of Foreign Affairs and International Trade of the Republic of Armenia, 2025. *Agreement on Establishment of Peace and Inter-State Relations between the Republic of Armenia and the Republic of Azerbaijan*, Article 1, [11 August, 2025]. [online]. Available from: https://www.mfa.am/en/press-releases/2025/08/11/Initialed%20Arm-Az%20Peace%20Agreement%20text/13394. [Last viewed: 24 September 2026].

2. Пак там, чл. 3.

3. Пак там, чл. 5.

4. EU Mission in Armenia, 2023. *About European Union Mission in Armenia.* [online]. Available from: https://www.eeas.europa.eu/european-union-mission-armenia/about-european-union-mission-armenia_en?s=410283. [Last viewed: 25 September 2026].

5. Ministry of Foreign Affairs and International Trade of the Republic of Armenia, 2025. *Agreement on Establishment of Peace and Inter-State Relations between the Republic of Armenia and the Republic of Azerbaijan*, Article 15, [11 August, 2025]. [online]. Available from: https://www.mfa.am/en/press-releases/2025/08/11/Initialed%20Arm-Az%20Peace%20Agreement%20text/13394. [Last viewed: 25 September 2026].

6. U. S. Department of State, 2026. *The TRIPP Implementation Framework (TIF),* p. 4. [online]. Available from: https://www.state.gov/wp-content/uploads/2026/01/TRIPP-Implementation-Framework.pdf. [Last viewed: 26 September 2026].

7. Trend News Agency, 2026. *Zangezur corridor's Armenian section set for co nstruction start in 2026*. [online]. Available from: https://www.trend.az/azerbaijan/politics/4212541.html. [Last viewed: 26 September 2026].

8. U. S. Embassy in Azerbaijan, 2026. *Joint Statement of the United States of America, Armenia, and Azerbaijan on the One-Year Anniversary of the White House Peace Summit* [10 August 2026]. [online]. Available from: https://az.usembassy.gov/joint-statement-peacesummit/. [Last viewed: 27 September 2026].

9. Пак там.

10. Euronews, 2026. *Armenia and Azerbaijan agree landmark internet deal as peace process continues*. [online]. Available from: https://www.euronews.com/2026/06/23/armenia-and-azerbaijan-agree-landmark-internet-deal-as-peace-process-continues. [Last viewed: 27 September 2026].

11. Constitutional Court of Republic of Armenia, 1990. *Armenian Declaration of Independence* [23 August 1990]. [online]. Available from: https://www.concourt.am/en/normative-legal-bases/declaration. [Last viewed: 28 September 2026].

REFERENCES

COYLE, J., 2018. *Russia's Border Wars and Frozen Conflicts.* CA: Center for Global Education Chapman University Orange. ISBN 978-3-319-84848-8.

CONTEMPORARY DIMENSIONS OF ARMENIAN-AZERBAIJANI RELATIONS AND EUROPEAN SECURITY

Abstract. The South Caucasus is increasingly emerging as a region of key importance to European security. Its importance in terms of energy, investment, transportation and logistics potential is among the main reasons why this part of the world was identified as particularly significant for Brussels in the EU's new strategy for the Black Sea region, adopted in May 2025. However, the realization of European priorities is largely tied to the future trajectory of relations between the historic adversaries Armenia and Azerbaijan.

Keywords: South Caucasus; energy; corridors; European security; Armenia; Azerbaijan

Dr. Dimitar Drinkov, Assist. Prof.
ORCID iD: 0000-0002-5742-1004
National and International Security Department
National Security and Defence Faculty
Rakovski National Defence College
1504 Sofia, Bulgaria
E-mail: d.n.drinkov@rndc.bg

https://doi.org/10. 66334/annu26_aicyberrole

РОЛЯТА НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ В КИБЕРСИГУРНОСТТА

Димитър Малкочев
Военна академия ,,Георги Стойков Раковски“

Абстракт. Публикацията акцентира върху ролята на изкуствения интелект в киберсигурността като начин за откриване на нетипично поведение в мрежите, което би могло да застраши сигурността на системите и данните в организацията.

Ключови думи: киберсигурност; извличане на информация; изкуствен интелект; поведенчески анализ; разпознаване на модели; сигурност на мрежи и системи

Актуалност на проблема

През последните години ролята на изкуствения интелект става все по-голяма, поради внедряването му в бизнеса и други инструменти за обработка на данни. Все по-често изкуственият интелект се използва в софтуери, които спомагат за бързото решаване на рутинни задачи. Много организации се опитват да разберат как биха могли да използват изкуствения интелект, за да подобрят сигурността на системите си. Това се превръща в голямо предизвикателство, като се има предвид недостигът на квалифицирани експерти, които да притежават умения за работа с изкуствен интелект и мрежова сигурност. В този контекст софтуерът с изкуствения интелект е чудесен инструмент за откриване и предотвратяване на злонамерени атаки, насочени срещу организациите.

Изследванията на изкуствения интелект (ИИ; на англ. *Artificial intelligence – AI*) се определят като изучаване на „интелигентни агенти“. Всяко устройство, което възприема околната среда и предприема действия, които увеличават шансовете му за успешно постигане на целите му, може да се определи като форма на „интелигентен агент“. Дейвид Никастро определя ИИ като „способността на дадена система да интерпретира правилно външни данни, да се учи от тези данни и да използва тези знания за постигане на конкретни цели и задачи чрез гъвкаво адаптиране“[1].

Границите, до които достига изкуственият интелект, са противоречиви, тъй като машините стават все по-способни, задачите, изискващи „интелект“, често се премахват от определението явление, известно като ефект на изкуствения интелект, което води до заключението в Теоремата на Теслер: „ИИ е всичко, което още не е направено“[2]. Съвременните възможности на машините, които обикновено се класифицират като изкуствен интелект, обхващат разбиране на човешка реч, съревнование на най-високо ниво в системи за стратегически игри, автономно управление на автомобили и интелигентно маршрутизиране в мрежи за пренос на данни и военни симулации.

Никастро класифицира изкуствения интелект в три различни типа системи за ИИ: аналитичен, вдъхновен от човека и хуманизиран изкуствен интелект. Аналитичният изкуствен интелект притежава характеристики, съответстващи на когнитивния интелект, като генерира когнитивно представяне на света и се самообучава на база отминал опит, за да информира за бъдещи решения. Вдъхновеният от човека AI се характеризира с елементи от когнитивния, както и от емоционалния интелект, като освен когнитивните елементи разбира и човешките емоции, отчитайки ги при вземането на решения. Хуманизираният ИИ показва характеристики на всички видове компетентности (т.е. когнитивна, емоционална и социална интелигентност), като е в състояние да се самоосъзнава и при взаимодействието с другите.[3]

Според Европейската комисия „Изкуственият интелект (AI) се отнася до системи, които проявяват интелигентно поведение, като анализират заобикалящата ги среда и предприемат действия, с известна степен автономност за постигане на конкретни цели“[4].

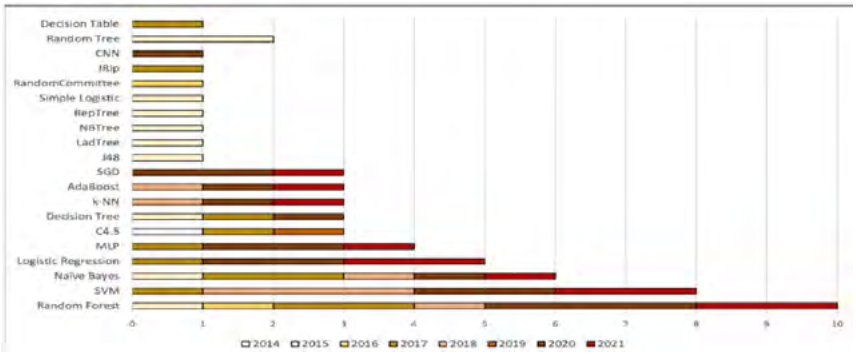
Технологиите с използването на изкуствен интелект в киберсигурността преминават през етапи на разработване, внедряване и експлоатация. Изкуственият интелект предоставя много възможности, които могат да се прилагат за широк спектър от задачи в различни области. В зависи-

мост от конкретния проблем и наличието на данни, техниките за машинно обучение могат да бъдат адаптирани и приложени, за да се постигнат точни прогнози и класификации (Loiko 2020). Изкуственият интелект има голямо предимство при интегрирането му в инструментите за защита на системите. Като негови предимства се определят:

– Ускоряване на реакцията при киберинцидент за сметка на автоматизирането на рутинните процеси;

– Поведенчески анализ на потребителите и системите;

– Намиране на неизвестни досега опасности и уязвимости.



Фигура 1. Използване на базовите модели за машинно обучение (Kotenko 2023, p. 14)

При решаването на проблеми в киберсигурността се прилагат следните модели, които демонстрират гъвкавостта на машинното обучение:

• Класификация – при нея основната задача е разпределянето на входни данни в предварително определени категории или класове. Впоследствие при това разпределение по класове се прилагат използвани от предишни наблюдавани данни и може да се приложи към нови неизвестни данни, които могат да бъдат класифицирани. Класификацията се използва широко в киберсигурността за откриване на злонамерено съдържание за зловреден софтуер, както и за фишинг и спам имейли. За тези видове приложения класификацията изисква примери както на доброкачествено, така и на злонамерено съдържание, които искаме да разграничим (Haider, Baig, Imran 2020).

• **Откриването на аномалии** е задача за идентифициране на модели или случаи, които се отклоняват значително от това, което се приема за нормално или очаквано в дадена система или набор от данни. То функционира чрез установяване на базова линия на нормално поведение и след това маркиране на всички точки данни или събития, които излизат извън тази

установена норма. Откриването на аномалии обикновено се използва в киберсигурността за установяване на базова линия на „нормално“ поведение в рамките на мрежа или система. След това отклоненията от тази базова линия се наблюдават непрекъснато и всички аномалии се маркират като индикация за потенциални заплахи за сигурността или компрометиране на системата.

• **Поведенческият анализ** е задача, близка до откриването на аномалии. Той включва изучаване и разбиране на типичните модели на поведение в дадена система, мрежа или дейност на потребителя. За разлика от откриването на аномалии, поведенческият анализ не се фокусира единствено върху отклоненията или аномалиите. Вместо това той има за цел да разбере обичайното или очакваното поведение на субектите в рамките на дадена система.

Анализът често включва създаване на профили на нормалното поведение на потребителите, устройствата или системите въз основа на исторически данни, действия на потребителите и дейности на системата. Идентифицирането на отклонения или промени от създадените профили може да показва потенциални рискове за сигурността, като например вътрешни заплахи или неоторизиран достъп.[58]

• **Разпознаването на модели** включва автоматичното откриване на значими модели в набори от данни. То позволява на системите да разпознават и тълкуват информация, атрибути или характеристики, които се повтарят или показват сходства, показателни за търсените модели. Разпознаването на образи се използва най-вече в киберсигурността под формата на извличане на признаци – процес на извличане на подходящи признаци от данни, които да представят интересуващите ни модели. В киберсигурността моделите на интерес обикновено са злонамереното съдържание и поведение, от които се извлича подпис. След това сигнатурите се използват за съпоставяне на модели и идентифициране на известни опити за фишинг, заразяване със зловреден софтуер, злонамерено поведение на потребителите и др. Приложенията на разпознаването на образи обикновено са противоположни на откриването на аномалии и поведенческия анализ, тъй като то има за цел да моделира специфично злонамерено съдържание и поведение, а не общо доброкачествено поведение (Loiko 2020).

Изкуственият интелект може да се използва и в помощ на експертите по киберсигурност. Целта на тези възможности е да се рационализират процесите на вземане на решения и да им се даде възможност да концентрират експертния си опит там, където той е най-ефективен.

• **Клъстеризацията** е техника за машинно обучение, която се използва за групиране на подобни точки от данни въз основа на присъщите им характеристики или особености. Тя има за цел да намери естествени групи или клъстери в набор от данни без предварително определени етикети или класове. Клъстеризацията може да се използва за подпомагане на анализа и категоризацията на голям обем данни за разузнаване на заплахи или идентифициране и групиране на различни варианти на зловреден софтуер. То може да се комбинира и с поведенчески анализ за групиране и идентифициране на различни потребителски или системни профили.

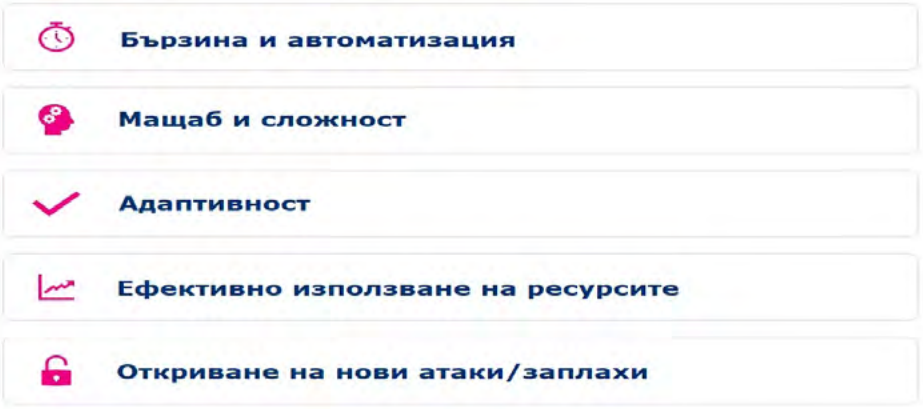
• **Извличането на информация** е задачата за извличане на полезна информация от съдържание, което съвпада или е семантично подобно на дадена заявка. Извличането на информация може да се използва за разузнаване на заплахи. Алгоритмите с изкуствен интелект могат да обработват, анализират, обобщават и категоризират големи обеми данни за разузнаване на заплахи от различни източници, като помагат на екипите по сигурността да идентифицират и реагират по-ефективно на възникващи заплахи.

• **Класирането** се отнася до задачата за подреждане на набор от елементи в определен ред въз основа на техните релевантност, важност или вероятност да отговорят на нуждите или предпочитанията на потребителя. ИИ извършва класиране, като се учи от маркирани или вече групирани данни, за да създаде модел за ранжиране. Ранжирането обикновено се използва в киберсигурността за определяне на приоритетите на усилията на експертите по сигурността. То може да се използва за приоритизиране при откриване на уязвимости в управлението на уязвимостите и за сортиране на инциденти в процесите за реагиране на инциденти или на събития в системите за управление на информацията и събитията в сигурността (SIEM).

• **Генерирането** е задачата за създаване на ново съдържание, което отговаря на предварително определена целева дистрибуция. Генерирането може да се използва в киберсигурността за оценка на уязвимостите и тестване за проникване. Инструментите за генериране, базирани на изкуствен интелект, могат да се използват за симулиране на атаки и идентифициране на уязвимости в системите или мрежите. Това може да помогне на организациите да открият уязвимости, преди да бъдат използвани, за да укрепят проактивно защитата си.

Приемането на решения, базирани на изкуствен интелект, за решаване на конкретен проблем на киберсигурността не е безпроблемен преход.

Като цяло експертите по киберсигурност не са запознати с техниките на ИИ и ползите от тях. В резултат на това конвенционалният подход разчита на човешкия опит и оперативните задачи, докато те не се окажат неподходящи. Въпреки това, когато организациите все пак изберат ИИ, те често търсят и често постигат следните ползи, представени на фигура 2.



Фигура 2. Ползи от изкуствения интелект в киберсигурността

Бързина и автоматизация. Кибератаките могат да се развият за няколко секунди и е необходима бърза реакция, за да се смекчат и сведат до минимум последиците от тях. Цифровите среди генерират огромно количество данни, които са от значение за мониторинга на сигурността – например файлове, обекти, събития, сигнали за сигурност и др. Анализирането на заплахите и ефективното им противодействие, представлява голямо предизвикателство за служителите по киберсигурност. Изкуственият интелект дава възможност за обработка и анализ на мащабни и разнообразни източници на данни в реално време. Той може да обобщава, наблюдава и извлича модели от големи количества сложни данни за много кратко време. Автоматизацията, управлявана от ИИ, може да рационализира процесите на реагиране при инциденти, като позволява по-бързи и по-ефективни действия за ограничаване, смекчаване и възстановяване от нарушения на сигурността (Patel 2023).

Мащаб и сложност. Съвременните цифрови среди са все по-сложни и изложени на множество заплахи. Огромното количество данни за мониторинг на сигурността трябва да се анализират своевременно, въпреки големия им мащаб. Изкуственият интелект в софтуерите за наблюдение на мрежите позволява мащабиране на операциите по киберсигурност, като

позволява на организациите да обработват ефективно огромни количества данни, независимо от мащаба или сложността (Li 2018).

Адаптивност. Киберсигурността се характеризира с постоянно променящи се заплахи. Това изисква защитата да се развива със същото темпо. Правилата за откриване трябва да се предефинират или адаптират, да се извлекат сигнатури от нов зловреден софтуер, да се идентифицират модели на нови атаки и т.н. Моделите на ИИ могат бързо да се учат от актуализираните данни с помощта на автоматизирано преквалифициране, което не изисква да се променят дизайнът или характеристиките на моделите на ИИ. Те могат да се адаптират към променящите се модели на атаки, което повишава способността им да откриват и предотвратяват нови заплахи.

Ефективно използване на ресурсите. Експертизата в областта на сигурността е оскъдна и автоматизацията чрез ИИ увеличава човешките възможности, като автоматизира обикновените повтарящи се задачи и освобождава време на експертите за по-стратегически и сложни операции по сигурността. Това дава възможност на анализаторите по сигурността ефективно да приоритизират ресурсите за справяне с критичните уязвимости на организацията и да разследват чувствителни към времето сигнали и открития в областта на сигурността.

Откриване на нови атаки/заплахи. Чрез възможности като откриване на аномалии и поведенчески анализ, техниките на изкуствения интелект имат потенциала да откриват нови и нововъзникващи заплахи. Чрез моделиране на нормалното поведение и разпознават отклоненията като потенциални нови атаки, тези техники на ИИ не е необходимо да дефинират заплаха или атака, за да ги откриват. Те могат да подпомогнат екипите по сигурността в проактивното идентифициране и смекчаване на нови заплахи и атаки.

Използването на изкуствения интелект като помощен метод за анализ и наблюдение дава възможност да се решават множество задачи на всички етапи при подготовката за отразяването на една кибератака, като ИИ е приложим и по време на локализирането, реакцията и премахването на последствията от инцидента. В резултат на гореописаните предимства при работа на изкуствения интелект в софтуерите за наблюдение на мрежи, става възможно значителното съкращаване на времето за откриване на заплаха за сигурността на мрежите и предотвратяване на атаки.

Заключение

• Изкуственият интелект играе ключова роля при в киберсигурността, но освен за защита на мрежите много често се използва и като спо-

соб за създаване на модели за атаки.

• Организациите ще създават все повече софтуерни продукти с интегриран изкуствен интелект, но успоредно с това киберпрестъпниците ще правят все повече опити да сриват киберзащитите на компаниите с цел да извлекат чувствителна информация.

• Киберсигурността е изправена пред постоянен поток от променящи се заплахи, които изискват иновативни решения, за да изпреварят нападателите. Изкуственият интелект е мощен инструмент, способен да направи революция в областта на киберсигурността.

• Развитието на изкуствения интелект в киберсигурността носи не само ползи при защитата на системите, а създава и нови опасности, на които трябва да се обърне сериозно внимание с цел недопускане изтичане на критична информация.

БЕЛЕЖКИ

1. NICASTRO, D., 2020. 7 Ways Artificial Intelligence is Reinventing Human Resources. *CMSWire* [online]. Available from: https://www.cmswire.com/digital-workplace/7-ways-artificial-intelligence-is-reinventing-human-resources

2. RUSSELL, Stuart; NORVIG, Peter, 2021. *Artificial general intelligence*. Pearson, 2021

3. NICASTRO, D., 2020. 7 Ways Artificial Intelligence is Reinventing Human Resources. *CMSWire* [online]. Available from: https://www.cmswire.com/digital-workplace/7-ways-artificial-intelligence-is-reinventing-human-resources

4. EC, 2026. European approach to artificial intelligence. *European Comission* [online]. Available from: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

5. RUSSELL, Stuart; NORVIG, Peter, 2021. *Artificial intelligence*. Pearson, 2021

ЛИТЕРАТУРА

КОТЕНКО, И.В., 2023. Ключевые области внимания на стыке искусственного интеллекта (ИИ) и кибербезопасности. *РусКрипто* [online]. Available from: https://ruscrypto.ru/resource/archive/rc2023/files/15_kotenko.pdf?ysclid=mgc0z8e8c4522833057

HAIDER, N.; BAIG, M.Z.; IMRAN, M., 2020. Artificial Intelligence and Machine Learning [Preprint]. *Arxiv* [online]. Available from: https://doi.org/10.48550/arXiv.2007.04490

LI, J.H. 2018. Cyber security meets artificial intelligence: A survey. *Front Inf Technol Electron Eng*, vol. 19, no 12, pp. 1462–74.

LOIKO, A.I., 2020. Interdisciplinary structury analysis systems in the. *Системный анализ и прикладная информатика,* с. 40 – 44.

PATEL, H., 2023. The Future of Cybersecurity with Artificial Intelligence (AI) and Machine Learning. *Preprints* [online]. Available from: https://www.preprints.org/manuscript/202301.0115

REFERENCES

HAIDER, N.; BAIG, M.Z.; IMRAN, M., 2020. Artificial Intelligence and Machine Learning [Preprint]. *Arxiv* [online]. Available from: https://doi.org/10.48550/arXiv.2007.04490

KOTENKO, I.V., 2023. Kljuchevye oblasti vnimanija na styke iskusstvennogo intellekta (II) i kiberbezopasnosti. *RusKripto* [online]. Available from: https://ruscrypto.ru/resource/archive/rc2023/files/15_kotenko.pdf?ysclid=mgc0z8e8c4522833057 [in Russian].

LI, J.H. 2018. Cyber security meets artificial intelligence: A survey. *Front Inf Technol Electron Eng*, vol. 19, no 12, pp. 1462–74.

LOIKO, A.I., 2020. Interdisciplinary structury analysis systems in the. *Системный анализ и прикладная информатика,* с. 40 – 44.

PATEL, H., 2023. The Future of Cybersecurity with Artificial Intelligence (AI) and Machine Learning. *Preprints* [online]. Available from: https://www.preprints.org/manuscript/202301.0115

INTERACTION BETWEEN CYBERSECURITY AND MODERN TRENDS IN THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE

Abstract. The publication focuses on contemporary trends in the development of artificial intelligence, specific applications and forms of AI-derived malware, and the vulnerability of information systems to new types of cyberattacks.

Keywords: agent-based AI; artificial intelligence; generative models; large language models; neuromorphic computing

Dimitar Malkochev
ORCID iD: 0009-0008-2733-0284
Rakovski National Defence College
82, Evlogi and Hristo Georgievi Blvd.
1504 Sofia, Bulgaria
E-mail: d.malkochev@rndc.bg

https://doi.org/10. 66334/annu26_threedimprint

THREE-DIMENSIONALLY PRINTED FIREARMS AS AN EMERGING SECURITY CHALLENGE: ACCESSIBILITY, DETECTION AND INVESTIGATIVE RESPONSES WITH IMPLICATIONS FOR BULGARIA AND SOUTH-EASTERN EUROPE

Dimitar Rangelov[1], Chavdar Georgiev[2,3,4]
[1]Saxion University of Applied Sciences (The Netherlands)
[2]Southeast European Law Enforcement Center (SELEC)
[3]Ministry of Interior of the Republic of Bulgaria (Bulgaria)
[4]Academy of the Ministry of Interior (Bulgaria)

Abstract. Firearms made with consumer three-dimensional printers have become a recurring finding in European criminal investigations. This paper combines a structured review of peer-reviewed studies, law enforcement and policy documents with an exploratory open-source snapshot of a public video-sharing platform to assess how accessible these weapons are, what threat they pose and how they can be detected. Low-cost printers, openly shared designs and online communities have lowered the barrier to entry, and hybrid designs combining printed frames with metal parts dominate both seizures and online content. Detection requires a layered approach spanning online monitoring, supply chain and financial controls, physical screening and specialised forensic

examination. For Bulgaria and South-Eastern Europe, where no large-scale production has been publicly documented, the paper recommends preparatory action: legal readiness for the proposed European Union rules on digital blueprints, dedicated data collection, first-responder training and targeted forensic capacity.

Keywords: forensic science; ghost guns; illicit firearms; security screening; South-Eastern Europe; three-dimensional printing

I. Introduction

Additive manufacturing, commonly called three-dimensional (3D) printing, builds objects layer by layer from a digital model. Its spread into homes and small workshops has created a security problem that traditional firearms control was not designed for: a person can now produce essential firearm components without a licensed manufacturer, without serial numbers and with limited contact with the physical supply chain. Such weapons are often called “ghost guns” because they escape the registration and tracing systems on which firearms investigations rely.

Since the publication of the first almost fully printed single-shot pistol in 2013, the phenomenon has evolved from symbolic, unreliable designs into semi-automatic hybrid weapons that have been seized in several European Union (EU) Member States (Schaufelbühl, Florquin, Werner, Delémont 2024). In February 2026 the European Commission proposed a directive that, for the first time at EU level, would criminalise the illicit creation, possession and dissemination of digital firearm blueprints.[59] The topic is therefore moving quickly from expert circles into national legislation and practice.

This paper addresses three questions: (1) how accessible 3D-printed firearms are and what threat they currently pose in Europe; (2) which methods exist to detect and investigate them; and (3) what these findings imply for Bulgaria and South-Eastern Europe. The paper deliberately stays at the level of threat assessment and countermeasures and does not reproduce any technical manufacturing information.

II. Methodology

The study is a structured narrative review. Sources were selected in three groups: peer-reviewed forensic and computer science literature indexed in ScienceDirect, Wiley and MDPI (2023 to 2026); reports of international

organisations and research bodies, including the United Nations Development Programme South Eastern and Eastern Europe Clearinghouse for the Control of Small Arms and Light Weapons (SEESAC), the Global Initiative Against Transnational Organized Crime (GI-TOC)[60] and the EU Global Threats programme; and legal and policy documents of the EU and the Republic of Bulgaria. In addition, an exploratory open-source intelligence (OSINT) snapshot was carried out on 17 September 2026 on a publicly accessible video-sharing platform. Eighteen English search terms were submitted to the platform's public search function and only the titles of the returned items were analysed; no files were downloaded and no instructional content was opened. The platform is deliberately not named, and no channel names or links are reported, in order to avoid amplifying the content. Documented cases were extracted into a comparative overview (Table 1), and detection and investigation methods were synthesised into a layered framework (Figure 3). The main limitation is that official statistics on 3D-printed firearms are rarely published separately, so the case evidence relies partly on media and open-source monitoring and should be read as indicative rather than complete.

III. Accessibility and the threat landscape

3.1. Categories of printed firearms

The forensic literature distinguishes three categories (Schaufelbühl, Szwed, Gallusser, Delémont, Werner 2023). Fully 3D-printed firearms consist almost entirely of polymer and are generally low-powered and unreliable. Hybrid firearms combine printed structural parts with metal components that can be sourced or produced without a licence. Parts kit completions or conversions use a printed frame or receiver together with commercially available parts of a conventional firearm. Printed accessories, most importantly devices that convert semi-automatic weapons to automatic fire, form a fourth, particularly dangerous group.

3.2. Why accessibility has increased

Four factors explain the growth. First, equipment is cheap: in 186 documented cases from 2014 to 2023, the most frequently seized printer was an entry-level model costing under 600 euros, and only standard polylactic acid filament appeared in the documented cases (Schaufelbühl, Florquin, Werner, Delémont 2024). Second, designs are openly available: a survey of the clear web recorded more than 2,100 firearm blueprint entries published between 2021

and April 2023, distributed through seven main websites and 45 distribution pathways, with more than 750 unique designs in the parts kit category alone (Schaufelbühl, Szwed, Gallusser, Delémont, Werner 2023). Third, knowledge transfer happens in online communities and encrypted messaging channels, where experienced designers support newcomers. The same study found that a small core of designers dominates this activity, which is relevant for targeted intervention. Fourth, production requires fewer physical interactions than buying a weapon on the black market, which appeals to actors who value anonymity, although it leaves a larger digital footprint (Meij 2024).

Accessibility should not be overstated. Building a functioning weapon still requires skill, time and patience, and Dutch police test-firing showed that reliability depends heavily on print and assembly quality (Meij 2024). However, each design generation lowers this barrier further.

3.3. Documented cases in Europe and the region

Reported cases were rare until 2020 and then increased sharply, with North America (110 cases) and Europe (45 cases) accounting for most of the global total (Schaufelbühl, Florquin, Werner, Delémont 2024). Seizures made up 88% of the documented cases, while discharges and sales were reported far less often. Table 1 summarises selected European and regional investigations that illustrate the range of actors, from individual workshops to networks linked to organised crime and violent extremism.

Table 1. Selected investigations involving 3D-printed firearms in Europe and South-Eastern Europe

Year	***Country***	***Case description***	***Source***
2020	Romania	Six house searches; 15 printers and hundreds of printed and conventional firearm parts seized	van der Meij 2024
2020	Spain	First illegal printing workshop detected in the country; 19 printed pistol frames seized	van der Meij 2024
2021	Finland	Printing facility with test range uncovered after an encrypted-communications operation; 10 printers seized	van der Meij 2024
2022	Sweden	Customs intercepted imported metal barrels; suspect had bought 38 printed pistol frames	van der Meij 2024
2022	Slovakia	Member of an online terrorist network sentenced after sharing a guide for a printed automatic-fire component	Stojanovski & Srbinovski 2026

Year	*Country*	*Case description*	*Source*
2022 onwards	Türkiye	Printed semi-automatic weapons offered on the Istanbul black market for about 470 to 530 euros	GI-TOC 2025
2024	France, Belgium	Coordinated action supported by Europol; 11 arrests; active printing workshop found	van der Meij 2024
2024	France	Network in Marseille dismantled; 14 suspects, 8 printers; sales paid in cryptocurrency	van der Meij 2024
2024	Greece	Group on Samos producing and selling printed semi-automatic weapons via encrypted platforms	GI-TOC 2025

For South-Eastern Europe the picture is mixed. SEESAC reported no seizures in the Western Balkans at the time of its study (Meij 2024), and GI-TOC found no public evidence of production or widespread use in Bulgaria, while noting journalistic indications of manufacturing and black-market sales elsewhere in the Balkans (GI-TOC 2025). The absence of evidence should be interpreted with caution: national statistics often group printed weapons with other homemade firearms, which masks trends (Stojanovski, Srbinovski 2026). The region also combines established trafficking routes, a legacy of conflict-era weapons and the prospect of large weapon flows after the war in Ukraine, which together form a favourable environment for new forms of illicit supply.

3.4. Open-source snapshot of available designs

The OSINT snapshot confirms that content on printed firearms is easy to find through ordinary social media search. The 18 queries returned 2,544 unique items. After removing unrelated results, such as video game content, 526 titles referred explicitly to printed or homemade firearms, published by 217 different channels. Titles were grouped into design families using keyword rules (Table 2).

Table 2. Design families identified in the open-source snapshot

Design family or item type	*Titles*	*Channels*
FGC-9 family (incl. MkII, Mini)	162	71
Liberator	3	3
Harlot .22 LR	10	9
Glock-pattern frames	128	51
AR-15 lower receivers	50	20

Design family or item type	*Titles*	*Channels*
Auto sears/conversion devices	7	6
Suppressors	10	9
Shotguns	3	3
Magazines	38	19
Other .22 LR designs	14	9
Barrels (incl. ECM rifling)	5	3
Printed ammunition	3	2
Urutau	4	3
Plastikov	3	3

Three observations stand out. First, the semi-automatic hybrid carbine that dominates European seizures is also the most visible design online (162 titles from 71 channels), which suggests that online visibility is a reasonable indicator of operational relevance. Second, printed frames for a widely sold pistol pattern and printed lower receivers for a common rifle pattern form the next largest groups, matching the parts kit completions described in the forensic literature. Third, a smaller but significant share of titles concerns high-risk items, namely devices for automatic fire, suppressors, barrel production and printed ammunition. The counts are indicative only: keyword matching can include unrelated or duplicate items and miss titles in other languages, and the results were not verified by viewing the content.

Figure 1 illustrates the range of these weapons with openly licensed photographs: an early fully printed single-shot pistol, the hybrid carbine that dominates current seizures, a printed revolver-type weapon intercepted during airport screening, an industrially produced metal-printed pistol, the hybrid carbine in use by an armed group in the Myanmar conflict, and a privately made pistol secured as evidence by police. The fifth example shows that these designs have already reached conflict zones, which is directly relevant for defence and security planning.

Figure 2 shows typical examples found during the open-source snapshot. The images are of high visual quality and present the weapons in the style of commercial product photography, which illustrates how normalised and accessible this content has become. Identifying marks were blurred and no sources are given, in line with the approach described in Section II.



Figure 1. Examples of printed and privately made firearms: (a) fully printed single-shot pistol; (b) hybrid carbine seized by a sheriff's office in the United States; (c) printed revolver-type weapon found in carry-on baggage; (d) metal-printed pistol; (e) hybrid carbine used in the Myanmar conflict; (f) privately made pistol in a police evidence box

Image credits: (a) Vvzvlad, CC BY-SA 3.0; (b) Fresno County Sheriff's Office, public domain; (c) U.S. Transportation Security Administration, public domain; (d) Solid Concepts Inc., CC BY-SA 4.0; (e) Myanmar Now, CC BY 3.0; (f) Los Angeles Police Department, public domain. All via Wikimedia Commons, accessed 17 September 2026.



Figure 2. Examples of printed firearms observed in the open-source snapshot: (a) fully printed single-shot pistol; (b) small-calibre printed pistols; (c) printed frame for a common pistol pattern; (d, e) printed rifle-pattern pistols; (f) rifle with printed lower receiver and stock; (g) rendering of a hybrid carbine; (h) hybrid carbines

IV. Detection and investigation

Because printed firearms can be interdicted before, during and after production, detection is best organised as a sequence of complementary layers (Figure 3). No single layer is sufficient, but each one can generate leads for the others.

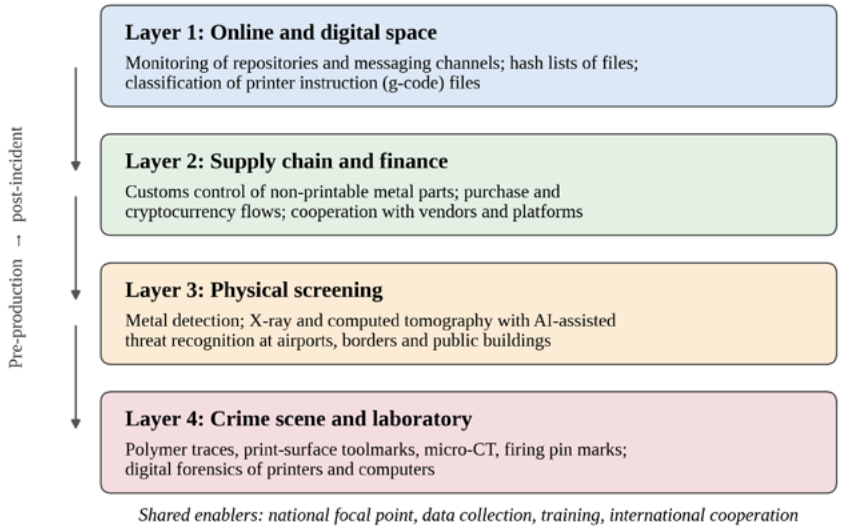


Figure 3. Layered framework for detecting and investigating 3D-printed firearms (authors' synthesis)

4.1. Online and digital space

The digital component is the most distinctive feature of this threat. Monitoring of design repositories and messaging channels supports early warning, and hash databases of known design files, such as the one developed in the United Kingdom, allow known files to be recognised on seized devices and online (Meij 2024). Research is also moving towards the files that printers actually execute: a recent proof of concept classified firearm and non-firearm objects from the geometric information in g-code files using machine learning (Garland, Mfodwo, Neyaz, Varol 2026). Such tools could support the triage of large volumes of seized data.

4.2. Supply chain and financial controls

Most seized weapons are hybrids, so their producers still depend on metal components. The Swedish case in Table 1 began when customs officers noticed barrels declared as industrial valve parts. Purchases of printers, filament, parts kits and design files, often paid in cryptocurrency, create financial traces. Involving financial investigators from the early stage of an investigation and during house searches is therefore recommended (Meij 2024).

4.3. Physical screening

Conventional metal detectors are effective against hybrids that contain metal barrels or springs, but they are less reliable against designs with minimal metal content. Journalists demonstrated this weakness in 2013 by carrying a printed pistol into the Israeli parliament, and airport X-ray screening in the United States has intercepted printed firearms in carry-on baggage.[61] Computed tomography combined with automated threat recognition is the most promising route, but progress is limited by a lack of training data for rare objects such as firearm components and by the absence of independent performance standards.[62] Synthetic data offers a partial solution: a detector trained only on 75,000 images generated from design models reached about 83% mean average precision on real printed components (Benjumea-Bellott, Torregrosa-Domínguez, Ramos-González, Soria-Morillo, Álvarez-García 2026).

4.4. Crime scene and laboratory examination

Printed firearms usually carry no serial number and may lack rifling, so classic tracing and ballistic comparison are less effective. They do, however, leave other traces. Polymer fragments were recovered around all six fully printed firearms in a controlled firing study (Szwed, Schaufelbühl, Gallusser, Werner, Delémont 2023), and chemical analysis of printing polymers can associate traces with reference material at source level (Falardeau, Mireault, Daoust, Muehlethaler 2024). Surface marks produced by the printer nozzle and the print bed may link a part to a specific printer (Pavlovich, Garrison 2023), and improvised firing pins leave impressions that can indicate a printed weapon (Meij 2024). Micro-computed tomography allows non-destructive examination of internal mechanisms before test firing and creates a permanent digital record for court (Goia, Cooper, Norman, Primeau, Hall, Hawley, Williams 2024). Finally, printers and computers can store print histories and design files, so a printer should not be switched off during a search while it is printing (Meij 2024).

V. Legal and regulatory framework

Across the EU, the manufacture and possession of unlicensed firearms, including printed ones, are already prohibited under Directive (EU) 2021/555, but the directive does not cover digital blueprints (Meij 2024). North Macedonia was the first European country to criminalise the possession and distribution of such blueprints (Meij 2024). The Commission proposal COM(2026) 102 would close this gap across the Union by setting a maximum penalty of at least two years

for the illicit creation, acquisition, possession and dissemination of blueprints. It would also require every Member State to establish a National Firearms Focal Point and to collect standardised data on seizures (European Commission 2026).

In Bulgaria, the Law on Weapons, Ammunition, Explosives and Pyrotechnic Articles regulates the manufacture and possession of firearms, and Article 339 of the Criminal Code punishes the unauthorised acquisition, possession or transfer of firearms with two to eight years of imprisonment. These provisions apply to a printed weapon once it exists, but they do not explicitly address digital design files or the preparatory digital stage. Once adopted, the EU directive will therefore require targeted amendments.

VI. Research results and implications for Bulgaria

The review leads to four findings. First, the barrier to entry is low and falling, and hybrid designs are the main operational threat. Second, the threat has a large digital and financial footprint that creates intervention points before any weapon exists. Third, detection works only as a layered system, with computed tomography and data-driven recognition as the key screening gap. Fourth, forensic science can recover new types of evidence, but most methods are still at the research stage. Table 3 translates these findings into preparatory measures for Bulgaria.

Table 3. Recommended preparatory measures for Bulgaria

Area	*Recommended measure*
Legislation	Prepare transposition of the proposed directive, including offences related to digital blueprints
Data	Record 3D-printed items as a separate category in seizure statistics and share data with Europol
Training	Include recognition of printed weapons, printers and waste material in first-responder and crime scene curricula
Forensics	Build capacity in polymer analysis, printer toolmarks, micro-computed tomography and printer digital forensics
Screening	Pilot computed tomography with automated threat recognition at airports, borders and courts
Cooperation	Participate in European and regional expert networks and link with universities and industry

For a defence and security education system, the topic also has a training dimension: officers, investigators and screening personnel need a shared basic understanding of the technology so that early indicators are not missed.

VII. Conclusion

3D-printed firearms are no longer a hypothetical risk in Europe. They are cheap to produce, supported by open design communities and increasingly reliable. At the same time, their digital, financial and material traces offer real opportunities for detection. Bulgaria and South-Eastern Europe have not yet seen large-scale production in public reporting, which gives the region time to prepare rather than react. Legal readiness for the new EU rules, dedicated data collection, training and focused forensic and screening capacity are the most effective steps. Future research should build shared reference datasets for screening systems and validate forensic methods for use in court.

Acknowledgements. Special gratitude is extended to the University of Twente, the Technologies for Criminal Investigations (TCI) research group, part of Saxion University of Applied Sciences and the Police Academy in the Netherlands, the Technical University of Sofia and the AI & CAD Systems Lab at Sofia Tech Park. Additionally, the work is supported by project No. BG16RFPR002-1.014-0014-C01, “Development Program with a Business Plan for the Laboratory Complex of Sofia Tech Park”, implemented under the Research, Innovation and Digitalization for Smart Transformation Program, co-financed by the European Union through the European Regional Development Fund and part of the project “Regiodeal Stedendriehoek” funded by the Dutch National Government.

REFERENCES

BENJUMEA-BELLOTT, C.; TORREGROSA-DOMÍNGUEZ, Á.; RAMOS-GONZÁLEZ, V.; SORIA-MORILLO, L.M.; ÁLVAREZ-GARCÍA, J.A., 2026. LEOPARD: Automated CAD-to-Synthetic Pipeline for 3D-Printed Firearm Detection in Civil Transit Security. *Applied Sciences*, vol. 16, no 10, 5104. Available from: https://doi.org/10.3390/app16105104.

FALARDEAU, M.; MIREAULT, C.; DAOUST, B.; MUEHLETHALER, C., 2024. Chemical analysis of polymers used for 3D printing of firearms. *Forensic Science International*, vol. 357, 111999. Available from: https://doi.org/10.1016/j.forsciint.2024.111999.

GARLAND, L.; MFODWO, E.; NEYAZ, A.; VAROL, C., 2026. 3D printed firearm identification: A comparison of machine learning models. *Journal of Forensic Sciences*, vol. 71, no 4, pp. 1621-1638. Available from: https://doi.org/10.1111/1556-4029.70355

GOIA, S.; COOPER, G.; NORMAN, D.G.; PRIMEAU, C.; HALL, M.; HAWLEY, J.; WILLIAMS, M.A., 2024. The use of micro-CT in the investigation of a case involving 3D printed firearms. Forensic *Science International*, vol. 363, 112157. Available from: https://doi.org/10.1016/j.forsciint.2024.112157.

MEIJ, M., 2024. *3D-Printed Firearms: State of Play, Challenges and Law Enforcement Approach*. Belgrade: UNDP SEESAC.

PAVLOVICH, S.; GARRISON, K., 2023. An exploratory study of topographical signatures within 3D fused deposition modelling using Polylactic Acid (PLA) filament. *Forensic Science International*, vol. 349, 111740. Available from: https://doi.org/10.1016/j.forsciint.2023.111740.

SCHAUFELBÜHL, S.; FLORQUIN, N.; WERNER, D.; DELÉMONT, O., 2024. The emergence of 3D-printed firearms: An analysis of media and law enforcement reports. *Forensic Science International: Synergy*, vol. 8, 100464. Available from: https://doi.org/10.1016/j.fsisyn.2024.100464.

SCHAUFELBÜHL, S.; SZWED, A.; GALLUSSER, A.; DELÉMONT, O.; WERNER, D., 2023. Investigating the availability of 3D-printed firearm designs on the clear web. *Forensic Science International: Synergy*, vol. 7, 100444. Available from: https://doi.org/10.1016/j.fsisyn.2023.100444.

STOJANOVSKI, T.; SRBINOVSKI, A., 2026. *Stemming the Tide: Arms Trafficking Dynamics in Central and South-Eastern Europe*. Geneva: Global Initiative Against Transnational Organized Crime.

SZWED, A.; SCHAUFELBÜHL, S.; GALLUSSER, A.; WERNER, D.; DELÉMONT, O., 2023. Was a 3D-printed firearm discharged? Study of traces produced by the use of six fully 3D-printed firearms. *Forensic Science International*, vol. 348, 111736. Available from: https://doi.org/10.1016/j.forsciint.2023.111736.

Dimitar Rangelov, Senior Researcher
ORCID iD: 0009-0005-8511-1555
Research Group Technology for Criminal Investigation
Saxion University of Applied Sciences
M.H. Tromplaan 28, 7513 AB
Enschede, The Netherlands
E-mail: d.g.rangelov@saxion.nl

Chavdar Georgiev, PhD Student
ORCID iD: 0009-0004-6950-3447
Director of Operations, Southeast European Law Enforcement Center (SELEC)
Deputy Director of the "Inspectorate" Directorate
Ministry of Interior of the Republic of Bulgaria
Department of Operational-Investigative Activity
Academy of the Ministry of Interior
1, Alexander Malinov Blvd.
Sofia, Bulgaria
E-mail: ChGGeorgiev@mvr.bg

https://doi.org/10. 66334/annu26_nanadaleopstrat

НАНАСЯНЕТО НА ДАЛЕКОБОЙНИ УДАРИ КАТО СРЕДСТВО ЗА ПОСТИГАНЕ НА ДЪЛГОСРОЧНИ ОПЕРАТИВНО-СТРАТЕГИЧЕСКИ ЦЕЛИ ВЪВ ВОЙНАТА В УКРАЙНА

старши лейтенант Димо Савов[1], Пламен Дяков[2]
[1]Военноморски сили на Република България
[2]Военна академия „Георги Стойков Раковски“

Абстракт. Докладът разглежда ключови аспекти от нанасянето на далекобойни удари като един от инструментите за реализиране на оперативно-стратегически цели с дългосрочни последици във войната в Украйна (2022-), извеждайки основни тенденции в използването на различни видове средства и тяхното влияние върху динамиката и развитието на конфликта. За постигането на гореспоменатата цел по балансиран и аргументиран начин ще бъде представен анализ, основаващ се на документалния метод и изготвен на базата на различни общодостъпни източници като научни статии и доклади, журналистически материали и експертни оценки, касаещи далекобойните удари, нанасяни и от двете противостоящи страни.

Ключови думи: Русия; Украйна; далекобойни удари; оперативно-стратегически цели с дългосрочни последици

Увод

Настоящият анализ се основава предимно на документалния метод, чрез който се събират, съпоставят и критично се оценяват данни от широк кръг открити източници, включително академични публикации, експертни анализи, специализирани изследвания и журналистически материали. При анализа на въоръжен конфликт от подобен характер установяването на пълна и надеждна картина на отделните удари е затруднено от ограничения достъп до информация, различията в оценките за нанесените поражения и наличието на твърдения, чиято достоверност не винаги може да бъде независимо проверена.

Поради значителния брой извършени далекобойни удари и широкия спектър от използвани средства тяхното изчерпателно проследяване би надхвърлило техническия обем и аналитичните цели на настоящата статия. Поради това не се поставя задача да бъдат разгледани всички регистрирани случаи, а да бъдат подбрани показателни примери, чрез които да се проследят основните тенденции в развитието и използването на далекобойните способности в периода 2022 – 2026 г. Подбраните случаи и изведените тенденции позволяват да бъдат разгледани различни способи за въздействие в отделните домейни на театъра на бойните действия, типовете цели и механизмите за постигане на непосредствени и потенциални дългосрочни оперативно-стратегически ефекти. По този начин фокусът се поставя не върху количественото обхващане на всички извършени атаки, а върху развитието на способностите и последиците от системните удари на оперативно-стратегическо ниво.

Далекобойни удари на въоръжените сили на Руската Федерация във войната в Украйна

Способностите на Съветския съюз за нанасяне на далекобойни удари са неизменна част от военната му доктрина още от възникването на първите средства за огнево въздействие с голяма далекобойност през 1930-те години, а именно бомбардировъчната авиация с далечно действие. С развитието на военните технологии, военната доктрина и възможностите на военнопромишления комплекс на страната, се увеличават различните типове средства и производствените им количества, подобряват се тактико-техническите им характеристики; въвежда се на въоръжение и се развива ядреното оръжие. В контекста на геополитическата обстановка и характера на съвременната въоръжена борба след 1991 г., Русия, като на-

следник на Съветския съюз, усилено продължава създаването и развитието на далекобойни средства за огнево поразяване за постигането на цели от оперативно и стратегическо значение. Бойното използване на съвременните образци далекобойно ракетно въоръжение на Русия става факт за първи път в периода 2015 – 2017 г., в контекста на войната в Сирия (Johnson 2015). Постигната е относително висока точност на дистанции от 1500 – 2000 км и е успешно демонстрирана възможността за водене на огън от различни типове бойни платформи – надводни кораби, подводници, стратегически бомбардировачи-ракетоносци. Въпреки това, в този период бойното използване на далекобойно оръжие от Русия по мащаби и по постигнати цели има ограничен характер.

Още с първите минути на войната, започнала на 24 февруари 2022 г., започват масираните далекобойни ракетни удари на Москва срещу цели в Украйна. Към този момент това са военни летища и кораби във военноморските бази, командни пунктове на въоръжени сили (ВС) на Украйна, постове за радиотехническо наблюдение, големи военни складове и нефтобази (Beaumont & Jones 2022). Основните цели на ръководството на ВС на Русия са: по този начин да бъдат постигнати господство във въздуха и господство в морските пространства; да бъде сериозно затруднена логистиката и процеса по командване и управление на украинските ВС, което на свой ред да спомогне за по-бързото и ефективно настъпление на сухопътните фронтове. Не малка част от ударите са успешни и поразяват своите цели, но украинското военно командване бързо предприема мерки, които да ограничат загубите в материална част и жива сила – основно чрез принципите на разсъредоточаване и маскировка; чрез често и навременно предислоциране[1] и строг контрол на емисиите на радиолокационните станции (Chiusa 2026). Многостранната подкрепа на трети страни, предимно финансова и материална, увеличава драстично отбранителния потенциал на Киев. Вследствие на тези фактори Русия постига временно въздушно превъзходство в определени участъци от въздушното пространство на Украйна, но не успява да достигне до пълно въздушно превъзходство или господство във въздуха (Bronk 2026).

Поради силно ограничения корабен състав на Военноморски сили (ВМС) на Украйна и успешността на далекобойните удари срещу тях още в първите дни на войната, Русия успява да постигне и временно да поддържа пълно господство на море, блокирайки стратегически важния за икономиката на Украйна „зърнен коридор“. Това състояние на надмощие продължава до потапянето на крайцера „Москва“ на 14 април 2022 г. от

страна на украински противокорабни ракети с брегово базиране. Впоследствие масираното използване от украинска страна на безпилотни надводни апарати (USV) за поразяване на руски кораби дава също значителни резултати. Поради многото бойни загуби на кораби на море и в базови условия, през есента на 2023 г. руското командване започна пребазиране на корабите, базирани в Севастопол, в Новоросийск. И в този пункт за постоянна дислокация обаче корабите на руския Черноморския флот са няколкократно атакувани от украински USV. Следователно украинските действия за възпрепятстване на действията на противника в морското пространство – Anti-access/area denial (Lancaster 2022), прерастват в усилия за постигането на превъзходство в морските пространства в определени зони на Черно море, възстановявайки корабоплаването през зърнения морския коридор[2]. Въпреки това, операциите на Руския черноморски флот за нанасяне на далекобойни удари от море не са прекратени.

Промените в стратегическата обстановка в морския и във въздушния домейн след успешните украински контраофанзивни действия влияят и на ситуация на сухопътния фронт. Още към края на пролетта на 2023 г. войната в Украйна окончателно се превръща във „война на изтощение“, при която и двете страни се стремят да изтощят другата чрез системно и целенасочено унищожаване на ресурсите на противника – военни, икономически, инфраструктурни и психологически. В тези условия далекобойните удари на Русия не само продължават, но и увеличават драстично своята интензивност и мащаби (Olmsted et al. 2026a). Стремежът на Руското военно командване към прекъсване на връзките между производството и потреблението на електроенергия и унищожаване на енергетиката чрез системни и целенасочени удари по ТЕЦ, ВЕЦ, възли на електропреносната мрежа и нейните подстанции дават резултати, които обаче към момента на писане на научния текст трудно могат да бъдат категорично и обективно оценени[3]. Сред целите на далекобойните удари на Руските ВС е и системата на логистиката – както цивилната, така и военната[4]. Примери за това са систематичните удари срещу телекомуникационната и интернет инфраструктура (Hodunova 2026) и съответно обекти на военнопромишления комплекс[5]. С масовото използване на безпилотни летателни апарати (БЛА) във въздушните удари нарастват количествените параметри на използваните в ударите средства (Atalan 2026) и респективно броят на използваните видове средства за огнево въздействие на далечни разстояние. Таблиците, по-долу, целят представянето на именно тези видове средства по достъпен и целесъобразен за научния труд начин.

Други цели, по които руските ВС водят системен и целенасочен огън от далечни разстояния, са търговски кораби в украински териториални води или извън тях, но плаващи към украински пристанища[6]. По този начин Русия оказва сериозен натиск върху икономиката на страната (Harding & Roth 2026), пряко зависима от износа на зърно (60 % от общия износ на страната), военните доставки и чуждестранните инвестиции.

Таблица 1. Средства за далекобойно огнево въздействие с наземно базиране, използвани от Русия във войната в Украйна

Ракетна система	***Тип ракета***	***Платформа носител***	***Вероятна дистанция на стрелба***
3М22 „Циркон“	Крилата	Брегови ракетен комплекс „Бастион-П“ (модифициран)	600 – 1000 км
9К720 „Искандер-М“	Балистична	Самоходна пускова установка 9П78-1	200 – 500 км
9К720 „Искандер-К“ (9М728 / 9М729)	Крилата	Самоходна пускова установка 9П78-1	до 500 км
П-800 „Оникс“	Противокорабна (използвана за удари по наземни цели)	Брегови ракетен комплекс „Бастион-П“	300 – 450 км
С-300 / С-400	Зенитна (използвана за удари по наземни цели)	Мобилни пускови установки на ПВО	40 – 200 км
„Герань-2“ (Shahed-136)	Дрон-камикадзе	Мобилни наземни катапулти	1000 – 2000 км

Таблица 2. Средства за далекобойно огнево въздействие с морско и въздушно базиране, използвани от Русия във войната в Украйна

Ракетна система	***Тип ракета***	***Платформа носител***	***Вероятна дистанция на стрелба***
Х-101 / Х-555	Крилата	Далечни бомбардировачи Ту-95МС/МСМ и Ту-160М1/М2	1500 – 2500 км
„Калибър“ (3М14)	Крилата	Фрегати пр. 11356М, корвети пр. 21631 / 22800, подводници пр. 636.3	300 – 2000 км

3М22 „Цир-кон“	Крилата	Фрегати пр. 22350, подводници пр. 885М	600 – 1000 км
Х-47М2 „Кинжал“	Балистична	Изтребители МиГ-31К; Ту-22М3/М3М	400 – 1000+ км
Х-22 / Х-32	Крилата	Бомбардировачи Ту-22М3/М3М	200 – 1000 км
Х-59 / Х-69	Крилата	Изтребители Су-30СМ/СМ2, Су-34, Су-35	100 – 400 км
Х-31П / Х-58	Противора-дио-лока-ционна	Многоцелеви изтребители Су-34, Су-35, Су-30СМ/СМ2	50 – 150 км
„Гром-Е1“	Планираща бомба-ракета	Су-30СМ/СМ2, Су-34, Су-35	до 120 км

Далекобойни удари на Украйна срещу Руската Федерация

В украинския случай развитието на способностите за нанасяне на далекобойни удари се превърна в един от инструментите за въздействие върху оперативната и стратегическата дълбочина на руските въоръжени сили и икономиката на страната. Еволюцията на тези способности може да бъде проследена последователно от началния период на войната до формирането на комплексен арсенал от ракетни, безпилотни и други средства за поразяване на цели в дълбочина.

Развитието на украинските способности започва още през 2022 г. и преминава през няколко последователни етапа. В началния период Киев разполага с ограничени възможности, но още през април 2022 г. поразяването на руския ракетен крайцер „Москва“ с украински противокорабни ракети „Нептун“ демонстрира възможността за въздействие върху ключови военноморски активи извън непосредствената зона на бойни действия. През есента на същата година започва използването и на морски безпилотни надводни апарати, включително при атаки срещу цели от Черноморския флот в Севастопол. Както вече бе споменато, тези действия поставят началото на направление, което впоследствие се превръща в съществен компонент от украинската стратегия за ограничаване на руските военноморски способности в Черно море (Dougherty 2025, pp. 120, 122).

През 2023 г. качественото разширяване на украинските възможности в контекста на „войната на изтощение“ постигнато с въвеждането на въоръжение на крилатите ракети Storm Shadow/SCALP, които дават на украинските ВС способността да нанасят високоточни удари срещу командни пунктове, логистични обекти (включително складове за боеприпаси) и други цели от оперативно-стратегическо значение в дълбочина. Паралелно с това морските безпилотни системи започват да се използват в още по-голям мащаб, като създават заплаха не само за корабите на Черноморския флот, но и за руската крайморска инфраструктура и военноморски бази в по-отдалечени райони на Черно море. В края на 2023 и началото на 2024 г. развитието продължава с въвеждането на ATACMS и с бързото усъвършенстване на украинските собствени далекобойни безпилотни средства. Така постепенно се формира многокомпонентна система за удари в дълбочина, в която различни средства могат да бъдат използвани самостоятелно или в съчетание в зависимост от типа на целта, необходимата дистанция на стрелба, бойната ѝ устойчивост и търсения оперативен ефект (Dougherty 2025, pp. 84 – 85; Swanston & Swanston 2025, p. 218).

През 2025 – 2026 г. тази тенденция се развива към все по-системно въздействие върху цели в дълбокия тил на Руската федерация. Наред с високоточните ракети, далекобойните безпилотни летателни апарати и морските безпилотни системи, Украйна провежда и специални операции за поразяване на цели, при които конвенционалните средства за огнево поразяване трудно могат да бъдат използвани, или които изискват различен способ на бойно използване (операция „Паяжина“). По този начин еволюцията на украинските далекобойни способности може да бъде разглеждана не просто като увеличаване на обсега на отделните средства, а като постепенно изграждане на разнообразен арсенал за въздействие върху военните способности, логистиката, военнопромишлената и енергийната инфраструктура и морските комуникации на противника. В тази връзка настоящият анализ се концентрира върху четири показателни направления – използването на Storm Shadow/SCALP и ATACMS, ролята на морските безпилотни системи срещу Черноморския флот на Руската федерация, ударите по руската нефтена и енергийна инфраструктура, както и операция „Паяжина“. Изборът им позволява да бъдат проследени различни способи за постигане на оперативно-стратегически ефекти чрез въздействие в дълбочина на противника.

Качествен етап в развитието на украинските способности за нанасяне на далекобойни удари настъпва през 2023 г. с получаването на кри-

латите ракети Storm Shadow/SCALP, а впоследствие и на балистичните ракети ATACMS. Storm Shadow е интегрирана със съветските изтребители-бомбардировачи Su-24M, които са на въоръжение във ВВС на Украйна. Съчетаването на бойния радиус на самолета с обсега на ракетата създава възможност за нанасяне на високоточни удари на значителна дълбочина, позволявайки на носителя да извършва пускове извън непосредствената зона на действие на част от руските средства за противовъздушна охрана (ПВО). Така Украйна получава способност за въздействие върху командни пунктове, логистични обекти, авиационна и военноморска инфраструктура и други високостойностни цели в оперативна дълбочина (Dougherty 2025, pp. 101, 124).

Особено показателна е серията от удари срещу обекти на Черноморския флот в Крим. На 13 септември 2023 г. е нанесен ракетен удар по корабостроителницата „Севморзавод“ в Севастопол, където в ремонт се намират десантният кораб „Минск“ и подводницата „Ростов на Дон“. И двата кораба получават тежки повреди, като поражения са нанесени и на ремонтната инфраструктура. Само девет дни по-късно е поразен щабът на Черноморския флот в Севастопол. Ударът от 22 септември причинява значителни поражения на сградата на щаба, като руската страна потвърждава повреждането на обекта, а редица източници свързват атаката с използването на Storm Shadow. Така в кратък период са атакувани и поразени както материални средства и инфраструктурата за тяхното поддържане, така и ключов елемент от системата за командване и управление на флота (Evans et al. 2023a; Childs 2023).

Последователността продължава с удари по други високостойностни военноморски цели. През ноември 2023 г. е поразена корветата „Асколд“ в корабостроителния завод „Залив“ край Керч, а на 26 декември – десантният кораб „Новочеркаск“ във Феодосия. При „Новочеркаск“ са нанесени тежки поражения на кораба и пристанищната инфраструктура. За тези атаки се посочва използването на Storm Shadow/SCALP, макар конкретният тип ракета да не може във всички случаи да бъде независимо потвърдена. Впоследствие, както вече бе споменато, значителна част от основните средства на Черноморския флот е преместена от Севастопол към Новоросийск, което увеличава дистанцията между тях и украинските средства за поразяване (Evans et al, 2023b; Clark & Wolkow 2023).

Първото използване на ATACMS в бойни действия е регистрирано на 17 октомври 2023 г., когато са нанесени удари по руските военни летища край Бердянск и Луганск. При атаката са използвани ракети с касетъчна

бойна глава, предназначена за поразяване на незащитена или слабо защитена техника, включително авиационни средства. Украинската страна съобщава за унищожени девет вертолета, пускова установка на ПВО, специална техника и складове за боеприпаси. Последвалият анализ на сателитни изображения потвърждава значителни поражения по авиационната техника и летищната инфраструктура. В района на Бердянск са идентифицирани множество поражения на локациите, където преди удара са били дислоцирани вертолети, а в Луганск са установени следи от поражения по няколко вертолета. Общият брой на повредените или унищожени машини на двата обекта вероятно е по-голям от първоначално обявените девет. Значението на атаката се определя не само от непосредствените загуби на авиационна техника. Бердянск представлява важна база за руската армейска авиация, включително за бойните вертолети Ka-52, които са използвани активно срещу украинските сили в южното направление. Ударът демонстрира, че новото средство притежава висока бойна ефективност, позволявйки едновременно поразяване на множество цели, разположени на летищна площадка, чрез една огнева задача. Това създава качествено различна заплаха за авиационните бази и увеличава необходимостта от повишване на тяхната бойна устойчивост чрез разсредоточаване на техниката, промяна в организацията на базиране и повишаване на защитата на авиационните обекти. По този начин ATACMS допълва способностите на Storm Shadow/SCALP, като предоставя наземно базирана възможност за бързо поразяване на цели в оперативна дълбочина (Gwadera 2023).

Следващ етап в използването на ATACMS е атака срещу обект на територията на Руската федерация. В нощта на 18 срещу 19 ноември 2024 г. е нанесен удар по 67-и арсенал на Главното ракетно-артилерийско управление (ГРАУ) край Карачев, Брянска област. Украинското военно командване съобщава за първоначална детонация и последвали 12 вторични взрива, докато руското Министерство на отбраната заявява, че по обекта са били изстреляни шест балистични ракети, включително ATACMS, като пет са били прехванати, а една – повредена от средствата за ПВО. Съобщава се, че арсеналът е съхранявал артилерийски боеприпаси, ракети за реактивни системи за залпов огън, средства за ПВО и авиационни боеприпаси. Поради различията между руските и украинските оценки степента на физическото поражение на обекта не следва да бъде определяна категорично. Независимо от това, самото достигане до такъв обект показва разширяване на географската дълбочина, в която руската военна инфраструктура може да бъде поставена под заплаха от украинските високоточни средства (Kushnikov 2024).

Паралелно с развитието на ракетните средства за далекобойно въздействие Украйна постепенно изгражда способност за нанасяне на удари по Черноморския флот на Руската федерация чрез безпилотни надводни апарати. Хронологично това направление предхожда използването на западните далекобойни крилати ракети: първата мащабна атака с морски дронове срещу Севастопол е осъществена през октомври 2022 г., докато предоставянето на Storm Shadow е обявено през май 2023 г. Така морските безпилотни системи се превръщат в един от ранните инструменти за въздействие върху Черноморския флот, а впоследствие развитието им се допълва от високоточните ракетни средства. Еволюцията на тази способност може условно да бъде проследена през три етапа – от действията им в района на Севастопол през 2022 г., до разширяването на оперативния им обсег до Новоросийск през 2023 г. и систематичното поразяване на руски бойни кораби през 2024 г.

Първият етап е свързан с атаката срещу руски военноморски обекти в Севастопол през октомври 2022 г., при която са използвани USV в комбинация с безпилотни летателни апарати. Макар непосредствените резултати от операцията да остават предмет на различни оценки, тя демонстрира възможността сравнително малки безпилотни плавателни средства да проникват в защитена пристанищна среда и да създават заплаха за военни кораби в базови условия. Качествено разширяване на тази способност е демонстрирано на 4 август 2023 г., когато морски дрон поразява десантния кораб „Оленегорский горняк“ в района на Новоросийск. Корабът получава тежки повреди, а атаката показва, че пребазирането на руски кораби в друга военноморска база не елиминира заплахата от украински атаки. Значението на случая се определя и от географското разширяване на застрашената зона: Новоросийск се намира значително по-далеч от украинското крайбрежие и е разглеждан като по-сигурна база за руските Военноморски сили. Така способността на USV да достигат отдалечени цели започва да влияе не само върху отделни кораби на море, но и върху решенията за тяхното базиране и защита. През началото на 2024 г. морските дронове вече демонстрират способност за систематично поразяване на бойни кораби. На 31 януари/1 февруари е потопена ракетната корвета „Ивановец“, а на 5 март е атакуван патрулният кораб „Сергей Котов“ край Керченския проток (Kaushal 2023; Pili 2024; Sutton 2024).

Развитието на морските безпилотни системи не протича изолирано от останалите украински средства за далекобойно въздействие. След като USV вече са създали непосредствена заплаха за корабите, въвеждането на

Storm Shadow/SCALP през 2023 г. добавя още една възможност за високоточни удари по свързани с флота обекти и инфраструктура в Крим. Така ракетите и морските дронове въздействат върху различни елементи на една и съща система: ракетите поразяват защитени обекти и инфраструктура в дълбочина, докато USV създават заплаха за самите плавателни средства и ограничават възможностите за тяхното базиране и маневриране. В съчетание с бреговите противокорабни средства това формира ешелонизация на отбраната, осигуряваща Anti-access/Area denial, при което целта е ограничаване на способността на противника да използва безпрепятствено определено морско пространство, оказващо критично влияние върху оперативната свобода на руските ВМС (Delanoe 2024; Kaushal 2024).

Развитието на тази способност продължава и след разглеждания период. През 2025 г. украински морски дронове са използвани отново срещу руски плавателни съдове, включително срещу танкери, свързвани от украинска страна със санкционния „сенчест флот“ на Кремъл, а през 2026 г. продължават съобщенията за атаки срещу руските Военноморски сили и инфраструктура в Черно море. Тези по-късни действия не променят избрания за настоящия анализ времеви фокус, а напротив – показват устойчивото развитие и запазването на морските безпилотни системи като инструмент за постигане на A2/AD, унищожавайки руското господство/превъзходство на море и осигурявайки превъзходство в определени морски зони, макар и посредством асиметрични способи.

С развитието на собствените далекобойни ударни безпилотни летателни апарати Украйна постепенно разширява възможностите си за въздействие върху обекти, разположени на значителна дълбочина на територията на Руската федерация. Особено място заемат нефтопреработващата, горивно-логистичната и военнопромишлената инфраструктура. За разлика от високоточните западни ракети, чието използване е ограничено от наличностите и редица политико-оперативни ограничения, далекобойните БЛА позволяват провеждането на по-продължителна кампания с многобройни удари по широк набор от цели. В енергийния сектор въздействието постепенно обхваща рафинерии, нефтени терминали, помпени станции и други елементи от системата за производство и транспортиране на горива. През 2026 г. сред поразените обекти са рафинериите в Туапсе, Перм, Ярославъл и Салават, както и обекти в Уралския регион. Украинското Министерство на отбраната отчита десетки удари срещу рафинерии и горивно-логистични съоръжения, докато независими оценки регистрират отделни случаи на прекъсване или ограничаване на руското производство. Тези действия

показват постепенно преминаване от поразяване на единични обекти към системно и целенасочено въздействие върху производството, съхранението и транспортирането на горива (Martin & Vatman 2026; Potter 2026).

Паралелно с това, далекобойните БЛА се използват срещу предприятия от руския военнопромишлен комплекс. Сред показателните цели са: „ВНИИР-Прогресс“ в Чебоксари, свързан с производството на навигационни системи; „АО Ангстрем” в Зеленоград, произвеждащ електронни компоненти; както и предприятие във Воронеж, свързано с производството на компоненти за Х-101, „Искандер-К“ и „Панцир-С1“. Ударите обхващат и химически предприятия, имащи значение за производството на взривни вещества и боеприпаси. По този начин целевият набор се разширява от завършени военни системи към отделни звена от производствената верига, осигуряваща тяхното създаване и поддръжка[7] (Olmsted et al. 2026b).

Натрупването на подобни удари създава допълнително натоварване върху руската система за производство и снабдяване с горива, боеприпаси и военна техника. Ефектът обаче не следва да се разглежда като автоматично прекъсване на руското производство или парализиране на военната икономика, тъй като Русия разполага с резервни мощности и възможности за адаптация. По-значим в оперативно-стратегически план е постоянният натиск върху дълбокия тил, който налага преразпределение на производството, възстановяване на повредени мощности и допълнително ангажиране на средства за тяхната защита.

Операция „Паяжина“ (операція „Павутина“), проведена на 1 юни 2025 г. от Службата за безопасност на Украйна, представлява показателен пример за асиметричен способ за нанасяне на далекобоен удар в стратегическата дълбочина на противника. За разлика от традиционното използване на далекобойни ракети или авиационни средства, при операцията са използвани малогабаритни FPV дронове, предварително разположени в близост до определени руски авиобази и впоследствие насочени срещу намиращите се на стоянка самолети. По този начин сравнително малки и трудно откриваеми средства са използвани за поразяване на високостойностни цели, разположени на значително разстояние от украинска територия. Операцията показва възможност за преодоляване на географската дистанция до стратегическата дълбочина на противника чрез нетрадиционен способ, без необходимост от използване на тежки далекобойни ракети или пилотирана авиация.

Основни цели са авиобазите „Оленя“, „Белая“, „Иваново-Северный“, „Дягилево“ и „Украинка“, използвани за базиране на стратегически бом-

бардировачи и други ключови авиационни платформи. Особеността на избрания способ позволява атаката да бъде извършена едновременно срещу няколко отдалечени обекта, което усложнява противодействието и разширява географския обхват на операцията. По този начин в обект на въздействие се превръща не просто отделна военна цел, а част от системата за базиране и използване на руската стратегическа авиация.

Най-съществени са резултатите от ударите по авиобазите „Оленя“ и „Белая“. Въз основа на анализи на публикувани визуални материали са документирани общо 12 унищожени самолета – седем Ту-95МС, четири Ту-22М3 и един Ан-12, както и поне един допълнително повреден Ту-22М3. На „Оленя“ са унищожени четири Ту-95МС/МСМ и един Ан-12, а на „Белая“ – три Ту-95МС и четири Ту-22М3 (плюс един повреден). Точният размер на загубите остава предмет на допълнителна оценка поради ограничения достъп до изображения с висока резолюция и техническа информация, но независимите анализи показват сходни резултати. Ударите засягат и авиобаза „Иваново-Северный“, където са базирани самолети А-50, предназначени за въздушно разузнаване, целеуказване, командване и управление. Разпространените кадри показват поразяване на два А-50, но не позволяват категорично да се определи степента на пораженията. При „Дягилево“ също са установени данни за въздействие върху авиационна техника, докато опитът за атака срещу „Украинка“ не води до потвърдено поразяване на самолети[8] (Mladenov 2025; Newdick 2025).

В оперативно-стратегически план непосредствените резултати от операцията се изразяват в унищожаването и повреждането на част от авиационния ресурс, използван за реализиране на руските далекобойни огневи действия. По този начин въздействието е насочено не само към отделни платформи, но и към способност, чрез която Русия нанася удари по цели на значителна дълбочина. Намаляването на наличния брой боеспособни самолети от този тип може да ограничи оперативната гъвкавост, да наложи промени в начина на тяхното базиране и да изисква допълнителни ресурси за възстановяване и защита на останалия авиационен парк.

Заключение

Разгледаните примери показват постепенно разширяване и диверсифициране на руските и украинските способности за нанасяне на далекобойни удари. Високоточните ракети осигуряват възможност за въздействие върху високостойностни цели в оперативна дълбочина на противника, но

ограничените количества и невъзможността за бързото им възстановяване налагат търсенето на допълнителни средства. В тази среда далекобойните ударни и разузнавателни БЛА придобиват все по-голямо значение, позволявайки провеждането на по-продължителна кампания срещу широк спектър от военни, енергийни и военнопромишлени обекти. Паралелното развитие на морските безпилотни системи и прилагането на асиметрични способи, демонстрирани от Украйна при операция „Паяжина“, показват стремеж към компенсиране на гореспоменатите ограничения чрез разнообразяване на средствата и способите за достигане до стратегическата дълбочина на противника. Едни от най-важните аспекти от проблематиката, свързана с производството и използването на безпилотни системи във въздушния и морския домейн са много по-ниските производствени разходи и риск за личен състав в сравнение с тези при използването на конвенционални далекобойни огневи средства – фактори, които благоприятстват драстичното увеличаване на производствените мощности и способстват за осигуряването на масирано използване на тези видове системи.

Руската и украинската практика в контекста на „войната на изтощение“ показват, че значението на далекобойните удари не се изчерпва с непосредственото физическо поражение на отделни цели. При определени условия тяхното системно прилагане може да окаже сериозно въздействие върху противниковия ударен потенциал, логистиката, производствените възможности, системата за базиране и защитата на военните средства, създавайки необходимост от усилия по адаптация и преразпределение на ресурси. Именно натрупването на подобни ефекти, а не отделният удар сам по себе си, представлява основата за потенциалното постигане на дългосрочни оперативно-стратегически цели, които могат да бъдат фактор за постигането на победа на едната или другата страна в конфликта.

БЕЛЕЖКИ

1. NATO MOUNTAIN WARFARE CENTRE OF EXCELLENCE (MWCOE), 2024. *Current Russo-Ukrainian Conflict: Ukrainian Air Defence Strategies Against the Russian Invasion. NATO Mountain Warfare Centre of Excellence (MWCOE),* November 2024 [online]. Available from: https://www.mwcoe.org/docs/lesson-learned-2024-workshop-summary/06-current-russo-ukraininan-conflict-ukrainian-air-defence-strategies-against-the-russian-invasion/. [Last viewed: 30.09.2026].

2. AL JAZEERA, 2023. *Russia and Ukraine warn each other travelling ships part of war*, July 2023 [online]. Available from: https://www.aljazeera.com/news/2023/7/20/russia-warns-ships-traveling-to-ukraine-considered-part-of-war. [Last viewed: 30.09.2026].

3. UA.NET, 2026. *1,613 energy facilities in Ukraine have been damaged as a result of Russian attacks, Shmyhal told the UN*, September 2026 [online]. Available from: https://ua.news/en/world/vnaslidok-atak-rf-v-ukrayini-poshkodzheno-1613-energoobiektiv-shmigal-v-oon. [Last viewed: 30.09.2026].

4. AL ARABIA ENGLISH, 2026. *Russia says it struck military infrastructure, vessel in Ukraine*, September 2026 [online]. Available from: https://english.alarabiya.net/News/world/2026/09/27/russia-says-it-struck-military-infrastructure-vessel-in-ukraine>. [Last viewed: 30.09.2026].

5. REUTERS, 2026. *Russia says it struck Ukrainian defence industry facilities, vessels*, September 2026 [online]. Available from: https://www.reuters.com/business/aerospace-defense/russia-says-it-struck-ukrainian-defence-industry-facilities-vessels-2026-09-25/. [Last viewed: 30.09.2026].

6. SAFETY4SEA, 2026. *Russian strike on commercial vessel in Odesa kills captain*, September 2026 [online]. Available from: https://safety4sea.com/russian-strike-on-commercial-vessel-in-odesa-kills-captain/. [Last viewed: 30.09.2026].

7. MINISTRY OF DEFENCE OF UKRAINE, 2026. *Since the start of the year, Ukraine's Defense Forces have struck three major russian military plants, two arsenals, and a key test range*, March 2026 [online]. Available from: https://mod.gov.ua/en/news/since-the-start-of-the-year-ukraine-s-defense-forces-have-struck-three-major-russian-military-plants-two-arsenals-and-a-key-test-range. [Last viewed: 30.09.2026]; MINISTRY OF DEFENCE OF UKRAINE, 2026. *Long-range sanctions reach moscow region, oil refineries keep burning: results of deep-strike operations in May*, June 2026 [online]. Availabe from: https://mod.gov.ua/en/news/long-range-sanctions-reach-moscow-region-oil-refineries-keep-burning-results-of-deep-strike-operations-in-may. [Last viewed: 30.09.2026].

8. RUSSIO-UKRAINIAN WAR SPOTTING, 2026. [online]. Available from: https://ukr.warspotting.net/search/?belligerent=2&weapon=11. [Last viewed: 30.09.2026].

REFERENCES

ATALAN, Y., 2026. Russian Firepower Strike Tracker: Analyzing Missile Attacks in Ukraine. *Center for Strategic and International Studies (CSIS)* [September 2026, online]. Available from: https://www.csis.org/programs/futures-lab/projects/russian-firepower-strike-tracker-analyzing-missile-attacks-ukraine. [Last viewed: 30.09.2026].

BEAUMONT, P. & JONES, S., 2022. Russia has invaded Ukraine: what we know so far', The Guardian. Available from: https://www.theguardian.com/world/2022/feb/24/russia-has-invaded-ukraine-what-we-know-so-far. [Last viewed: 28.09.2026].

BRONK, J., 2026. Four Years On: An Update on the Air War Over Ukraine. *Royal United Services Institute (RUSI)* [July 2026, online]. Available from: https://www.rusi.org/explore-our-research/publications/commentary/four-years-update-air-war-over-ukraine. [Last viewed: 30.09.2026].

CLARK, M. & WOLKOW, N., 2023. Special Edition Campaign Assessment: Ukraine's Strike Campaign Against Crimea. *Institute for the Study of War (ISW)* [October 2023, online]. Available from: https://understandingwar.org/research/russia-ukraine/

special-edition-campaign-assessment-ukraines-strike-campaign-against-crimea/. [Last viewed: 30.09.2026].

CHILDS, N., 2023. Ukraine darkens Russia's naval prospects in the Black Sea. *International Institute for Strategic Studies (IISS)* [September 2023, online]. Available from: https://www.iiss.org/online-analysis/military-balance/2023/09/ukraine-darkens-russias-naval-prospects-in-the-black-sea/ [Last viewed: 30.09.2026].

CHIUSA, S., 2026. Forged in War: The Evolution of Ukraine's Air Defenses. *Geopolitical Monitor* [September 2026, online]. Available from: https://www.geopoliticalmonitor.com/forged-in-war-the-evolution-of-ukraines-air-defenses./ [Last viewed: 30.09.2026].

DELANOE, I., 2024. Russia's Black Sea Fleet in the "Special Military Operation" in Ukraine. *Foreign Policy Research Institute (FPRI)* [February 2024, online]. Available from: https://www.fpri.org/article/2024/02/russias-black-sea-fleet-in-the-special-military-operation-in-ukraine/. [Last viewed: 30.09.2026].

DOUGHERTY, M., 2025. *Aircraft, Tanks and Artillery of the Ukraine War.* Amber Books. ISBN: 978-1-83886-350-0.

EVANS, A. et al., 2023a. Russian Offensive Campaign Assessment, [September 25, 2023]. *Institute for the Study of War (ISW)* [September 2023, online]. Available from: https://understandingwar.org/research/russia-ukraine

EVANS, A. et al., 2023b. Russian Offensive Campaign Assessment, [December 23, 2023]. *Institute for the Study of War (ISW)* [December 2023, online]. Available from: https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment_23-11/. [Last viewed: 30.09.2026].

GWADERA, Z., 2023. Ukraine targets Russian airfields with US-supplied ATACMS missile. *International Institute for Strategic Studies (IISS)* [October 2023, online]. Available from: https://www.iiss.org/online-analysis/missile-dialogue-initiative/2023/10/ukraine-targets-russian-airfields-with-us-supplied-atacms-missile. [Last viewed: 30.09.2026].

HODUNOVA, K., 2026. Russian strikes on Kyiv data centers disrupt operations at several Ukrainian media outlets. *The Kyiv Independent* [September 2026, online]. Available from: https://kyivindependent.com/russian-strikes-on-kyiv-data-centers-disrupt-operations-at-several-ukrainian-media-outlets/. [Last viewed: 30.09.2026].

HARDING, L. & ROTH, A., 2026. Ukraine 'offering Russia deal to halt attacks on civilian ships in Black Sea'. *The Guardian* [August 2026, online]. Available from: https://www.theguardian.com/world/2026/aug/13/ukraine-proposes-deal-with-russia-to-halt-attacks-on-civilian-ships-in-black-sea. [Last viewed: 30.09.2026].

JOHNSON, R., 2015. How Russia fired missiles at Syria from 1,000 miles away. *The Washington Post* [October 2015, online]. Available from: https://www.washingtonpost.com/graphics/world/russian-cruise-missile/. [Last viewed: 29.09.2026].

KUSHNIKOV, K., 2024. Arsenal in Bryansk region struck by ATACMS missiles. *Militarnyi* [November 2024, online]. Available from: https://militarnyi.com/en/news/arsenal-in-bryansk-region-struck-by-atacms-missiles/. [Last viewed: 30.09.2026].

KAUSHAL, S., 2023. Ukraine's Uncrewed Raid on Sevastopol and the Future of War at Sea. *Royal United Services Institute (RUSI)* [February 2023, online]. Available from: https://www.rusi.org/explore-our-research/publications/commentary/ukraines-uncrewed-raid-sevastopol-and-future-war-sea. [Last viewed: 30.09.2026].

KAUSHAL, S., 2024. Lessons for the Royal Navy's Future Operations from the Black and Red Sea. *Royal United Services Institute (RUSI)* [July 2024, online]. Available from: https://www.rusi.org/explore-our-research/publications/commentary/lessons-royal-navys-future-operations-black-and-red-sea. [Last viewed: 30.09.2026].

LANCASTER, J., 2022. An Anti-Access Denial Strategy for Ukraine. Center for International Maritime Security. *Center for International Maritime Security (CIMSEC)* [April 2022, online]. Available from: https://cimsec.org/an-anti-access-denial-strategy-for-ukraine/. [Last viewed: 30.09.2026].

MLADENOV, A., 2025. A mission like no others: Ukraine's drone attack on Russian strategic bomber bases. *HeliopsMag* [June 2025, online]. Available from: https://www.heliopsmag.com/antares/articles/a-mission-like-no-others-ukraines-drone-attack-on-russian-strategic-bomber-bases/. [Last viewed: 30.09.2026].

MARTIN, D. & VATMAN, T., 2026. Russian refining sector struggles amid intensifying Ukrainian attacks. *The International Energy Agency (IEA)* [September 2026, online]. Available from: https://www.iea.org/commentaries/russian-refining-sector-struggles-amid-intensifying-ukrainian-attacks. [Last viewed: 30.09.2026].

NEWDICK, T., 2025. Confirmed Losses of Russian Aircraft Mount After Ukrainian Drone Assault. *The War Zone* [June 2025, online]. Available from: https://www.twz.com/air/firm-evidence-of-russian-aircraft-losses-after-ukrainian-drone-strikes. [Last viewed: 30.09.2026].

OLMSTED, J. et al., 2026a. Russian Offensive Campaign Assessment, June 22, 2026. *Institute for the Study of War (ISW)* [June 2026, online]. Available from: https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment-june-22-2026/. [Last viewed: 30.09.2026].

OLMSTED, J. et al., 2026b. Russian Offensive Campaign Assessment, September 26, 2025. *Institute for the Study of War (ISW)* [September 2026, online]. Available from: https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment-september-26-2025/. [Last viewed: 30.09.2026].

PILI, G., 2024. Sea drones at war: Tactical, operational and strategic analysis of maritime uncrewed systems. *European Security and Defence (ESD)* [September 2024, online]. Available from: https://euro-sd.com/2024/09/articles/40191/sea-drones-at-war-tactical-operational-and-strategic-analysis-of-maritime-uncrewed-systems/. [Last viewed: 30.09.2026].

POTTER, M., 2026. What has been hit in Ukraine's attacks on Russian energy sites? *Reuters* [June 2026, online]. Available from: https://www.reuters.com/business/energy/ukraine-attacks-russian-energy-sites-what-has-been-hit-2026-08-27/. [Last viewed: 30.09.2026].

SWANSTON, M. & SWANSTON, A., 2025. *Air Warfare Illustrated Atlas*. Amber Books. ISBN 978-1-83886-494-1.

SUTTON, H., 2024. Uncrewed Platforms Have Been Critical to Ukraine's Success in the Black Sea. *Royal United Services Institute (RUSI)* [August 2024, online]. Available from: https://www.rusi.org/explore-our-research/publications/commentary/uncrewed-platforms-have-been-critical-ukraines-success-black-sea. [Last viewed: 30.09.2026].

LONG-RANGE STRIKES AS A MEANS OF ACHIEVING LONG-TERM OPERATIONAL-STRATEGIC OBJECTIVES IN THE UKRAINE WAR

Abstract. The paper examines key aspects of long-range strikes as one of the instruments for achieving operational-strategic objectives with long-term implications in the war in Ukraine (2022–present), identifying major trends in the employment of different types of strike capabilities and their impact on the dynamics and development of the conflict. To this end, a balanced and well-substantiated analysis is presented, based on the documentary research method and drawing upon a variety of publicly available sources, including academic articles and reports, journalistic materials, and expert assessments concerning long-range strikes conducted by both opposing sides.

Keywords: Russia; Ukraine; long-range strikes; operational-strategic objectives with long-term implications

Lieutenant Junior Grade (LTJG) Dimo Savov
ORCID iD: 0009-0008-9871-8980
Bulgarian Navy Command
16, Preslav St.
9000 Varna, Bulgaria
E-mail: dimo.kr.savov@gmail.com

Plamen Dyakov
ORCID iD: 0009-0003-2848-9733
Rakovski National Defence College
82, Evlogi i Hristo Georgievi Blvd.
1504 Sofia, Bulgaria
E-mail: plamen.dyakov.jr.99@gmail.com

https://doi.org/10. 66334/annu26_opintraisyst

ВЪЗМОЖНОСТИ ЗА ВЪВЕЖДАНЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ В СИСТЕМИТЕ ЗА ОБРАБОТКА НА БАГАЖ НА ЛЕТИЩАТА

д-р Елена Стоянова
Военна академия „Георги Стойков Раковски“

Абстракт. Постепенното въвеждане на изкуствения интелект в наземното обслужване на летищата поставя нови въпроси пред авиационната сигурност, особено по отношение на обработката и проверката на регистрирания багаж, където значителна част от дейностите са вече автоматизирани. Целта на изследването е да се изясни с какво би допринесъл изкуственият интелект за усъвършенстване на мерките за сигурност при интегрирането му в системите за обработка на багаж (Baggage handling system – BHS), системите за откриване на експлозиви (Explosive Detection System – EDS) и процесите, свързани със съпоставянето на багажа с регистриралия го пътник. Чрез анализ на нормативни документи, съвременни технологични решения и въведени практики на летища, се обосновава тезата, че изкуственият интелект не замества автоматизираната система за откриване на експлозиви, а изпълнява аналитична функция въз основа на данните, предоставени от системата за обработка на багаж. Анализирани са потенциалните възможности за откриване на аномалии, проследяване на багажа и подпомагане на човешкото решение, както и ограниченията, отнасящи се до качеството на данните, грешките на алгоритмите, киберсигурността и прекаленото предоверяване към автоматизираните системи.

Ключови думи: изкуствен интелект; авиационна сигурност; наземно обслужване; системи за обработка на багаж, система за откриване на експлозиви

I. Въведение

През последните години въздушният транспорт се развива с изключително бързи темпове. Летищната инфраструктура и оперативните дейности не успяват да догонят този ръст. Закъсненията на полетите се превръщат в ежедневие, като значителна част от тях се дължат на оперативна неефективност на летищата, авиокомпаниите, техническата поддръжка, проблеми с разпределянето на екипажите, забавяне при почистване и зареждане на въздухоплавателните средства, както и на трудности при обработването на багажа на перона[1]. Една от основните причини за експлоатационните затруднения на операторите по наземно обслужване е критичният недостиг на квалифициран персонал. В рамките на наземното обслужване, управлението на багажната система е от съществено значение за рационализиране на летищните дейности и намаляване на закъсненията на полетите. Поради тази причина автоматизацията и изкуственият интелект (ИИ) се явяват като закономерни решения за оптимизиране работата на съществуващия персонал и на дейностите, свързани с обработването на регистрирания багаж. Автоматизацията постепенно променя не само начина, по който се осъществяват отделните оперативни дейности, но и начина, по който се управляват взаимовръзките между тях (Aleksandrova, Tagareva, Vasileva 2005). Багажът на пътника преминава през няколко етапа, свързани с безопасността и сигурността на полетите. Процесът включва предаване от пътника на гише за регистрация, идентификация, съпоставяне на пътника с багажа му, транспортиране по багажната лента, проверка за сигурност, сортиране за съответния полет и натоварване на въздухоплавателното средство. За постигане на максимална ефективност е необходимо всички тези процеси да се интегрират в цялостна взаимосвързана система.

В програмата си за 2026 г. Международната асоциация за въздушен транспорт поставя въпроса за адаптиране на наземното обслужване към изкуствения интелект, като свързва технологичното развитие с безопасността, ефективността, устойчивостта и човешката експертиза[2]. Акцентът се поставя върху съчетаването на технологиите с експертизата на персонала, което доказва, че основното предизвикателство вече не е дали изкуственият интелект ще навлезе в дейностите по наземно обслужване, а как точно той ще бъде интегриран и контролиран. От гледна точка на авиационната сигурност от основно значение е как ще бъде интегриран изкуственият интелект с багажната система и автоматизираните решения. Европейската нормативна рамка изисква регистрираният багаж да премине проверка

за сигурност преди да бъде натоварен на въздухоплавателното средство, като багажът задължително трябва да бъде съпоставен с пътника, който го е регистрирал, и да бъде защитен от външна намеса до неговото натоварване[3]. Основният изследователски въпрос е свързан с определянето на конкретната допълнителна стойност, която би донесло въвеждането на изкуствен интелект за проверката на регистрирания багаж, при положение че съвременните системи вече използват автоматизиран анализ на заплахите. Отговорът на този въпрос не следва да се основава на предположението, че новият алгоритъм непременно е по-ефективен от съществуващия. Настоящото изследване стъпва на хипотезата, че допълнителната стойност се проявява на ниво интеграция, тоест при съпоставяне на данните от системите за откриване на експлозиви с информацията за пътника, идентификацията на багажа му, движението по багажната лента, съответния полет, трансферния статут и друга съотносителна оперативно-техническа информация.

II. Изложение

2.1. Правна основа

Регламент за изпълнение (ЕС) 2015/1998 на Комисията определя автоматизираната система за откриване на експлозиви (EDS) като един от основните методи за проверка на регистрирания багаж. Наред с изискванията за неговата идентификация, съпоставяне и защита, регламентът урежда и действията, които операторът по сигурност следва да предприеме, когато не може да установи дали багажът съдържа забранени предмети[4].

Същият регламент налага и важно оперативно ограничение, според което лицата, извършващи преглед на рентгенови изображения, не могат да прекарват повече от двадесет минути непрекъснато пред монитора, след което трябва да почиват задължително поне десет минути[5]. В тази връзка въвеждането на изкуствен интелект може да се разглежда като средство за намаляване на рисковете, свързани с човешката умора. Допълнително, стандартите по сигурност предвиждат, че ако даден багаж се превърне в непридружен поради отказ на пътника да се качи на борда, той задължително се сваля от самолета, което изисква изключителна координация между Системата за обработка на багаж, оператора по наземно обслужване и летищния оператор.

Важно и да се отбележи, че интегрирането на изкуствения интелект не трябва да се разглежда като замяна на съществуващите мерки и на човека в системата, а като средство за повишаване на ефективността на при-

лаганите процедури (Demirov, Aleksandrova, Tagareva 2006). Чрез анализ на изображенията от EDS, както и на данните, генерирани в процеса на обработка на багажа, алгоритмите могат да откриват отклонения от стандартните експлоатационни практики, свързани с процесите по обработка на регистрирания багаж, да подпомагат откриването на подозрителни характеристики, и да предоставят допълнителна информация. По този начин изкуственият интелект има потенциал да подобри точността и последователността на проверките, като същевременно, крайната отговорност за взимане на решение остава при обучените служители по авиационна сигурност.

2.2. Практически примери с въведен изкуствен интелект на международните летища

Въведените технологични практики в световен мащаб показват ясна тенденция към интегриране на ИИ в реалната летищна експлоатация. На летище Франкфурт, летищният оператор Fraport съвместно с Федералната полиция използва алгоритми на изкуствен интелект за анализ на изображенията от EDS, вследствие на което пропускателната способност на пунктовете за проверка се повишава с над дванадесет процента[6]. Допълнително, чрез използването на компютърно зрение в системата за наблюдение, летището превръща визуалните събития на перона в структурирани данни, оптимизирайки координацията при натоварването на контейнерите в самолета[7]. Опитът от използването на изкуствен интелект при проверката на пътници и ръчен багаж показва потенциала на тези технологии за повишаване на ефективността на проверките за сигурност. Подобни подходи могат да бъдат приложени и в системите за проверка на регистриран багаж.

Летище Амстердам Схипхол е въвело ИИ за оптимизиране както на проверките, така и на физическата обработка на багажния поток. Чрез участие в международни изследователски проекти летището прилага компютърно зрение за откриване на експлозиви и оръжия на пунктовете за проверка въз основа на отворени софтуерни платформи[8]. За преодоляване на недостига на персонал в зоната за обработка на багаж, Схипхол въвежда роботизирани системи за автоматизирано подреждане и натоварване на регистриран багаж в специални контейнери, които работят в пълен синхрон с автономни електрически влекачи на перона[9].

На летище Лондон Хийтроу се провежда мащабна модернизация на стойност един милиард лири, при която новите системи за откриване на експлозиви се управляват от специализирани алгоритми[10]. В допълнение

към традиционните проверки по авиационна сигурност, на летище Хийтроу се използват мултимодални модели на изкуствен интелект за анализ на рентгенови изображения на регистрирания багаж. Системите са предназначени за идентифициране на предмети, свързани с незаконния трафик на защитени видове от дивата природа, като демонстрират висока степен на точност и при откриването на контрабандни товари[11].

В Азия летище Сингапур Чанги интегрира ИИ като съществен елемент от новия си Терминал 5, като фокусът е насочен към елиминиране на човешките грешки при наземното транспортиране на дълги разстояния. Летището въвежда в редовна експлоатация автономни безпилотни влекачи за превоз на багажни контейнери между съществуващите терминали[12]. Алгоритмите управляват трафика на перона при тежки тропически метеорологични условия, докато човешкият персонал е преквалифициран в дистанционни оператори, наблюдаващи процесите от централизиран команден пункт.

2.3. Оперативни предимства и системни рискове за сигурността

Описаните примери за приложение на ИИ са пряко обвързани с новата правна рамка за наземно обслужване, въведена с Регламент (ЕС) 2025/24 на Комисията, който за първи път хармонизира изискванията към операторите и изрично включва обработката, идентификацията, сортирането и трансфера на багажа в обща система за управление на безопасността[13]. Важен аспект на тази нова регулация е, че организациите, извършващи обработка на багаж, попадат под обхвата на изискванията за информационна сигурност (Part-IS), въведени от Европейската агенция за авиационна безопасност[14]. Това означава, че защитата на ИИ моделите и каналите за обмен на данни в багажната система вече е задължително правно изискване, целящо предотвратяване на киберинциденти, които биха могли да компрометират авиационната сигурност[15].

Оперативните предимства от внедряването на ИИ се изразяват в способността му да поддържа постоянна степен на детекция, елиминирайки фактора човешка умора, и да открива сложни несъответствия между данните за пътника и неговия багаж, които остават невидими за изолираните системи за откриване на експлозиви. Независимо от това, Националният институт за стандарти и технологии на САЩ подчертава, че ограниченията на изкуствения интелект извън условията, при които технологията е разработена, трябва да бъдат детайлно документирани. Основен риск за сигурността е феноменът Automation bias, при който човешкият оператор

развива сляпо предоверяване към системата и спира да извършва контролна проверка на изображенията, разчитайки изцяло на ИИ[16].

Допълнителна уязвимост представлява приплъзването на данните (Data drift), тъй като появата на нови видове взривни вещества или иновативни методи за укриването им, може да понижи точността на ИИ, тъй като той не е обучен да ги разпознава. Свързването на подсистемите в единна дигитална мрежа създава и уязвимост от целенасочени кибератаки срещу самите модели (adversarial attacks), при които минимална модификация в цифровия код на рентгеновото изображение може да направи опасен предмет напълно невидим за изкуствения интелект (Metin et al. 2006). Поради тези причини Актът за изкуствения интелект на Европейския съюз класифицира системите, използвани в авиационната сигурност, като високорискови, налагайки строги правила за прозрачност и задължителен човешки надзор[17].

III. Заключение

На базата на извършения анализ може да се обобщи, че изкуственият интелект притежава значителен потенциал за трансформиране на летищната сигурност, но неговата роля не трябва да се тълкува като механична замяна на съществуващото оборудване за откриване на експлозиви. Практическата стойност на технологията се намира на ниво интеграция, където тя действа като интелигентен аналитичен слой, обединяващ оперативните събития от багажната система с данните за сигурност. Успешното внедряване на ИИ изисква стриктно управление на технологичните рискове, произтичащи от грешки в алгоритмите, киберзаплахи и психологическото предоверяване от страна на служителите (Vidhate et al. 2025).

В перспектива, развитието на сигурността при обработката на багаж ще се определя от способността на летищните оператори да изграждат архитектури, съвместими с принципа за постоянен човешки контрол, при които машината обработва големи масиви от данни в реално време, но крайното решение и юридическата отговорност остават изцяло в ръцете на човека.

БЕЛЕЖКИ

1. OAG, 2025. *AI and trusted data: Building resilient airline operations* [online]. Available from: https://www.oag.com/ai-aviation-operations.

2. International Air Transport Association (IATA), 2026. *IATA Ground Handling Conference 2026: Adapting Ground Operations in an Era of AI*, 15 April 2026 [online].

Available from: https://www.iata.org/en/pressroom/2026-releases/2026-04-15-01/.

3. Европейска комисия, 2015. Регламент за изпълнение (ЕС) 2015/1998 на Комисията от 5 ноември 2015 година за установяване на подробни мерки за прилагането на общите основни стандарти за сигурност във въздухоплаването. *EUR-Lex* [online]. Available from: https://eur-lex.europa.eu/eli/reg_impl/2015/1998/2025-05-21/eng.

4. Пак там.

5. Пак там.

6. Future Travel Experience, 2025. *Lufthansa, Fraport and zeroG drive innovation at FRA with AI-supported ground processes* [online]. Available from: https://www.futuretravelexperience.com/2025/07/lufthansa-fraport-and-zerog-drive-innovation-at-fra-with-ai-supported-ground-processes/.

7. Пак там.

8. Schiphol Group Aviation Solutions, 2024. *Collaborating to use AI in security screening: Pangiam Project DARTMOUTH.* Royal Schiphol Group. [online]. Available from: https://www.schiphol.nl/en/aviation-solutions/pangiam-project-dartmouth/.

9. Inter Airport Europe, 2025. *Airport Technology Innovations: Automation, AI & Safety Upgrades at Leading Hubs* [online]. Available from: https://www.interairportglobal.com/en-gb/blog/industry-insights/airport-technology-automation-ai-safety-innovations.html.

10. Smiths Detection, 2026. Smiths Detection 3D X-ray technology deployed in £1bn Heathrow upgrade, [30 January 2026]. [online]. Available from: https://www.smithsdetection.com/press-releases/smiths-detection-3d-x-ray-technology-deployed-in-1bn-heathrow-upgrade/.

11. British Aviation Group, 2024. *Heathrow Airport trials AI-based screening technology for detecting wildlife trafficking* [online]. Available from: https://www.britishaviationgroup.co.uk/knowledge/heathrow-airport-trials-ai-based-screening-technology-for-detecting-wildlife-trafficking/.

12. Changi Airport Group, 2026. *Changi Airport rolls out autonomous tractors in major step towards airside automation.* Changi Airport Media Hub [online]. Available from: https://www.changiairport.com/en/corporate/our-media-hub/newsroom/2026/autonomous-tractors.html.

13. Европейска комисия, 2025. Регламент за изпълнение (ЕС) 2025/24 на Комисията от 19 декември 2024 година за изменение на Регламент (ЕС) № 965/2012 по отношение на изискванията към операторите на въздухоплавателни средства, свързани с дейностите по наземно обслужване. *EUR-Lex* [онлайн]. Достъпно на: https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:32025R0024.

14. European Union Aviation Safety Agency (EASA), 2026. *EASA releases latest issue of its Concept Paper on Artificial Intelligence for comment* [online]. Available from: https://www.easa.europa.eu/en/newsroom-and-events/news/easa-releases-latest-issue-its-concept-paper-artificial-intelligence.

15. Bentley, S., 2025. *EASA information & cyber security regulations: Impact on aviation,* [10 March 2025]. Sassofia Aviation Blog. [online]. Available from: https://sassofia.com/blog/easa-information-cyber-security-regulations-impact-on-aviation/.

16. European Union Aviation Safety Agency (EASA), 2026. *EASA releases latest issue of its Concept Paper on Artificial Intelligence for comment* [online]. Available from: https://www.easa.europa.eu/en/newsroom-and-events/news/easa-releases-latest-issue-its-concept-paper-artificial-intelligence.

17. Европейски парламент и Съвет, 2024. Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 година за установяване на хармонизирани правила относно изкуствения интелект и за изменение на регламенти (ЕО) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и директиви 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828 (Акт за изкуствения интелект). *EUR-Lex* [онлайн]. Достъпно на: https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32024R1689.

18. Европейска комисия, 2025. Регламент за изпълнение (ЕС) 2025/23 на Комисията от 19 декември 2024 година за определяне на правила за прилагането на Регламент (ЕС) 2018/1139 на Европейския парламент и на Съвета по отношение на изискванията за надзор над наземното обслужване и организациите, които го предоставят. *EUR-Lex* [онлайн]. Достъпно на: Регламент за изпълнение - ЕС - 2025/23 - EN - EUR-Lex.

19. European Civil Aviation Conference (ECAC), 2025. *Frequently Asked Questions (FAQs) about the ECAC Common Evaluation Process (CEP) of Security Equipment* (Version 5.7.2) [online]. Available from: https://www.ecac-ceac.org/images/activities/security/FAQs-ECAC%20CEP_20251015.pdf.

20. National Academies of Sciences, Engineering, and Medicine, 2025. *Exploring the Impact of Artificial Intelligence on the Airport Industry* (ACRP Web-Only Document 67). Washington, DC: The National Academies Press. https://doi.org/10.17226/29426.

ЛИТЕРАТУРА

АЛЕКСАНДРОВА, В.; ТАГАРЕВА, В. & ВАСИЛЕВА, В., 2025. Относно, потребностите от знанието и изкуствения интелект, като гаранция за промяната на съвременна България – етични аспекти от приложението на изкуствения интелект в автономните системи. В: *Сборник научни доклади от XVIII Международна конференция по открит и подводен добив на полезни изкопаеми,* [08 – 12 септември 2025 г., Варна], с. 225 – 233. София: НТС по МДГМ. ISSN 2535-0854.

ДЕМИРОВ, П.; АЛЕКСАНДРОВА, В. & ТАГАРЕВА, В., 2026. *Изкуственият интелект като архитект, стратег и оптимизатор.* София: Авангард прима. ISBN 978-619-279-262-6.

METIN, B., DÜMER, H. & WYNN, M., 2026. Aviation cybersecurity governance: Towards an operational framework and solutions agenda for the airport domain. *Information,* vol. 17, no. 2, p. 177. https://doi.org/10.3390/info17020177.

VIDHATE, K.; SAWANT, S.; CHAVAN, S.; VAGADIYA, B.; TALAPATRA, D.; BIDWE, R. & JOSHI, A., 2025. A computer vision framework for proactive anomaly detection and risk reduction in airport baggage logistics. *Scientific Reports,* vol. 15, no. 37980. [online]. Available from: https://www.nature.com/articles/s41598-025-21959-7. ISSN (online) 2045-2322.

REFERENCES

ALEKSANDROVA, V.; TAGAREVA, V. & VASILEVA, V., 2025. Otnosno, potrebnostite ot znanieto i izкyctvenia intelekt, kato garantsia za promyanata na savremenna Bulgaria – etichni aspekti ot prilozhenieto na izkustvenia intelekt v avtonomnite sistemi. In: *Sbornik nauchni dokladi ot HVIII Mezhdunarodna konferentsia po otkrit i podvoden dobiv na polezni izkopaemi*, [08 – 12 septemvri 2025 g., Varna], pp. 225 – 233. Sofia: NTS po MDGM. ISSN 2535-0854. [in Bulgarian].

DEMIROV, P.; ALEKSANDROVA, V. & TAGAREVA, V., 2026. *Izkustveniyat intelekt kato arhitekt, strateg i optimizator.* Sofia: Avangard prima. ISBN 978-619-279-262-6. [in Bulgarian].

METIN, B., DÜMER, H. & WYNN, M., 2026. Aviation cybersecurity governance: Towards an operational framework and solutions agenda for the airport domain. *Information,* vol. 17, no. 2, p. 177. https://doi.org/10.3390/info17020177.

VIDHATE, K.; SAWANT, S.; CHAVAN, S.; VAGADIYA, B.; TALAPATRA, D.; BIDWE, R. & JOSHI, A., 2025. A computer vision framework for proactive anomaly detection and risk reduction in airport baggage logistics. *Scientific Reports,* vol. 15, no. 37980. [online]. Available from: https://www.nature.com/articles/s41598-025-21959-7. ISSN (online) 2045-2322.

OPPORTUNITIES FOR THE INTRODUCTION OF ARTIFICIAL INTELLIGENCE IN AIRPORT BAGGAGE HANDLING SYSTEMS

Abstract. The gradual introduction of artificial intelligence into airport ground handling raises new questions for aviation security, particularly with regard to the handling and screening of checked baggage, where a significant part of the activities is already automated. The aim of this study is to clarify how artificial intelligence could contribute to improving security measures through its integration into baggage handling systems (Baggage handling system – BHS), explosive detection systems (Explosive Detection System – EDS), and the processes related to baggage reconciliation with the passenger who checked it in. Through an analysis of regulatory documents, contemporary technological solutions, and implemented airport practices, the study substantiates the thesis that the artificial intelligence does not replace the automated explosive detection system but rather performs an analytical function based on the data provided by the baggage handling system. The potential capabilities for anomaly detection, baggage tracking, and support of human decision-making are analyzed, as well as the limitations related to data

quality, algorithmic errors, cybersecurity, and excessive reliance on automated systems.

Keywords: artificial intelligence; aviation security; ground handling; baggage handling systems; explosive detection system

Dr. Elena Stoyanova, Assist. Prof.
ORCID iD: 0000-0002-3057-8693
Air Force and Air Defence Department
Command and Staff Faculty
Rakovski National Defence College
82, Evlogi i Hristo Georgievi Blvd.
1504 Sofia, Bulgaria
E-mail: e.stoyanova@rndc.bg

https://doi.org/10. 66334/annu26_privawar

ПРИВАТИЗАЦИЯТА НА ВОЙНАТА: ЧАСТНИТЕ ВОЕННИ КОМПАНИИ КАТО ФАКТОР ЗА ОТБРАНАТА И СИГУРНОСТТА В ПРОМЕНЯЩИЯ СЕ СВЯТ

Запрян Вълков
Университет за национално и световно стопанство

Абстракт. Настоящата статия изследва отражението на частното участие върху отбранителните способности, държавния контрол и публичната отчетност в съвременните конфликти. Съпоставени са три групи казуси – реорганизацията на руските военни мрежи в Африка, предложената поддръжка на системите Patriot и снабдяването с дронове за Украйна и частната охрана при разпределянето на помощи в Газа. Анализът се основава на целево подбрани изследвания и публични документи. Данните за украинските поръчки показват увеличаване на броя производители в определена платформа, но не позволяват да се установи общият брой на частните фирми. Съпоставката разкрива различни форми на държавна координация и различни рискове за отчетността и устойчивостта на снабдяването. Обоснована е необходимостта оценката на изпълнителите да включва техните функции, фактическия контрол, възможностите за разследване и зависимостта от критични компоненти.

Ключови думи: частни военни и охранителни компании; производители на дронове; Украйна; държавен контрол; публична отчетност

I. Увод

Частното участие в съвременните конфликти обхваща различни дейности – от охрана и техническа поддръжка до разработване и доставка на безпилотни системи. Тази разнородност поставя въпроса не само какво възлага държавата, но и дали запазва контрол върху изпълнението и последиците. Авант разглежда именно промените в контрола върху употребата на сила при възлагане на охранителни функции (Avant 2005). Производителят на дронове обаче не може да бъде приравнен на частна военна компания единствено защото доставя изделие за въоръжените сили[1].

Основната цел на статията е да изясни как различните форми на участие влияят върху отбранителните способности и публичната отчетност. Изходната теза е, че правният и политическият анализ не бива да се ограничава до собствеността на фирмата: значение имат възложената задача, фактическото командване, договорното отношение и възможността да се потърси отговорност. В този смисъл контролът върху една организация и контролът върху действията ѝ са свързани, но не тъждествени въпроси.

Приложен е качествен сравнителен подход към руските военни мрежи в Африка, поддръжката и дроновите доставки за Украйна и охраната на помощи в Газа. Използвани са научни публикации и публични документи до септември 2026 г. Казусите се съпоставят по функции, държавни връзки, зависимости и отчетност. Подборът не е представителен, броят фирми, договори и доставки се тълкува според обхвата на източника.

II. Понятия и аналитична рамка

2.1. *Функции и правен статут*

Необходимо е най-напред да се уточни обхватът на понятието „частни военни и охранителни компании“ (ЧВОК). В Документа от Монтрьо то обозначава частни стопански субекти, които предоставят военни или охранителни услуги, включително въоръжена охрана, поддръжка на оръжейни системи и обучение. Следователно предметът на договора е по-важен от названието на фирмата. Самата продажба на дрон не е достатъчна, за да бъде производителят определен като ЧВОК, такава преценка изисква да се установи дали той изпълнява и услуги от посочения вид.

Разграничението има значение и за правния статут на служителите. Според Документа от Монтрьо той се определя с оглед на функциите и конкретните обстоятелства, а гражданските лица са защитени от нападение,

освен ако и докато участват пряко във военните действия. Производството на въоръжение само по себе си не решава този въпрос. Частният договор не освобождава държавата от собствените ѝ международноправни задължения, същевременно отговорността ѝ за определено деяние на изпълнителя зависи от конкретните основания за приписването му.

2.2. *Държавно влияние и пазарно изпълнение*

Проблемът за контрола не се изчерпва с формалното разграничение между публичен възложител и частен изпълнител. При „Вагнер“ Ларсен описва преплитане на институционални отношения и неформални зависимости с руската държава (Larsen 2025). При производството на дронове за Украйна Дрокалос, обратно, акцентира върху държавно определените условия за допускане и поръчки, при които се конкурират множество фирми (Drokalos 2026). Двете изследвания разглеждат различни дейности, затова съпоставката им служи за изясняване на формите на контрол, а не за приравняване на участниците.

III. Форми на частно участие в конфликтите

3.1. *Преструктурирането на руските военни мрежи*

Руският случай показва защо промяната на организационната форма не бива да се приема за пълно прекъсване на предишните отношения. Според Изследователската служба на Конгреса на САЩ „Африканският корпус“ се намира под надзора на руското военно разузнаване, но в дейността му могат да участват и бивши кадри на „Вагнер“, и служители на други частни военни компании. В Мали корпусът формално поема мрежите на „Вагнер“ в средата на 2025 г. (Arieff et al. 2026). Ето защо той не следва да се представя просто като поредната частна фирма, същевременно формалната промяна не доказва, че местните връзки са изчезнали.

По-ясната командна принадлежност сама по себе си не отговаря на въпроса как се разследват действията на формированието. Human Rights Watch съобщава, че през юли 2026 г. при операция в Бомбори, Мали, са убити девет цивилни, сред които четири деца, и приписва действията на бойци от „Африканския корпус“, придружавани от малийски военнослужещи[2]. Констатациите са основани и на дистанционни интервюта и не представляват съдебна присъда. Случаят поставя въпрос за независимото установяване на фактите, без да доказва причинна връзка между реорганизацията и насилието.

3.2. *Украйна: техническа поддръжка и снабдяване с дронове*

При Украйна частното участие обхваща различни по характер услуги. През август 2025 г. DSCA уведомява за *възможна* продажба на поддръжка за системите Patriot, като посочва RTX и Lockheed Martin за основни изпълнители и предвижда техни представители за обучение и срещи в Европейското командване на САЩ[3]. Уведомлението не доказва сключен договор или предоставена услуга. То поставя въпроса за зависимостта от специализирана поддръжка, резервни части и софтуерни обновления, различен от въпроса кой командва въоръжен персонал.

Разрастването на дроновата индустрия очертава друга форма на участие. Reuters съобщава за около 200 производители в Украйна през март 2024 г. и за фирма, доставяща части и софтуерни промени пряко на подразделенията (Young 2024). Това е моментна оценка, не изчерпателен регистър. През април 2025 г. украинското министерство посочва договори със 76 производители през 2024 – 2025 г.[4]. Числото се отнася до контрагентите по тези договори и не разкрива собствеността на всяка фирма или размера на целия сектор.

Съпоставими сведения за повече доставчици идват от една и съща платформа – през юли 2025 г. в DOT-Chain Defence участват 11 производители, а през август каталогът предлага 146 модела от 20 производители[5]. Подразделенията избират изделие, докато агенцията управлява договора, логистиката и плащането. Към август Министерството отчита доставки чрез платформата на стойност 127 млн. гривни[6]. Данните се отнасят само до този пилотен канал, не до цялата индустрия.

Разширяването на производството не премахва уязвимостите в снабдяването. Според Reuters програмите за дронове с минореактивни двигатели зависят от ограничен кръг европейски доставчици, а представители на сектора съобщават за недостиг на двигатели и материали (Kahn et al. 2026). Анализ на RUSI посочва, че много от необходимите компоненти не се произвеждат в Украйна и значителна част се набавя от Китай (Niederkofler 2025). Следователно местното сглобяване и наличието на повече производители не са равнозначни на независимост по цялата верига за доставки.

3.3. *Частната охрана при разпределянето на помощи в Газа*

В Газа на преден план излиза въоръжената охрана. Според Reuters през 2025 г. UG Solutions охранява пунктове на Gaza Humanitarian Foundation, чиято безопасност за търсещите помощи е критикувана от ООН. Компа-

нията заявява, че не контролира действията на израелските сили. През февруари 2026 г. се съобщава за разговори за нова роля, без окончателна договореност (Magid & Ayyub 2026). Смъртните случаи край пунктовете не установяват сами по себе си вина на компанията, за оценката са необходими отделни данни за действията на всеки участник.

IV. Сравнителен анализ и значение за отбранителната политика

Казусите не очертават единен модел на „приватизация на войната“. В Африка държавата поема пряк контрол върху наследени военни мрежи, в Украйна възлага технически услуги и производство, в Газа частна фирма охранява пунктове за помощи (Arieff et al. 2026; Magid & Ayyub 2026). Дейностите нямат еднакъв правен статут или последици. Съпоставката им поставя въпроса кой определя задачите, контролира действията и проверява резултатите, без да предполага морална равнозначност.

За отбранителното планиране това налага ясно разграничаване на възложените задачи от правомощията за употреба на сила. Проверката следва да обхваща изпълнителите, подизпълнителите и достъпа до сведения за нарушения. При дроновете са важни резервните части, ремонтът, софтуерните обновления и възможността за смяна на доставчика[7,8] (Young 2024; Niederkofler 2025). Предложенията засягат оценката на зависимостите, а не установена празнота в българското законодателство.

V. Заключение

Частното участие в конфликтите не може да се оцени само по собствеността на организацията. Руското преструктуриране и украинските поръчки показват съответно държавно командване над военни мрежи и възлагане на производство на множество фирми[9] (Arieff et al. 2026). Производителят на дрон не става автоматично частна военна компания – определяща е предоставяната услуга[10]. В същото време недостигът на компоненти налага да се отчита устойчивостта на доставките (Kahn et al. 2026; Niederkofler 2025).

Водещият практически въпрос е дали държавата може да определя задачите, да проверява изпълнението и при необходимост да замени доставчика, без да прекъсне критични функции. Този извод се отнася до разгледаните случаи, публичните данни не позволяват количествено обобщение за целия сектор.

БЕЛЕЖКИ

1. ICRC, 2008. *Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security*

Companies during Armed Conflict. Available from: https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/montreux-document-eng.pdf [viewed: 11.09.2026].

2. HUMAN RIGHTS WATCH, 2026. Mali: Russia's 'Africa Corps' Massacres Villagers. 20 August. Available from: https://www.hrw.org/news/2026/08/20/mali-russias-africa-corps-massacres-villagers [viewed: 15.09.2026].

3. DSCA, 2025. Ukraine – Patriot Air Defense System Sustainment. Transmittal 25-69, 29 August. Available from: https://www.dsca.mil/Press-Media/Major-Arms-Sales/Article-Display/Article/4290514/ukraine-patriot-air-defense-system-sustainment [viewed: 24.09.2026].

4. MINISTRY OF DEFENCE OF UKRAINE, 2025a. In 2024 – 2025, the MoD allocated UAH 104.2 billion to Ukrainian drone manufacturers. 16 April. Available from: https://mod.gov.ua/en/news/glib-kanievskyi-in-2024-2025-the-ministry-of-defence-allocated-uah-104-2-billion-to-ukrainian-drone-manufacturers [viewed: 14.09.2026].

5. MINISTRY OF DEFENCE OF UKRAINE, 2025b. To date, the MoD's DPA has onboarded 11 drone manufacturers to the DOT-Chain Defence weapons marketplace. 31 July. Available from: https://mod.gov.ua/en/news/to-date-the-mo-d-s-dpa-has-onboarded-11-drone-manufacturers-to-the-dot-chain-defence-weapons-marketplace [viewed: 17.09.2026].

6. MINISTRY OF DEFENCE OF UKRAINE, 2025c. The DOT-Chain Defence drone catalog: UAVs from 20 manufacturers are now available to the military. 22 August. Available from: https://mod.gov.ua/en/news/the-dot-chain-defence-drone-catalog-uavs-from-20-manufacturers-are-now-available-to-the-military [viewed: 16.09.2026].

7. Ministry of Defence of Ukraine 2025a...

8. ICRC 2008...

9. Ministry of Defence of Ukraine 2025a...

10. ICRC 2008...

REFERENCES

ARIEFF, A.; BLANCHARD, C.M.; BLANCHARD, L.P. & BOWEN, A.S., 2026. Russia's Security Operations in Africa. In: *Focus IF12389. Congressional Research Service*. [Updated 8 April]. Available from: https://www.congress.gov/crs-product/IF12389 [viewed: 15.09.2026].

AVANT, D.D., 2005. *The Market for Force: The Consequences of Privatizing Security*. Cambridge: Cambridge University Press. Available from: https://doi.org/10.1017/CBO9780511490866.

DROKALOS, S.F., 2026. Innovation state at war? Ukraine's state-orchestrated, market-executed drone industry. *Journal of Strategic Studies*, published online 28 July. Available from: https://doi.org/10.1080/01402390.2026.2698656.

KAHN, M.; MUKHERJEE, S. & BALMFORTH, T., 2026. Ukraine's attack drone fleet faces a mini jet engine supply crunch. *Reuters.* [7 April]. Available from: https://www.reuters.com/business/aerospace-defense/ukraines-attack-drone-fleet-faces-mini-jet-engine-supply-crunch-2026-04-07/ [viewed: 03.09.2026].

LARSEN, K. P., 2025. The Wagner Group and its relationship with the Russian state. *International Affairs*, vol. 101, no. 2, pp. 643 – 663. Available from: https://doi.org/10.1093/ia/iiae324.

MAGID, P. & AYYUB, R., 2026. Exclusive: US firm in Gaza aid program, criticized by UN, in talks for new role. *Reuters.* [11 February]. Available from: https://www.reuters.com/world/middle-east/us-firm-gaza-aid-program-criticized-by-un-talks-new-role-2026-02-12/ [last viewed: 15.09.2026].

NIEDERKOFLER, M., 2025. Drones Win Battles, Components Win Wars. *Royal United Services Institute.* [17 December]. Available from: https://www.rusi.org/explore-our-research/publications/commentary/drones-win-battles-components-win-wars [viewed: 22.09.2026].

YOUNG, S., 2024. UK firm supports Ukrainian armed forces in drone tech race. *Reuters.* [28 March]. Available from: https://www.reuters.com/business/aerospace-defense/uk-firm-supports-ukrainian-armed-forces-drone-tech-race-2024-03-27/ [viewed: 26.09.2026].

THE PRIVATIZATION OF WAR: PRIVATE MILITARY COMPANIES AS A FACTOR FOR DEFENSE AND SECURITY IN A CHANGING WORLD

Abstract. This article examines how different forms of private participation affect defence capabilities, state control and public accountability in contemporary conflicts. It compares three purposively selected groups of cases: the restructuring of Russian military networks in Africa; proposed Patriot sustainment and drone supply for Ukraine; and private security at aid-distribution sites in Gaza. The analysis draws on selected research and public documents. Ukrainian procurement data indicate an increase in the number of manufacturers on a specific platform but do not establish the total number of private firms. The cases illustrate different forms of state coordination and distinct risks for accountability and supply resilience. Contractor assessment should therefore consider assigned functions, actual control, avenues for investigation and dependence on critical components.

Keywords: private military and security companies; drone manufacturers; Ukraine; state control; public accountability

Zapryan Valkov
ORCID iD: 0009-0006-4313-9506
University of National and World Economy
19, December 8th St.
Sofia, Bulgaria
E-mail: zapryan.valkov@unwe.bg

https://doi.org/10. 66334/annu26_satsuma

FROM SATSUMA SAMURAI TO MEIJI JAPAN: A SCIENTIFIC INVESTIGATION OF THE PARTICIPATION AND CONTRIBUTIONS OF SEIGO YAMAZAWA IN THE LIBERATION OF BULGARIA

In commemoration of the 180th anniversary of the birth of the samurai Seigo Yamazawa and on the eve of the 150th anniversary of the Pleven Epic of 1877

Dr. Ivan Botev[1], Dr. Atanas Vladikov, Assoc. Prof.[2]
[1]Toita Women's College – Tokyo (Japan)
[2]University of Plovdiv – Plovdiv (Bulgaria)

Abstract. This paper presents results from the authors' completed monographic investigation of the Japanese samurai and officer Seigo Yamazawa (1846 – 1897) and his participation in the Russo-Turkish War of 1877 – 1878. Based on Japanese archival records, Bulgarian and Russian historical sources, and field and documentary research in Japan and Bulgaria, the study traces Yamazawa's trajectory from Satsuma to the emerging Meiji state and subsequently to the European theatre of war. Methodologically, it distinguishes documented facts from probable historical

reconstructions and interpretative hypotheses. The results identify Yamazawa as a distinctive historical link between two nineteenth-century transformations: Japan's transition from the samurai order to the Meiji state and Bulgaria's Liberation and restoration of statehood. His biography provides new perspectives on early Bulgarian-Japanese historical contacts and Japanese observation of European warfare.

Keywords: Seigo Yamazawa; Satsuma; Sanpogiri; Meiji Japan; Russo-Turkish War; Liberation of Bulgaria

I. Introduction

The second half of the nineteenth century was an era of profound political and institutional transformation in Japan and Southeastern Europe. In Japan, the Boshin War of 1868 – 1869 and the Meiji Restoration marked the transition from the Tokugawa domain-based order towards a centralized state under the emperor. Across the Pacific, the American Civil War (1861–1865) had similarly demonstrated the profound political and institutional transformations reshaping states during this period. In the Balkans, the Russo-Turkish War of 1877 – 1878 became the decisive international conflict associated with the Liberation of Bulgaria and the restoration of Bulgarian statehood.

The life of Seigo Yamazawa (1846 – 1897) provides an unusual human intersection between these transformations. Born into the samurai environment of Satsuma, he experienced Japan's transition to the Meiji state. Within less than a decade of the Restoration, his career brought him from Kagoshima to Europe and eventually to the Balkan theatre of war.

This paper presents selected results from the authors' completed monographic investigation (Vladikov & Botev 2026). It examines three interconnected dimensions: Yamazawa's origins in Satsuma and transition from samurai to officer of the new Japanese state; his mission to Europe and attachment to the Russian Imperial Army; and the documentary evidence concerning his presence in the military theatre associated with the Liberation of Bulgaria.

The research applies critical source examination and comparative verification. Japanese archival records are cross-referenced with Bulgarian, Russian and other historical sources. The methodological principle is a strict distinction between documented facts, probable historical reconstructions and interpretative hypotheses. The objective is not to reproduce a heroic narrative, but to establish what the available evidence permits us to conclude.

II. From Sanpogiri and satsuma to the Meiji state

Seigo Yamazawa was born in 1846 into a samurai family in Satsuma, present-day Kagoshima Prefecture. His formative years belonged to the political and social world immediately preceding the Meiji Restoration.

Under the Shimadzu, Satsuma became one of the principal political forces involved in the events leading to the restoration of imperial rule. The transformation profoundly altered the position of the samurai class and required individuals originating within the old domain system to assume new institutional roles.

Yamazawa's biography illustrates this transition. His professional development took place within the structures of the new state, and by 1874 he held the rank of lieutenant colonel. His identity was consequently multidimensional: a Satsuma samurai, an officer of the new Imperial Japanese Army, and later a Japanese military observer attached to the Russian Imperial Army in Europe. His career therefore embodied Japan's institutional transformation.

The internationally familiar image of Satsuma is frequently associated with Saigō Takamori and the final generation of samurai. Popular culture later amplified this association through "The Last Samurai." Such representations are not historical evidence, but provide a recognizable cultural contrast. Yamazawa represents another trajectory from the same Satsuma environment: service within the institutions of Meiji Japan that eventually carried him to Europe. In this analytical sense, the familiar "Last Samurai" and the less familiar "First Samurai" frame two different trajectories from the transformation of Satsuma.

III. From Japan to Europe and the Russian imperial army

The Meiji state created a strong institutional demand for knowledge of foreign political, technological and military practices. Japanese officials and military personnel were dispatched abroad to observe foreign institutions. Yamazawa's European mission should be understood within this environment of institutional learning.

Japanese archival documentation provides a firm basis for reconstructing his mission. A telegram from Paris dated 27 April 1877 concerns his possible attachment to the Russian Imperial Army. An official decision of 17 May 1877, preserved as JACAR Ref. A24010804400, documents his dispatch as a military observer. JACAR Ref. C04026974600 documents his arrival at Russian headquarters on 30 June 1877.[1]

The latter source records that Yamazawa and other Japanese representatives arrived at the headquarters of the Russian Imperial Army and were received by Commander-in-Chief Grand Duke Nicholas Nikolaevich.[2]

Terminological precision is important. Yamazawa has sometimes been described as a Japanese “military attaché” in St Petersburg. The archival evidence examined here supports the more cautious designation **military observer attached to the Russian Imperial Army**. Diplomatic accreditation and military observation should not be conflated.

His presence within the Russian military environment is therefore documented. The central historical problem concerns the nature and geographical extent of his subsequent activity.

IV. Yamazawa in the military theatre of the liberation of Bulgaria: evidence and reconstruction

Three evidentiary levels must be distinguished.

4.1. Documented evidence

Japanese documentation establishes Yamazawa’s official dispatch and arrival at Russian headquarters. The research further identifies him, with the rank of lieutenant colonel of infantry, as assigned to the IX Army Corps, commanded by Lieutenant General Baron Nikolai Kridener, commander of the Russian Western Detachment.

This affiliation is operationally significant. IX Corps participated directly in the capture of Nikopol and the initial operations of the Siege of Pleven. Russian documentation used in the completed monographic study provides additional evidence. Order No. 147, reproduced in the *Collection of Materials on the Russo-Turkish War of 1877 – 1878 in the Balkan Peninsula*, contributes to reconstruction of this military context, while A. A. Stachevsky mentions Yamazawa as a military observer (Stachevsky 1878, p. 448).

Japanese archival documentation extends beyond his arrival. A field record dated 22 September 1877 concerns Yamazawa’s conduct in a combat environment, although its surviving text permits only partial reconstruction. Documents from December 1877 and January 1878 concern permission for him to wear the Russian Order of St Vladimir, 4th Degree with Swords, while a record dated 16 May 1878 formally recognizes his merits. The documentary sequence continues through 1879 and 1880 with records relating to Russian and Romanian distinctions.[3]

Material evidence provides another documented point. A historical photograph preserved by the Regional Military History Museum – Pleven depicts Yamazawa among members of the Russian imperial military headquarters and other foreign military representatives at San Stefano on 19 February 1878 (Old Style), corresponding to 3 March 1878 (New Style).[4] It establishes an important

geographical endpoint: Yamazawa remained associated with the Russian military environment through the concluding phase of the war.

4.2. Contextual reconstruction

The second evidentiary level concerns conclusions that are historically plausible but cannot presently be treated as directly documented facts.

Yamazawa's association with IX Corps places him institutionally within a formation involved in operations around Nikopol and Pleven. It does not, by itself, prove his personal presence in every battle fought by units of that corps.

This distinction is particularly important for Pleven and Gorni Dubnik. The campaign around Pleven became a prolonged struggle in which communications and supply routes acquired exceptional operational importance. Japanese archival documentation indicates that Yamazawa's observational responsibilities included attention to military communications. The battle of Gorni Dubnik in October 1877 therefore provides relevant operational context for reconstructing his possible movements.

Nevertheless, unless a source directly places Yamazawa at a particular engagement, his personal presence there must remain a **probable historical reconstruction rather than an established documentary fact**.

The testimony of American military observer Francis Vinton Greene provides a useful methodological comparison. Sent by the United States War Department to observe Russian operations, Greene subsequently published *The Russian Army and Its Campaigns in Turkey in 1877 – 1878* (Greene 1879). He explicitly identified battles that he personally witnessed, including Shipka, Plevna and Philippopolis. His account demonstrates that the movements of a military formation to which an observer was attached cannot automatically be equated with that observer's personal presence at every engagement.

The same evidentiary standard must be applied to Yamazawa.

4.3. Limits of the evidence and of the present study

The popular formulation that Yamazawa simply "fought at Pleven" reduces a complex evidentiary problem to a categorical statement. The surviving sources support stronger conclusions concerning his official mission, attachment to the Russian military environment, proximity to operations, conduct in a combat environment, subsequent recognition and presence at San Stefano than concerning his personal participation in every battle traditionally associated with his biography.

This distinction does not reduce his historical significance. The documentary record reveals a former Satsuma samurai serving the Meiji state, deliberately

dispatched to observe a major European war and operating within the Russian military environment.

The investigation also has identifiable limitations. It was conducted independently and financed by the authors, with documentary and field research undertaken primarily in Japan and Bulgaria during 2025–2026. Its conclusions therefore reflect the archival and material corpus identified and examined during that period. Additional relevant archival units may exist in Kagoshima, Tokyo, Paris, St Petersburg and elsewhere.

A Japanese press report provides further evidence of how Yamazawa's experience entered public knowledge. Shiba notes that the *Yomiuri* of 3 December 1878 reported on Yamazawa's account to Emperor Meiji concerning his experience in the Russo-Turkish War (Shiba 2011, p. 7). Later Japanese sources also preserved accounts concerning recognition associated with his mission (Tsutsui 1911; Terajima 1982, pp. 138 – 144).

His historically defensible trajectory is already exceptional: **Sanpogiri – Satsuma – Meiji Japan – Europe – Russian Imperial Army – the Balkans – San Stefano – Japan.** It requires no embellishment.

V. Research results

The analysis produces five principal results.

First, Yamazawa cannot adequately be understood through the category of "samurai" alone. His biography embodies the transition between the samurai world of Satsuma and the institutions of the Meiji state.

Second, the Japanese archival corpus substantially strengthens the documentary foundation for his European mission. Its integration with Bulgarian, Russian and international sources allows the research to move beyond narratives based primarily on later commemoration.

Third, the sources establish Yamazawa's attachment to the Russian military environment and his presence in the operational theatre while demonstrating the necessity of distinguishing institutional affiliation from reconstructed presence at individual engagements.

Fourth, the San Stefano photograph provides independent material evidence confirming his continued presence within the Russian headquarters environment at the conclusion of the campaign.

Fifth, Yamazawa's biography reveals an unusual intersection between two nineteenth-century national transformations. Japan entered the 1870s after the collapse of the Tokugawa political order and establishment of the Meiji state.

Bulgaria entered the decade without independent statehood and emerged from the Russo-Turkish War on the path towards restored political institutions.

These transformations were fundamentally different and should not be artificially equated. Their historical intersection lies in Yamazawa himself. He originated in Satsuma, one of the principal domains associated with the transformation that produced Meiji Japan. Less than a decade after the Restoration, service to the new Japanese state brought him into a European conflict decisive for the restoration of Bulgarian statehood.

This was not yet a formal Bulgarian-Japanese political relationship. It represents an earlier individual and institutional contact produced by the international circulation of knowledge during an era of rapid state transformation.

One samurai thus becomes a historical point of contact between two nations in transformation.

VI. Conclusion

The reconstruction of Seigo Yamazawa's trajectory demonstrates the value of integrating Japanese archival documentation with Bulgarian, Russian and international historical sources.

The evidence establishes his dispatch as a military observer, arrival at Russian headquarters, integration into the Russian military environment, documentary recognition associated with the campaign, and presence at San Stefano. Claims concerning his personal participation in individual engagements, however, should not be converted from plausible reconstruction into documented fact without direct corroboration.

This distinction strengthens rather than diminishes his historical significance. Once later embellishments are separated from documentary evidence, an exceptional transnational biography remains: a Satsuma samurai who became an officer of Meiji Japan and whose official mission brought him into the events associated with the Liberation of Bulgaria.

In 2026, the 180th anniversary of Yamazawa's birth, and on the eve of the 150th anniversary of the Pleven Epic of 1877, his life offers an opportunity to reconsider this little-known intersection of Japanese and Bulgarian history.

One samurai. Two nations in transformation.

NOTES

1. Japan Center for Asian Historical Records (JACAR), National Archives of Japan, Ref. A24010804400, official decision of 17 May 1877 concerning the dispatch of Seigo Yamazawa as a military observer; JACAR Ref. C04026974600, documentation concerning his arrival at the headquarters of the Russian Imperial Army.

2. JACAR Ref. C04026974600 records Yamazawa and other Japanese representatives at Russian headquarters and their reception by Grand Duke Nicholas Nikolaevich.

3. Japanese archival documents examined in the completed monographic study concern Yamazawa's mission and subsequent recognition between 1877 and 1880, including records relating to the Order of St Vladimir and later distinctions.

4. Photograph of Seigo Yamazawa with the Russian imperial military headquarters at San Stefano, 19 February 1878 (Old Style) / 3 March 1878 (New Style). Regional Military History Museum – Pleven, Scientific-Exposition and Collections Department; supplied to the authors for the present research in December 2025.

REFERENCES

GREENE, F.V., 1879. *The Russian Army and Its Campaigns in Turkey in 1877 – 1878*. New York: D. Appleton and Company.

SHIBA, R., 2011. Images of the Balkans in the Japanese Media of the Meiji Period. *Godišnjak za društvenu istoriju*, XVIII, no. 3, p. 7.

STACHEVSKY, A. A., 1878. *Pamjatnik Vostochnoj vojny 1877 – 1878 gg.: opisyvajushhij po alfavitnomu porjadku biograficheskie ocherki vseh otlichivshihsja, ubityh, ranenyh i kontuzhennyh – generalov, shtabnyh i ober-oficerov, doktorov, sanitarov i miloserdnyh sestjor, a takzhe otlichivshegosja rjadovogo sostava*. St Petersburg. [in Russian].

TERAJIMA, K., 1982. History and Present State of the Japanese-Bulgarian Cultural Exchange. In: *Proceedings of the International Symposium Fundamental Studies on Cultural Exchange between Japan and Eastern Europe*, pp. 138 – 144. Tokyo: Association for the Study of Relations between Japan and Eastern Europe.

TSUTSUI, J., 1911. *Encyclopedia of Japanese Nobility.*

VLADIKOV, A. & BOTEV, I., 2026. *Parviyat samuray. Monografichno izsledvane na uchastieto na Seygo Yamadzava ot Kagoshima v Osvobozhdenieto na Bulgaria*. Plovdiv: NITON MEDIA. ISBN 978-954-347-153-9. [in Bulgarian].

Dr. Ivan Botev
ORCID iD: 0009-0007-8757-5059
Department of International Communication and Culture
Toita Women's College
2-21-17 Shiba, Minato-ku
Tokyo 105-0014, Japan
E-mail: botev@toita.ac.jp

Dr. Atanas Vladikov, Assoc. Prof.
ORCID iD: 0000-0001-9489-3775
Faculty of Economic and Social Sciences
University of Plovdiv "Paisii Hilendarski"
24, Tsar Asen St.
Plovdiv, Bulgaria
E-mail: avladikov@uni-plovdiv.bg

https://doi.org/10. 66334/annu26_altuprmilitrisk

АЛТЕРНАТИВИ ЗА УПРАВЛЕНИЕ НА ВОЕННИЯ РИСК ЗА ТЪРГОВСКОТО КОРАБОПЛАВАНЕ В ЗОНИ НА КОНФЛИКТ

доц. д-р Иван Вълков
Висше военновъздушно училище „Георги Бенковски“

Абстракт. От ноември 2023 г. движението „Ансар Алах“ (хутите) напада търговски кораби в Червено море и протока Баб ел-Мандеб с ракети, безпилотни летателни апарати и безекипажни катери, а през юли 2026 г. обявява блокада на Саудитска Арабия. Преминаванията през Суецкия канал намаляват почти наполовина, а застрахователната премия за военен риск нараства многократно и в пиковете става съизмерима с разхода за обиколка около Африка. Военните командвания отчитат успеха на своите операции с броя на поразените цели и съпроводените кораби. Корабоплавателните компании решават дали корабите им да минават през Червено море, или да заобикалят Африка, според разходите за едно преминаване. Разработката изследва кои мерки за защита на корабоплаването променят това решение и в какъв срок. Осем алтернативи са класифицирани по вариантите за третиране на риска по ISO 31000 и оценени по шест критерия. Данните показват, че застрахователите повишават застрахователната премия в рамките на няколко дни след нападение, а я понижават едва след период от няколко месеца.

Ключови думи: военен риск; застрахователна премия за военен риск; защита на корабоплаването; морска комуникационна линия; Червено море; ISO 31000

I. Увод

От ноември 2023 г. йеменското движение „Ансар Аллах“, известно като хутите, води кампания срещу търговското корабоплаване в Червено море, протока Баб ел-Мандеб и Аденския залив.[1] Хутите нападат търговски кораби с противокорабни балистични и крилати ракети, безпилотни летателни апарати и безекипажни катери. По оценка на Knights само до април 2024 г. те са изстреляли около 135 балистични и 87 крилати ракети, 263 безпилотни летателни апарата и 38 безекипажни катера.[2] Нападенията затихват след края на септември 2025 г. На 20 юли 2026 г. хутите обявяват морска блокада на Саудитска Арабия, а два дни по-късно нападат саудитски танкери.[3]

За защита на корабоплаването срещу нападенията на хутите са разгърнати две морски операции. Многонационалната операция „Prosperity Guardian“ под ръководството на Съединените щати е обявена през декември 2023 г., а операцията на Европейския съюз „Aspides“ започва през февруари 2024 г. Съединените щати водят и ударните въздушни кампании „Poseidon Archer“ (от януари 2024 г.) и „Rough Rider“ (март – май 2025 г.) срещу ракетните пускови установки и други военни обекти на хутите в Йемен. В част от ударите участва и Обединеното кралство.[4]

Въздействието на кампанията на хутите върху корабоплаването може да се измери по различни показатели. По данни на UNCTAD в началото на 2024 г. броят на преминаванията през Суецкия канал е с 42% под най-високото месечно равнище.[5] Средният брой кораби, преминаващи за денонощие през Баб ел-Мандеб, намалява от 74 през 2023 г. до около 33 през всяка от следващите три години.[6] Стойностите са изчислени по сигналите от автоматичната идентификационна система на корабите (*Automatic Identification System – AIS*), а в настоящата разработка мярката за обема на трафика е броят на преминалите кораби за едно денонощие.

Военните командвания отчитат резултата от операциите си с броя на поразените цели, прехванатите ракети и съпроводените кораби. Корабоплавателните компании решават дали корабите им да минават през Червено море, или да заобикалят Африка, според разходите за едно преминаване. В тези разходи влиза и застрахователната премия за военен риск (*additional war risk premium*). Това е допълнителната сума, която корабособственикът плаща на застрахователя за всяко преминаване през район, обявен за ри-

сков, изразена като процент от застрахователната стойност на кораба.[7] Изследователският проблем, който статията разглежда, е несъответствието между двата начина за оценка на резултата.

В съюзната доктрина за планиране на операциите AJP-5 решаващото условие (*decisive condition*) е съвкупност от обстоятелства или ключово събитие, чието настъпване дава на командващия подчертано предимство.[8] В предходно изследване като решаващо условие за успеха на отговора срещу кампанията на хутите е определено възстановеното доверие на корабоплавателните компании и на застрахователите в безопасността на морската комуникационна линия (*sea line of communication – SLOC*) през Червено море (Valkov 2026). Там застрахователната премия, чрез която това доверие може да се измери, не беше изразена със стойности, а настоящият текст се стреми да преодолее това ограничение.

Темата е актуална, защото през 2026 г. корабоплаването е застрашено едновременно в Червено море и в Ормузкия проток. Изследователският интерес на автора е предизвикан от това, че съюзното планиране оценява подробно собствените си действия, но почти не измерва въздействието им върху корабоплавателните компании, застрахователите и екипажите.

Обект на изследването е защитата на търговското корабоплаване в Червено море и Баб ел-Мандеб от ноември 2023 г. до септември 2026 г.[9] Предмет на изследването са алтернативите за управление на военния риск и срокът, в който всяка от тях влияе върху решението на корабоплавателните компании да използват морския път.

Тезата на доклада е, че застрахователите преоценяват военния риск асиметрично. Те повишават застрахователната премия в рамките на няколко дни след ново нападение, а я понижават едва месеци след като получат убедителни сведения, че заплахата е отслабнала. Затова решението за маршрута на кораба зависи повече от вероятността застрахователната премия да се повиши отново, докато корабът е на път, отколкото от сегашния ѝ размер. Военната намеса променя това решение, когато намалява вероятността за ново повишение на застрахователната премия по начин, който застрахователите могат да проверят.

Възможните аналогии с войната в Украйна и със застраховането на въздухоплавателните средства срещу военен риск остават извън обхвата на разработката. Изследването е вторичен анализ на открити източници. Като установен факт се представя само твърдение, потвърдено от международна организация или от два независими източника, а останалите се привеждат с изрично позоваване на източника. Числата не се осредняват, а степента

на увереност се изразява по вероятностна скала.[10] Изчисленията без посочен източник са на автора.

II. Военният риск като измерима величина

2.1. Застраховане на военния риск

На лондонския застрахователен пазар за военния риск се прилагат клаузите за военни рискове и стачки на Института на лондонските застрахователи (*Institute War and Strikes Clauses*). Те дават и на застрахователя, и на застрахования корабособственик право да прекратят застраховката със седемдневно предизвестие.[11]

Районите с повишен военен риск (*Listed Areas*) се определят от Съвместния военен комитет (*Joint War Committee – JWC*), в който участват представители на застрахователите от пазара „Лойдс“ (*Lloyd's*) и от Международната асоциация на застрахователите (*International Underwriting Association – IUA*). Размерът на застрахователната премия не се определя от комитета, а се договаря за всяко преминаване между застрахователя и брокера на корабособственика.[12]

Според анализ на специализирания уебсайт *Straits* морски район се включва в списъка на *JWC* след нападение, след достоверна заплаха или при общо влошаване на обстановката, а се изключва от него едва когато обстановката остане стабилна за продължителен период.[13] В тази разлика между условията за включване и за изключване се крие един от източниците на асиметрията, която се разглежда в точка III. Предложената от застрахователя цена (*quotation*) е валидна за кратък срок, а през януари 2024 г. той е съкратен до 24 часа.[14]

2.2. Участниците в решението за маршрута

В решението дали корабът да мине през протока участват четири страни. Застрахователят определя цената и условията за преминаване, екипажът може да откаже плаването, корабоплавателната компания определя маршрута, а военните командвания определят как да бъдат защитени корабите.

Правото на екипажа да откаже плаване произтича от колективните трудови договори на моряците. Те се договарят в Международния форум за колективно договаряне (*International Bargaining Forum – IBF*) между работодателите и синдикатите на моряците. На 22 декември 2023 г. форумът обявява южното Червено море за зона с висок риск (*High Risk Area*).[15] На

12 март 2024 г., след ракетното попадение в кораба „True Confidence“, при което загиват трима моряци, зоната е обявена за зона на бойни действия (*Warlike Operations Area*) и е разширена до Аденския залив.[16] Към март 2026 г. тази класификация е в сила.[17] В двете категории зони морякът има право да откаже плаването, да бъде репатриран за сметка на работодателя и да получи обезщетение в размер на две основни месечни заплати.[18]

III. Асиметрията на преоценката

Стойностите на застрахователната премия за Червено море са обобщени в таблица 1. Повечето са от един източник, а от два независими са потвърдени пикът през януари 2024 г. и повишението през юли 2026 г.

Таблица 1. Застрахователна премия за военен риск при преминаване през Червено море*

Период	***% от стойността на кораба****	***Събитие***	***Източник***
Преди кризата	0,05 – 0,1	Мирновременно равнище	International Transport Forum 2024[19]
декември 2023	0,3 – 0,5	Удвояване за седмица след поредица нападения	Lloyd's List[20]
Трета седмица на януари 2024	0,7 – 1	Удари на САЩ и Обединеното кралство	Reuters[21]; Notteboom et al. 2024
март 2025	≈ 0,5	Нападенията са редки	S&P Global[22]
пролет – лято 2025	0,2 – 0,3	Затишие	Bloomberg[23]
юли 2025	≈ 1	Потопени „Magic Seas“ и „Eternity C“	Bloomberg[24]
Начало на декември 2025	≈ 0,2	Най-ниско от ноември 2023 г.	S&P Global[25]; Splash247[26]
17 – 21.07.2026	0,3 → 0,75	Обявена блокада на Саудитска Арабия	Reuters[27]
30.07.2026	1 – 2	Нападения; JWC разширява района	Reuters[28]

* Ориентировъчни цени за едно преминаване, съобщени от различни източници за различни кораби. Не се осредняват.

Застрахователната премия се повишава в рамките на няколко дни. След като хутите потопяват корабите „Magic Seas“ и „Eternity C“ в начало-

то на юли 2025 г., тя нараства за седмица от 0,2 – 0,3% до около 1%.[29] След обявяването на блокадата срещу Саудитска Арабия тя нараства два и половина пъти за два дни и надхвърля 1% три дни по-късно.[30]

Понижаването на застрахователната премия обаче продължава месеци. От пика през януари 2024 г. до около 0,5% през март 2025 г. минават над 13 месеца, през които тя не намалява съществено, макар нападенията да стават по-редки.[31] След повишението през юли 2025 г. тя достига около 0,2% едва в началото на декември – повече от два месеца след последното нападение от 29 септември 2025 г.[32]

Броят на преминаванията не се увеличава дори след понижаването на застрахователната премия. През декември 2025 г., когато тя е най-ниска от началото на кампанията, през Баб ел-Мандеб преминават средно 32,7 кораба за денонощие, или около 44 % от средния брой за 2023 г.[33]

За сравнение през юли 2026 г. застрахователната премия за Ормузкия проток, за който обходен морски път няма, е 7,5 – 10%.[34] Това е с порядък повече, отколкото в Червено море, където при застрахователна премия от 0,5 – 1% корабите предпочитат да заобиколят Африка.

IV. Алтернативи за управление на военния риск

4.1. Основа за класифициране на алтернативите

Алтернативите за управление на военния риск се класифицират по вариантите за третиране на риска (*risk treatment*) от международния стандарт ISO 31000:2018.[35] Избран е граждански стандарт, защото е разбираем и за военните планиращи органи, и за застрахователите и позволява да се отделят алтернативите, които може да приложи командващият операцията, от онези, които могат да приложат гражданските участници. Стандартът предвижда седем варианта, които могат да се съчетават.[36] Осемте алтернативи са означени с кодове от A0 до A7 и са оценени по шест критерия (Таблица 2).

Таблица 2. Алтернативи за управление на военния риск по шест критерия*

Код	***Алтернатива (кой я прилага)***	***Вариант по ISO 31000***	***K1***	***K2***	***K3***	***K4***	***K5***	***K6***
A0	Удари по пусковите установки и обектите на хутите (САЩ, Обединеното кралство)	Отстраняване на източника	↓	↓	↓	↓	→	→
A1	Съпровождане (ескорт) от бойни кораби (ЕС, САЩ)	Промяна на вероятността	→	→	↓	→	→	→

Код	*Алтернатива (кой я прилага)*	*Вариант по ISO 31000*	*К1*	*К2*	*К3*	*К4*	*К5*	*К6*
А2	Обиколка около нос Добра надежда (корабоплавателна компания)	Избягване	↑	↓	↑	↑	↑	↑
А3	Държавно застраховане на военния риск (държава)	Споделяне	↑	→	→	↑	↑	↓
А4	Смяна на флага или собствеността (корабособственик)	Промяна на вероятността	↑	↑	↓	→	↓	↓
А5	Договорено изключение от нападенията (държава и хутите)	Промяна на вероятността	↑	↑	↓	↑	↓	↓
А6	Информационно осигуряване (военни командвания и граждански участници)	Промяна на вероятността	→	↑	↑	↑	→	↑
А7	Преминаване срещу допълнителна застрахователна премия (корабоплавателна компания)	Задържане; поемане с цел възможност	↑	→	→	↑	↓	→

* К1 – време до въздействие върху застрахователната премия и трафика; К2 – разходи и кой ги поема; К3 – възможност за разширяване и устойчивост; К4 – риск от ескалация; К5 – зависимост от волята на противника; К6 – правни и съюзни ограничения. ↑ – благоприятно, → – умерено, ↓ – неблагоприятно. Оценки на автора.

4.2. Оценка на алтернативите

Ударите по ракетните пускови установки и военните обекти на хутите (А0) не понижават застрахователната премия в краткосрочен план. Седмица след първите удари на Съединените щати и Обединеното кралство на 12 януари 2024 г. тя нараства от около 0,7% до около 1%.[37] Вероятната причина е, че непосредствено след удара застрахователят оценява вероятността за следващо нападение като по-висока, защото противникът може да отвърне, без да е загубил способността си да напада. Според Paes et al. честотата на нападенията остава почти непроменена до август 2024 г. въпреки ударите (Paes, Beales, Hinz, Vidal 2024).

Обявяването на операция за съпровождане от бойни кораби (А1) е единственото военно действие, след което е отчетено бързо, макар и частично понижение на застрахователната премия. Скоро след обявяването на „Prosperity Guardian“ през декември 2023 г. тя спада до 0,3 – 0,35%.[38] Възможностите му обаче са ограничени от броя на бойните кораби. По оценка на Leccese операцията „Aspides“ разполага средно с три бойни кораба при необходими поне десет.[39]

Обиколката около нос Добра надежда (А2) удължава рейса между Азия и Северна Европа с 10 – 12 дни в една посока (Notteboom et al. 2024).[40] По модела на Международния транспортен форум към ОИСР[41] допълнителният разход за рейс в двете посоки на контейнеровоз с вместимост 12 500 TEU е около 1,7 млн. USD при цените от 2024 г.[42] Обиколката премахва риска веднага, но разходите ѝ се плащат през цялото време на кризата.

Държавното застраховане на военния риск (А3) не е прилагано в разглеждания район. Програмата на Съединените щати по дял XII от Закона за търговския флот (*Merchant Marine Act*) се задейства автоматично само при война с друга велика сила, а за отделен кораб – само когато търговска застраховка не се предлага при разумни условия.[43] В Червено море търговският пазар продължава да предлага застраховка, макар и скъпа.

Договореното изключение (А5) действа от деня на обявяването си, но само за корабите, които противникът изключи от целите си. Примирието между Съединените щати и хутите от май 2025 г. изключва от нападенията американските военни кораби и корабите под флага на Съединените щати.[44] Изборът кой кораб да премине остава в ръцете на противника, а промяната на флага или собствеността на кораба (А4) следва същата логика.

Информационното осигуряване на корабоплаването (А6) е единствената алтернатива, за която намаляването на застрахователната премия е изрично посочено като очакван резултат. НАТО го включва сред ползите от военноморското сътрудничество и насоките за корабоплаването (*Naval Cooperation and Guidance for Shipping – NCAGS*).[45] В района на конфликта Съвместният морски информационен център (*Joint Maritime Information Centre – JMIC*) в Бахрейн съобщава за всяко нападение до 24 часа след него.[46] Тъй като застрахователят оценява вероятността за следващо нападение по наличните сведения, може да се очаква, че чрез навременни и проверими сведения военните командвания могат да ускорят понижаването на застрахователната премия.

4.3. Проверка чрез анализ на конкуриращи хипотези

Тезата е проверена по логиката на анализа на конкуриращи хипотези (*Analysis of Competing Hypotheses – ACH*), разработен от Heuer за разузнавателния анализ (Heuer 1999). Методът изисква всяко наблюдение да се съпостави не само с тезата, но и с другите правдоподобни обяснения в най-силния им вид, като се търсят преди всичко опровергаващите данни. Методът се прилага в опростен вид, с три конкуриращи хипотези.

Според първата хипотеза, която поставя тезата под най-сериозно съмнение, застрахователната премия е само следствие от обстановката. Корабоплавателната компания избира маршрута по пълната цена на превоза, по договорите си и по разписанието, а застрахователната премия е само едно от разходните пера. По модела на Международния транспортен форум обиколката струва около 1,7 млн. USD за рейс в двете посоки, а при застрахователна премия от 1% едно преминаване струва до около 1 млн. USD.[47] Ако рейсът в двете посоки включва две преминавания през протока, разходът за обиколката се отнася към разхода за застрахователна премия като 0,85 – 1,7 към 1. При застрахователна премия от 0,2% обиколката е 4 – 8,5 пъти по-скъпа.[48]

Следователно хипотезата важи само за част от периода. При около 1% двата разхода са от един порядък. При 0,2% преминаването през протока е многократно по-евтино, но корабите не се връщат и размерът на застрахователната премия не обяснява решенията на компаниите.

Двете наблюдения се съгласуват, ако решаващата величина е вероятността застрахователната премия да се повиши отново. Рейсът между Азия и Европа през Суецкия канал продължава около месец в една посока.[49] През това време застраховката може да бъде прекратена със седемдневно предизвестие, а застрахователната премия може да се утрои в рамките на няколко дни. Компания, която върне редовната си линия през Суецкия канал, рискува това да се случи, докато корабите ѝ са на път. Според *BIMCO* компаниите *CMA CGM* и *Maersk* посочват условията за сигурност като основание за решенията си дали да се върнат през Суецкия канал.[50] Затова предпазливостта на компаниите е обяснима реакция на асиметричната преоценка, а не отделна причина. Първата хипотеза се приема частично, а тезата се уточнява.

Според втората хипотеза решаващо е правото на екипажа да откаже плаване. При повишаването на риска застрахователите реагират по-бързо. Застрахователната премия се удвоява за седмица през декември 2023 г.,[51] а *IBF* обявява зоната с висок риск повече от месец след първото нападение. При понижаването екипажите реагират по-бавно, защото класификацията като зона на бойни действия е в сила и през март 2026 г., три месеца след най-ниската застрахователна премия.[52] Тази хипотеза се приема като допълнение към тезата.

Според третата хипотеза военните командвания не влияят на застрахователния пазар, а застрахователната премия само изостава от действителната безопасност. Тезата не отрича това, но твърди, че без проверими

за застрахователя сведения изоставането се удължава. Подкрепата за това е частична и се оценява като реалистична възможност, а асиметрията като цяло – като вероятна, защото е наблюдавана при три повишения и две понижения.

V. Заключение

Изводите от изследването и условията, при които са валидни, са следните:

– Военната намеса понижава застрахователната премия за военен риск, когато създава проверими за застрахователя сведения за отсъствието на заплаха и ги поддържа по-дълго, отколкото трае рейсът.

– Ударите по ракетните пускови установки и военните обекти на противника повишават застрахователната премия в краткосрочен план. Те я понижават едва когато правят ново нападение малко вероятно.

– Съпровождането и информационното осигуряване са алтернативите, които военните командвания могат да приложат, за да намалят вероятността за ново повишение на застрахователната премия.

В резултат на анализите в доклада се предлага ефективността на военните операции за защита на корабоплаването, както на морските операции, така и на ударните въздушни кампании, да се оценява и с показатели от застрахователния пазар. Такива са размерът на застрахователната премия, границите на обявения от *JWC* рисков район, срокът на валидност на предложената цена и времето от последното нападение до понижаването на застрахователната премия под определен праг.

Научният принос на доклада е в измеримия израз на решаващото условие чрез скоростта на преоценка на военния риск. Научноприложният принос е класифицирането на алтернативите по ISO 31000 според това кой ги прилага, а приложният – предложените показатели за ефективност.

БЕЛЕЖКИ

1. Названието идва от рода на основателя на движението Хюсеин Бадреддин ал-Хути (Hussein Badreddin al-Houthi), убит през 2004 г. От 2014 г. движението владее столицата Сана без международно признание.

2. KNIGHTS, M., 2024. Assessing the Houthi War Effort Since October 2023. *CTC Sentinel* [online] [last viewed 24.09.2026]. Available from: https://ctc.westpoint.edu/assessing-the-houthi-war-effort-since-october-2023

3. Human Rights Watch, 2026. Yemen: New Attacks by Houthi Include Likely War Crimes. *Human Rights Watch* [online] [last viewed 19.09.2026]. Available from:

https://www.hrw.org/news/2026/09/15/yemen-new-attacks-by-houthi-include-likely-war-crimes

4. House of Commons Library, 2025. UK and International Response to Houthis in the Red Sea 2024/25. Research Briefing CBP-9930. *House of Commons Library* [online] [last viewed 18.09.2026]. Available from: https://commonslibrary.parliament.uk/research-briefings/cbp-9930

5. UNCTAD, 2024a. Navigating Troubled Waters: Impact to Global Trade of Disruption of Shipping Routes in the Red Sea, Black Sea and Panama Canal. *UNCTAD* [online] [last viewed 18.09.2026]. Available from: https://unctad.org/system/files/official-document/osginf2024d2_en.pdf

6. IMF Portwatch, 2026. Chokepoint transit calls. *IMF Portwatch* [online] [last viewed 24.09.2026]. Available from: https://portwatch.imf.org

7. Военен риск (на англ. *war risk*) е рискът от загуба или повреда на кораба вследствие на военни и враждебни действия. По-нататък под „застрахователна премия“ се разбира застрахователната премия за военен риск за едно преминаване.

8. NATO, 2026. AJP-5 Allied Joint Doctrine for the Planning of Operations. Edition B, version 1. *NATO Standardization Office* [online] [last viewed 19.09.2026], т. 2.47. Available from: https://assets.publishing.service.gov.uk/media/6a35198c25c5199bda11783a/AJP_5_EdB_NATO.pdf

9. Обстановката е разгледана към 20 септември 2026 г. Това е последната дата с данни за трафика през протока.

10. Използвана е британската скала *PHIA (Probability Yardstick)*, в която „реалистична възможност“ е 40 – 50%, а „вероятно“ – 55 – 75%.

12. Institute of London Underwriters, 1983. Institute War and Strikes Clauses Hulls – Time (1/10/83). *Hiller Marine* [online] [last viewed 18.09.2026], кл. 5. Available from: https://abhillermarine.com/documents/clauses/INSTITUTE%20WAR%20AND%20STRIKES%20CLAUSES%20TIME.pdf

13. LMA, 2026. Joint War Committee. *LMA* [online] [last viewed 28.09.2026]. Available from: https://lmalloyds.com/committee/joint-war-committee

14. Straits, б. г. What the Joint War Committee actually does. *STRAITS* [online] [last viewed 28.09.2026]. Available from: https://straits.live/blog/what-the-jwc-actually-does

15. Reuters, 2024. Red Sea war insurance rises with more ships in firing line. *Business Insurance* [online] [last viewed 28.09.2026]. Available from: https://www.businessinsurance.com/red-sea-war-insurance-rises-with-more-ships-in-firing-line

16. IMEC, 2023. IBF to establish a High-Risk Area in the Red Sea. *IMEC* [online] [last viewed 28.09.2026]. Available from: https://imec.org.uk/post/ibf-to-establish-a-high-risk-area-in-the-red-sea

17. Seatrade Maritime, 2024. IBF designates Red Sea and Gulf of Aden ‘warlike’. *Seatrade Maritime* [online] [last viewed 28.09.2026] Available from: https://www.seatrade-maritime.com/ship-operations/ibf-designates-red-sea-and-gulf-of-aden-warlike-

18. ITF Seafarers, 2026. IBF List of designated risk Areas with applicable benefits (as of 26 March 2026). *ITF Seafarers* [online] [last viewed 28.09.2026]. Available from:

https://www.itfseafarers.org/sites/default/files/node/resources/files/IBF%20List%20of%20designated%20risk%20Areas%20with%20applicable%20benefits%20(as%20of%2026%20March%202026).pdf

19. ITF Seafarers, б. г. ITF warlike and high risk areas. *ITF Seafarers* [online] [last viewed 28.09.2026]. Available from: https://www.itfseafarers.org/en/resources/itf-warlike-and-high-risk-areas

20. International Transport Forum, 2024. The Red Sea Crisis: Impacts on Global Shipping and the Case for International Co-operation. *OECD Publishing* [online] [last viewed 28.09.2026]. Available from: https://www.itf-oecd.org/sites/default/files/repositories/red-sea-crisis-impacts-global-shipping.pdf

21. Lloyd's List, 2023. Red Sea war risk rates still rising after doubling in past week. *Lloyd's List* [online] [last viewed 28.09.2026]. Available from: https://www.lloydslist.com/LL1147660/Red-Sea-war-risk-rates-still-rising-after-doubling-in-past-week

22. Reuters, 2024. Red Sea war insurance rises with more ships in firing line. *Business Insurance* [online] [last viewed 28.09.2026]. Available from: https://www.businessinsurance.com/red-sea-war-insurance-rises-with-more-ships-in-firing-line

23. S&P Global Commodity Insights, 2025. Oil importers stare at costly tanker insurance despite fall in Red Sea attacks. *S&P Global Commodity Insights* [online] [last viewed 28.09.2026]. Available from: https://spglobal.com/commodity-insights/en/news-research/latest-news/shipping/031225-oil-importers-stare-at-costly-tanker-insurance-despite-fall-in-red-sea-attacks

24. Bloomberg, 2025. Red Sea Insurance Premium Spikes as Houthi Risks Return. *Bloomberg* [online] [last viewed 28.09.2026]. Available from: https://www.bloomberg.com/news/articles/2025-07-11/red-sea-insurance-premium-spikes-as-houthi-risks-return

25. Bloomberg, 2025. Red Sea Insurance Premium Spikes as Houthi Risks Return. *Bloomberg* [online] [last viewed 28.09.2026]. Available from: https://www.bloomberg.com/news/articles/2025-07-11/red-sea-insurance-premium-spikes-as-houthi-risks-return

26. S&P Global Commodity Insights, 2025. Maritime war risk premiums fall in Red Sea, rise in Black Sea amid changing security dynamics. *S&P Global Commodity Insights* [online] [last viewed 28.09.2026]. Available from: https://www.spglobal.com/energy/en/news-research/latest-news/shipping/120425-maritime-war-risk-premiums-fall-in-red-sea-rise-in-black-sea-amid-changing-security-dynamics

27. AJDIN, A., 2026. Suez traffic still 60% down 100 days after last Houthi attack. *Splash247* [online] [last viewed 24.09.2026]. Available from: https://splash247.com/suez-traffic-still-60-down-100-days-after-last-houthi-attack

28. SAUL, J., 2026. Red Sea War Insurance Costs Rise After Houthi Blockade, Sources Say. *Insurance Journal (Reuters)* [online] [last viewed 24.09.2026]. Available from: https://www.insurancejournal.com/news/international/2026/07/21/878345.htm;

29. SAUL, J., 2026. Houthis' Red Sea Attacks Prompt London Insurers to Widen High-Risk Zone. *Insurance Journal (Reuters)* [online] [last viewed 24.09.2026]. Available from: https://www.insurancejournal.com/news/international/2026/07/30/879653.htm

30. Bloomberg, 2025. Red Sea Insurance Premium Spikes as Houthi Risks Return. *Bloomberg* [online] [last viewed 28.09.2026]. Available from: https://www.bloomberg.com/news/articles/2025-07-11/red-sea-insurance-premium-spikes-as-houthi-risks-return

31. SAUL, J., 2026. Red Sea War Insurance Costs Rise After Houthi Blockade, Sources Say. *Insurance Journal (Reuters)* [online] [last viewed 24.09.2026]. Available from: https://www.insurancejournal.com/news/international/2026/07/21/878345.htm; SAUL, J., 2026. War Risk Insurance Costs Surge for Southern Red Sea Voyages After Houthi Attacks. *Insurance Journal (Reuters)* [online] [last viewed 24.09.2026]. Available from: https://www.insurancejournal.com/news/international/2026/07/23/878788.htm

32. S&P Global Commodity Insights, 2025a. Oil importers stare at costly tanker insurance despite fall in Red Sea attacks. *S&P Global Commodity Insights* [online] [last viewed 28.09.2026]. Available from: https://spglobal.com/commodity-insights/en/news-research/latest-news/shipping/031225-oil-importers-stare-at-costly-tanker-insurance-despite-fall-in-red-sea-attacks

33. S&P Global Commodity Insights, 2025b. Maritime war risk premiums fall in Red Sea, rise in Black Sea amid changing security dynamics. *S&P Global Commodity Insights* [online] [last viewed 28.09.2026]. Available from: https://www.spglobal.com/energy/en/news-research/latest-news/shipping/120425-maritime-war-risk-premiums-fall-in-red-sea-rise-in-black-sea-amid-changing-security-dynamics; AJDIN, A., 2026. Suez traffic still 60% down 100 days after last Houthi attack. *Splash247* [online] [last viewed 24.09.2026]. Available from: https://splash247.com/suez-traffic-still-60-down-100-days-after-last-houthi-attack

34. IMF Portwatch, 2026. Chokepoint transit calls. *IMF Portwatch* [online] [last viewed 24.09.2026]. Available from: https://portwatch.imf.org

35. SHAMIM, S., 2026. How shipping insurance rates are rising, as Hormuz, Bab al-Mandeb shut down. *Al Jazeera* [online] [last viewed 24.09.2026]. Available from: https://www.aljazeera.com/economy/2026/7/23/how-shipping-insurance-rates-are-rising-as-hormuz-bab-al-mandeb-shut-down

36. ISO, 2018. *ISO 31000:2018 Risk Management – Guidelines*. Geneva: International Organization for Standardization, т. 6.5.2

37. Избягване, поемане на риск заради възможност, отстраняване на източника, промяна на вероятността, промяна на последиците, споделяне и задържане на риска (преразказани по вторичен източник).

38. Reuters, 2024. Red Sea war insurance rises with more ships in firing line. *Business Insurance* [online] [last viewed 28.09.2026]. Available from: https://www.businessinsurance.com/red-sea-war-insurance-rises-with-more-ships-in-firing-line

39. Lloyd's List, б. г. Red Sea war risk rates soften as insurers price in Prosperity Guardian. *Lloyd's List* [online] [last viewed 28.09.2026]. Available from: https://www.lloydslist.com/LL1147831/Red-Sea-war-risk-rates-soften-as-insurers-price-in-Prosperity-Guardian

40. LECCESE, G., 2026. „With the Shield, or On It?": Aspides and the EU's Aspirations for Sea Control. *CIMSEC* [online] [last viewed 18.09.2026]. Available from: https://cimsec.org/with-the-shield-or-on-it-aspides-and-the-eu-aspirations-for-sea-control

41. UNCTAD, 2024b. Review of Maritime Transport 2024. *UNCTAD* [online] [last viewed 28.09.2026]. Available from: https://unctad.org/system/files/official-document/rmt2024ch2_en.pdf

42. International Transport Forum, 2024. The Red Sea Crisis: Impacts on Global Shipping and the Case for International Co-operation. *OECD Publishing* [online] [last viewed 28.09.2026]. Available from: https://www.itf-oecd.org/sites/default/files/repositories/red-sea-crisis-impacts-global-shipping.pdf

43. TEU (на англ. *twenty-foot equivalent unit*) е единица за вместимост, равна на един двадесетфутов контейнер. Разходът включва гориво и наеми, намалени със спестените такси за Суецкия канал.

44. ECFR, 2026. 46 CFR Part 308 – War Risk Insurance. *ECFR* [online][last viewed 28.09.2026]. Available from: https://www.ecfr.gov/current/title-46/chapter-II/subchapter-G/part-308

45 BLANCHARD, Christopher M., 2026. Yemen: Conflict, Red Sea Attacks, and U.S. Policy. – In: *Focus IF12581*, version 17. *Library of Congress* [online] [last viewed 25.09.2026]. Available from: https://crsreports.congress.gov/product/pdf/IF/IF12581

46. NATO SHIPPING CENTRE, б. г. Naval Cooperation and Guidance for Shipping (NCAGS). *NATO* [online] [last viewed 28.09.2026]. Available from: https://mc.nato.int/nsc/activities/naval-cooperation-and-guidance-for-shipping-ncags

47. UKMTO, б. г. JMIC Products. *UKMTO* [online] [last viewed 28.09.2026]. Available from: https://www.ukmto.org/partner-products/jmic-products

48. International Transport Forum, 2024. The Red Sea Crisis: Impacts on Global Shipping and the Case for International Co-operation. *OECD Publishing* [online] [last viewed 28.09.2026]. Available from: https://www.itf-oecd.org/sites/default/files/repositories/red-sea-crisis-impacts-global-shipping.pdf

49. При две преминавания по 1,0 млн. USD съотношението е 1,7 / 2,0 = 0,85, а при едно преминаване е 1,7 / 1,0 = 1,7. При 0,2% и стойност на кораба 100 млн. USD съотношенията са 1,7 / 0,4 = 4,25 и 1,7 / 0,2 = 8,5. Стойността от 100 млн. USD е изчислена по оценката на Международния транспортен форум (1 млн. USD при 1%).

50. UNCTAD, 2024b. Review of Maritime Transport 2024. *UNCTAD* [online] [last viewed 28.09.2026]. Available from: https://unctad.org/system/files/official-document/rmt2024ch2_en.pdf

51. AJDIN, A., 2026. Suez traffic still 60% down 100 days after last Houthi attack. *Splash247* [online] [last viewed 24.09.2026]. Available from: https://splash247.com/suez-traffic-still-60-down-100-days-after-last-houthi-attack

52. Lloyd's List, 2023. Red Sea war risk rates still rising after doubling in past week. *Lloyd's List* [online] [last viewed 28.09.2026]. Available from: https://www.lloydslist.com/LL1147660/Red-Sea-war-risk-rates-still-rising-after-doubling-in-past-week

53. ITF Seafarers, 2026. IBF List of designated risk Areas with applicable benefits (as of 26 March 2026). *ITF Seafarers* [online] [last viewed 28.09.2026]. Available from: https://www.itfseafarers.org/sites/default/files/node/resources/files/IBF%20List%20of%20designated%20risk%20Areas%20with%20applicable%20benefits%20(as%20of%2026%20March%202026).pdf

ЛИТЕРАТУРА

ВЪЛКОВ, И.К., 2026. Асиметрична война в морето – изводи за съвместното планиране от Хуситската кампания в Червено море и протока Баб ел-Мандеб. В: *Съвременни аспекти на сигурността – предизвикателства, подходи, решения*. Научна сесия на факултет „Командно-щабен“, 28 септември 2026 г. София: Военна академия „Г. С. Раковски“, годишен том 7, с. 103 – 114. ISSN 2738-7526.

HEUER, R.J., 1999. *Psychology of Intelligence Analysis*. Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency.

NOTTEBOOM, T.; HARALAMBIDES, H.; CULLINANE, K., 2024. The Red Sea Crisis: Ramifications for Vessel Operations, Shipping Networks, and Maritime Supply Chains. *Maritime Economics & Logistics*, vol. 26, pp. 1-20. Available from: https://doi.org/10.1057/s41278-024-00287-z

PAES, W.-C.; BEALES, E.; HINZ, F.; VIDAL, A., 2024. Navigating Troubled Waters: The Houthis' Campaign in the Red Sea and the International Response. *International Institute for Strategic Studies* [online] [last viewed 24.09.2026]. Available froma: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2024/12/navigating-troubled-waters.pdf

REFERENCES

HEUER, R.J., 1999. *Psychology of Intelligence Analysis*. Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency.

NOTTEBOOM, T.; HARALAMBIDES, H.; CULLINANE, K., 2024. The Red Sea Crisis: Ramifications for Vessel Operations, Shipping Networks, and Maritime Supply Chains. *Maritime Economics & Logistics*, vol. 26, pp. 1-20. Available from: https://doi.org/10.1057/s41278-024-00287-z

VALKOV, I.K., 2026. Asimetrichna voyna v moreto – izvodi za savmestnoto planirane ot Husitskata kampania v Cherveno more i protoka Bab el-Mandeb. In: *Savremenni aspekti na sigurnostta – predizvikatelstva, podhodi, reshenia. Nauchna sesia na fakultet „Komandno-shtaben“, 28 septemvri 2026 g.* Sofia: Voenna akademia „G. S. Rakovski“, vol. 7, pp. 103 – 114. ISSN 2738-7526 [in Bulgarian].

ALTERNATIVES FOR MANAGING WAR RISK TO MERCHANT SHIPPING IN CONFLICT ZONES

Abstract. Since November 2023 the Ansar Allah movement (the Houthis) has attacked merchant ships in the Red Sea and the Bab el-Mandeb Strait with missiles, unmanned aerial vehicles and uncrewed surface vessels, and in July 2026 it declared a blockade of Saudi Arabia. Transits through the Suez Canal fell by almost half, while the war risk insurance premium rose many times over and at its peaks became comparable to the cost of sailing around Africa. Military commands measure success by targets struck, while shipping companies choose their route by the cost of a single transit. The paper examines which protective measures change

this choice, and for how long. Eight alternatives are classified by the risk treatment options of ISO 31000 and assessed against six criteria. The data show that insurers raise the premium within days but lower it only over months.

Keywords: ISO 31000; protection of shipping; Red Sea; sea line of communication; war risk; war risk insurance premium

Dr. Ivan Valkov, Assoc. Prof.
ORCID iD: 0009-0006-5116-957X
Chair of Navigation Training and Aviation Management
Faculty of Aviation
Georgi Benkovski Bulgarian Air Force Academy
1, Sv. sv. Kiril i Metodiy St.
5855 Dolna Mitropolia, Bulgaria
E-mail: ivan.valkovphd@gmail.com

https://doi.org/10. 66334/annu26_usloreaevo

УСЛОВИЯ ЗА УСПЕШНА РЕАЛИЗАЦИЯ НА ЕВОЛЮИРАЩИ СИСТЕМИ ЗА КОМАНДВАНЕ, УПРАВЛЕНИЕ, КОМУНИКАЦИИ, КОМПЮТРИ, КИБЕРПРОСТРАНСТВО, РАЗУЗНАВАНЕ, НАБЛЮДЕНИЕ И ВОЙСКОВО РАЗУЗНАВАНЕ (C5ISR) С ОТВОРЕНА АРХИТЕКТУРА

доц. д-р Иван Иванов[1], д-р Антон Манчев[1],
полковник доц. д-р Иван Чакъров[2]
[1] Институт по отбрана „Професор Цветан Лазаров“
[2] Военна академия „Георги Стойков Раковски“

Абстракт. Системата за командване, управление, комуникации, компютри, киберпространство, разузнаване, наблюдение и войсково разузнаване (C5ISR) е непрекъснато еволюираща система от системи. Тя се изгражда постепенно от самостоятелни системи с различен жизнен цикъл, а единството ѝ се осигурява от архитектурата. Нормативният отговор на тази особеност е модулният отворен системен подход в САЩ и отворената архитектура във Великобритания. В него отвореността е свойство на спецификацията на архитектурата, а модулността е свойство на конструкцията на системата.

Нормативното изискване обаче не е достатъчно. Разгледани са проблемите, които възникват при реализирането на отворена архитектура в система от системи. Чрез съпоставка на успешни и неуспешни проекти са формулирани условията за успешна реализация на еволюиращи системи C5ISR с отворена архитектура.

Ключови думи: еволюираща система; модулен отворен системен подход; отворена архитектура; C5ISR

I. Увод

Системите за командване, управление, комуникации, компютри, киберпространство, разузнаване, наблюдение и войсково разузнаване (C5ISR) се състоят от самостоятелни и полезни системи, които заедно пораждат способност, каквато никоя от тях няма (Henshaw 2011, p. 16).[1] Всяка от съставните системи има свой жизнен цикъл и се развива независимо от цялото.[2] Техниката, върху която са изградени, остарява бързо[3]: цикълът на информационните технологии е около 18 месеца.[4] Остаряват не само компютърните платформи, но и концепциите за реализиране на услугите. Дълготрайна е единствено дейността по командване и управление, която останалите съставки осигуряват (Ivanov 2025, p. 15). Затова такава система не се въвежда наведнъж, а се изгражда постепенно и остава в експлоатация, докато частите ѝ се подменят, т.е. тя е еволюираща система (на англ. *evolving system*).

Първата трудност е, че придобиването изостава от остаряването: при големите информационни системи на Министерството на отбраната на САЩ до първата доставена способност изтичат средно 91 месеца.[5] Предишното поколение тактически комуникационни системи е замисляно като единно цяло: американската програма TRI-TAC е учредена през 1971 г., за да проектира и въведе обща тактическа комуникационна система за трите вида въоръжени сили (Raggett 1982, p. 661). Националните опорни мрежи *RITA*, *AUTOKO*, *Ptarmigan*, *ZODIAC* и *MSE* (Ryan, Frater 2002, p. 125) са разработени за корпусна зона в конфликт с висока интензивност и след Студената война се използват в обстановка, за която не са предназначени (Ryan, Frater 2002, p. 131). Пример за мащаба е британската *Bowman*: 48 000 радиостанции и 28 000 терминала в до 15 700 машини, както и в кораби и вертолети.[6] До първата оперативна способност на една програма могат да изминат до десет години, а при системи от такъв мащаб бюджетирането, възлагането и приемането не могат да следват 18-месечния цикъл.[7] Затова

единството на системата не може да се осигури с една доставка и се пренася от конструкцията в архитектурата.

Втората трудност засяга външните проектни роли. Успешна е системата, която отговаря на очакванията им, а те са многобройни и променливи (Levenchuk 2022, p. 11); при неотчетена роля системата е неуспешна (Levenchuk 2023, pp. 249, 251). При система от системи заинтересованите страни са на две равнища с конкуриращи се интереси, не всички са разпознати, а цялото няма власт над всички съставни системи.[8] Отличава я не устройството ѝ, а независимостта на създаващите я системи една от друга: отговорният за цялото няма правомощия да предпише обща модернизация на частите му (Levenchuk 2024, pp. 149 – 153). Затова неотчетената роля тук не е пропуск на отделния проект, а свойство на класа.

Опитът в създаването на такива системи е дълъг и добре документиран, но проектите и досега не постигат целите си. Според Националната сметна палата на Обединеното кралство (NAO) въвеждането в експлоатация на 13 от 20 големи британски програми за въоръжение се очаква да закъснее общо с 254 месеца.[9] Сметната палата отбелязва още, че програми като *Bowman* по своята същност се развиват поетапно и непрекъснато, защото техническите промени извън тях, обновяването на софтуера, развитието на доктрината и оперативният опит налагат редовни изменения.[10] Националният изследователски съвет на САЩ стига до същия извод за информационните системи в отбраната: придобиването им многократно е неуспешно въпреки повече от 20 години препоръки.[11] Повтарянето на неуспеха въпреки наличното знание показва, че причината е в начина на създаване на такива системи. Оттук произтича основният изследователски въпрос: При какви условия проект за система, която по устройство никога не е завършена, достига приета конфигурация в предвидения обхват и срок?

Отговор на тези трудности се търси първо в САЩ. През 1994 г. ръководителят на придобиването в Министерството на отбраната на САЩ нарежда отворените стандарти да се прилагат в електрониката на оръжейните системи, а министерството създава работна група по отворените системи за по-ниски разходи през жизнения цикъл и по-добра оперативна съвместимост.[12] Издаденото от нея ръководство определя модулния отворен системен подход (*Modular Open Systems Approach – MOSA*) чрез пет принципа: благоприятна среда, модулен строеж, определяне на ключовите интерфейси, отворени стандарти за тях и удостоверяване на съответствието.[13] От 2016 г. подходът е задължителен по закон за големите програми, а от 2021 г. – и за всички програми за оръжейни системи.[14] Законът го определя

като единна търговска и техническа стратегия с модулни интерфейси, консенсусни стандарти, заменяеми компоненти и права върху техническите данни.[15] Във Великобритания сродното начинание се нарича отворена архитектура (*open architecture*) и присъства в придобиването поне от 2008 г.[16] (Henshaw 2011, p. 12). Двете названия не са синоними: американското означава подход към придобиването, а британското е свойство на архитектурата.

Тезата е, че отворената архитектура е полезно, но недостатъчно условие за успеха на проекта. Успех тук означава приета конфигурация, т.е. състояние на системата, преминало приемане и въведено в експлоатация в предвидения обхват и срок. Приемането е институционалната форма, в която външните проектни роли дават съгласието си в даден момент, а при еволюираща система то се подновява с всяка конфигурация (Levenchuk 2023, p. 249). При еволюционна разработка никой екземпляр не е последен, защото всяка реализирана версия е прототип на следващата (Levenchuk 2022, pp. 96-97). Изследването е концептуален анализ чрез целеви преглед на документи към 20 септември 2026 г.: условията се извеждат от съпоставка на документирани проекти и се проверяват върху британския проект *Morpheus*.

II. Отворената архитектура: определения и очаквани ползи

Възможностите на отворената архитектура се изясняват едва след разграничаване на модулността, архитектурата и отвореността. Модулността е обособеност на частите: функционалните елементи са взаимосвързани, но ограничени и самостоятелни. Модулът е такъв елемент, който се придобива, поддържа и продава отделно и има самостоятелна оперативна полза (Henshaw 2011, p. 17, 19). Границата между два модула, която осигурява спрягането им, е интерфейсът (Levenchuk 2023, p. 604, 701). Конструкцията е модулна, когато функциите и компонентите си съответстват еднозначно, а интерфейсите не обвързват компонентите, т.е. промяна в едния не налага промяна в другия; интерфейсът може да е стандартен или фирмен (Ulrich 1995, §2–3).

Архитектурата е основната концепция на системата в средата ѝ, въплътена в елементите, отношенията и принципите на проектирането и развитието ѝ (Henshaw 2011, p. 16), и се описва в спецификация от модули, интерфейси и правила. Отвореността е свойство на спецификацията, не на системата: отворена е спецификацията, публикувана за определена общ-

ност толкова подробно, че независими участници да реализират съвместими части (Henshaw 2011, pp. 15-16). В системата отвореността се проявява като възможност да се добавят или заменят модули от различни доставчици (Henshaw 2011, p. 2, 16). Модулността е техническо свойство, а отвореността – търговско (Henshaw 2011, p. 10, 19).

Очакваните ползи са три: технологично обновяване през жизнения цикъл, конкуренция след първоначалния избор и ограничаване на зависимостта от един доставчик. Първата произтича от модулността, другите две – от отвореността. Ползите имат цена и тя е на границата между модулите. Възложителят придобива способност, а доставчикът продава модул; способността обхваща много модули и възниква само ако работи и частта отвъд границата на модула, която не е в договора на доставчика.

III. Нормата и резултатът: неуспешни и успешни проекти

Включването на отворена архитектура в нормативните изисквания не е достатъчно и това се вижда първо там, където то е най-старо. През 2000 г. генералният инспектор на Министерството на отбраната на САЩ установява, че целите на отворените системи не са приложени докрай в планирането на придобиването. През 2023 г. Сметната палата на САЩ (GAO) отчита, че повечето програми заявяват подхода, без да планират последователно проверка на прилагането му.[17] Тридесет години законодателни и политически усилия още не са довели до последователно прилагане.[18] Дори привърженици на подхода отчитат, че последните тактически безжични мрежи са скромно подобрение спрямо наследените от началото на 90-те години, а програмата *Joint Tactical Radio System* има многобройни закъснения и съществено поскъпване (Elmasry 2012, pp. 207-208).

Очакваните ползи са по-слабо обосновани, отколкото предполага нормата. Никоя от двадесетте програми, проверени от GAO, не документира анализ на разходите и ползите, а самото министерство не разполага с приет метод за оценка.[19] Според съвместната британска оценка отвореността сама по себе си не е нито изискване, нито полза, ползите не настъпват неизбежно, а повечето идват от модулността (Henshaw 2011, p. 11, 44). Патентните, лицензионните и договорните условия остават, а подмяната на изпълнител не е универсален критерий (Radoman et al. 2025, pp. 20-23).

Организациите, които проектират системи, създават проекти, които повтарят комуникационните им структури (Conway 1968). Затова първо се проектира по-добрата структура на системата, а след това организацията

на създателя се приспособява към нея (Levenchuk 2022, p. 143). Създателят на система C5ISR не е една организация, а множество независими субекти. Обща комуникационна структура те имат само чрез договорите, които определят кой на кого дължи данни, изпитване и приемане, и системата я повтаря.

И в САЩ, и във Великобритания има неуспешни проекти както за системи от типа C5ISR, така и за системи с предписана отворена архитектура. Системата *Bowman* не спазва първоначалния си срок – 1995 г. Обявена е за въведена в експлоатация през 2004 г. с 27 уговорки, придружаващата я платформа – с година закъснение, а програмата е преработена, защото сроковете са прекомерно амбициозни спрямо техническите трудности.[20] Американската програма *Joint Tactical Radio System* има за цел да създаде обща софтуерно-дефинирана радиостанция за всички видове въоръжени сили, но след многобройни закъснения и разходи от 6 млрд. долара не осъществява замисъла за пълна съвместимост. Сред причините са мащабът ѝ и постоянното разширяване на изискванията (Ivanov 2025, p. 20). Брониранатa машина *Ajax* е проектирана по британския стандарт за отворена архитектура на машините, задължителен от 2010 г. (Henshaw 2011, p. 36), но Националната сметна палата (NAO) установява неразбрани спецификации на компонентите и на интеграцията им, четири години закъснение и около 1200 изисквания за способност към всеки от шестте типа машини.[21]

Документираните успешни приложения на отворената архитектура са малко и се отнасят до платформени подсистеми: Министерството на отбраната на САЩ посочва пред GAO самолета P-8A и бойните системи на подводниците.[22] Американската програма *Acoustic Rapid COTS Insertion (A-RCI)* превръща интегрираната акустична система на подводниците в модулна със значително по-ниски разходи и по-добри показатели. Софтуерът се обновява ежегодно, а хардуерът – на две години. Ключовите интерфейси, стандарти и протоколи се контролират строго, конкуренцията е при равни условия, сътрудничеството между спечелилите е договорено, правата върху интелектуалната собственост са структурирани, а потребителите участват пряко (Boudreau 2006, pp. 185-186). Крайната точка на програмата не е била определена, но всяка стъпка е. Референтната архитектура *PYRAMID* за авиониката е собственост на Министерството на отбраната на Великобритания. Стандартът ѝ разграничава проектанта на системата, проектанта на компонент и интегратора[23], а при проверката през 2022 г. втори доставчик разработва компонент по публикувания пакет и го инте-

грира в технологичния демонстратор на водещия изпълнител.[24] Резултатът обаче е технологичен демонстратор, а не приета конфигурация.

Съпоставката показва, че отворената архитектура не разграничава двете групи: тя е налице и при закъсняващия *Ajax*, и при успешната *A-RCI*. Разликите са четири. Първата е определеният резултат за всяка стъпка: *A-RCI* доставя ежегодно без предварително определена крайна точка, а *Ajax* и *Bowman* обвързват пълния обем изисквания с един срок. Втората е органът, който отговаря за границите: ключовите интерфейси на *A-RCI* и архитектурата *PYRAMID* са под един орган на възложителя, а при *Ajax* спецификациите на интеграцията остават неразбрани. Третата е договорното уреждане на границите: при *A-RCI* сътрудничеството между спечелилите е договорно задължение, а не добра воля. Четвъртата са правата: *A-RCI* структурира интелектуалната собственост, а МО на Великобритания притежава *PYRAMID*. И в двата успешни случая системата е подсистема на платформа с един възложител. Изследването на *A-RCI* оставя открит въпроса дали подходът се пренася в мащаба на системите за командване и управление (Boudreau 2006, p. 186). Към този въпрос се отнася проектът *Morpheus*.

IV. Проектът *Morpheus*

Британският проект *Morpheus* е подходящ обект за проверка на изводите по три причини. По състав той е система от типа *C5ISR*: обхваща връзките за глас и данни от войника до щаба, мрежата, приложенията и интерфейсите към платформите, към наследената система, към съюзниците и към домейните на електронната война и киберпространството. Отворената архитектура е изрично заявена като негова цел: преходът към нея (*Evolve to Open – EvO*) е предмет на основния му договор[25] (Clark, Armstrong 2022, pp. 8-9). За проекта има и публичен договорен замисъл, независим одит и последвали промени в модела на придобиване. В програмата за тактическите комуникационни и информационни системи на британските сухопътни сили (*LETacCIS*) той трябва да замени системата *Bowman* – затворена, на един изпълнител и с тридесетгодишна технология; включва поддържането ѝ, прехода към отворена архитектура, нови радиосредства и приложения[26] (Clark, Armstrong 2022, pp. 6-7).

Договорът *Evolve to Open Transition Partner (EvO TP)*, възложен през 2017 г. за £330 млн. (Clark, Armstrong 2022, p. 4), трябва да осигури до декември 2020 г. лабораторно изпитан технически проект на отворена

архитектура. Срокът не е спазен и договорът е приключен през декември 2023 г., без да е удостоверена доставена оперативна система.[27] През септември 2026 г. МО на Великобритания отговаря на парламентарен въпрос, че проектът няма да продължи като самостоятелен, но потребността остава и ще бъде разгледана в друга програма.[28]

Документираните причини са четири и съвпадат с разликите от съпоставката. Първата е несъответствието между публично описаното предназначение на програмата (Clark, Armstrong 2022, pp. 5-6) и договорения резултат. Изпълнителят посочва, че до 2020 г. се е очертало разминаване в очакванията на страните (Clark, Armstrong 2022, p. 9). Втората е наследството: според министерството *Bowman* е фирмена система на изпълнителя и затова договорът не може да се възложи повторно чрез конкуренция (Cartlidge 2024). Третата е капацитетът на възложителя: според Националната сметна палата (NAO) министерството няма достатъчен капацитет за замисления роля на псевдо-главен изпълнител (на англ. *pseudo-prime*) и изпитва затруднения при гъвкава разработка с твърда цена.[29] Четвъртата е техническият мащаб: изискванията са прекомерно амбициозни и прекалено конкретни и нямат слой за електронна война и киберпространство.[30] Проектът е замислен, преди да се оформи концепцията за многодомейнни операции. Тя и изискването за коалиционна съвместимост се появяват след възлагането на договора.[31] Явлението не е особеност на този проект: изискванията се променят в хода на проекта както при системата *Bowman*[32], така и при програмата *Joint Tactical Radio System* (Ivanov 2025, p. 20).

Тези причини произтичат от границите на отворената система. За архитектурата не може да се съди, преди да е известно поведението на системата в обкръжението ѝ (Levenchuk 2023, p. 423). При *Morpheus* обаче предмет на договора е базова отворена архитектура, върху която да се изгражда (Clark, Armstrong 2022, pp. 8-9), а целевото решение остава неясно.[33] Отвореността се отнася до спецификациите на интерфейсите, а протоколите на границата с *Bowman* са собственост на изпълнителя (Cartlidge 2024). Отворената система е трябвало да започне от затворени и чужди сглобки, а новото се приспособява към старото.[34] Наследената архитектура е интегрална, т.е. компонентите ѝ реализират по няколко функции наведнъж (Ulrich 1995, §3). Тя не се отваря чрез публикуване, а трябва да се раздели наново на модули;. Това е възложено на страната, за която модулността означава загуба на продажби. Създателят на новата система има един договор с един изпълнител, чиято комуникационна структура е затворената стара система. Съгласно закона на Конуей се очаква проектът да я повтори.

С базовата отворена архитектура проектът *Morpheus* придобива правото да сменя модули, но не и системата, в която да ги сменя.

V. Условия за успешна реализация

Четирите разлики от съпоставката и четирите причини при *Morpheus* сочат едни и същи условия. Британските реформи след проекта им дават институционална форма, но успехът им все още не е доказан. Първото условие е определен резултат за всяка стъпка: моделът *Integrated Procurement Model* въвежда спирално развитие чрез минимална използваема способност (*Minimum Deployable Capability*).[35]

Второто условие е орган, който носи архитектурната отговорност и разполага с права, информация, хора и средства и който превръща субектите на създателя в система. За това са нужни финансирана работа по границите и приемане на две равнища: на модула по интерфейсната спецификация и на конфигурацията за експлоатация. При система C5ISR той се нуждае и от споразумения за интерфейсите извън програмата или премества границата навътре: от чуждата платформа в системата влизат само интерфейсните модули, а платформата остава външно обкръжение (Levenchuk 2023, p. 677). При липса на правомощия над интерфейсите архитектът все пак има задача: да определи границата на системата си. Организацията може да е концентрирана, когато главният изпълнител отговаря и за архитектурата, както при *Morpheus*, или разпределена, когато контролът остава у възложителя, както при *A-RCI*.

Третото условие е договорната структура да е съгласувана с техническите зависимости и с темпа на изменение. При разпределен създател договорът е комуникационната структура, затова всяка граница в архитектурата трябва да е нечие платено задължение с данни, изпитване и приемане. Сегментираният подход към придобиването обособява модулните обновявания на комуникациите и сензорите като отделен конкурентен сегмент.[36] Четвъртото условие е пазар с реални алтернативи и права върху спецификацията и данните, без които алтернативите не могат да се използват.[37]

VI. Заключение

Системите C5ISR се опират на бързо остаряващи компютърни платформи и концепции за реализиране на услугите: те се изграждат постепенно от самостоятелни системи и единството им се осигурява от архитектурата. Затова нормативният отговор е отворената архитектура и затова

неуспехът ѝ има висока цена. Тя е полезно, но недостатъчно условие за успешна реализация на такава система: отваря границата на модула, но не я прави нечие задължение. Съпоставката на проектите и случаят *Morpheus* сочат четири условия: определен резултат за всяка стъпка, орган с архитектурна отговорност, договорна структура, съгласувана с техническите зависимости, и пазар с алтернативи и права върху данните.

За възложител без собствена индустрия условията са проверими още преди договора: наследената система, правата върху нея и капацитетът за водещата роля са или не са налице. Без тях отворената архитектура дава право на избор, но не и система, в която той да се приложи.

БЕЛЕЖКИ

1. National Research Council, 2010. *Achieving Effective Acquisition of Information Technology in the Department of Defense*. Washington, DC: The National Academies Press. ISBN 978-0-309-14828-3. DOI: 10.17226/12823

2. United States Department of Defense, 2008. *Systems Engineering Guide for Systems of Systems, Version 1.0*. Washington, DC: Office of the Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering, p. 11, 19

3. Defense Science Board, 2009. *Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology.* Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, p. ix.

4. National Research Council, 2010. *Achieving Effective Acquisition of Information Technology in the Department of Defense*. Washington, DC: The National Academies Press, p. 31. ISBN 978-0-309-14828-3. DOI: 10.17226/12823

5. Defense Science Board, 2009. *Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology.* Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, p. 36.

6. National Audit Office, 2006. *Ministry of Defence: Delivering digital tactical communications through the Bowman CIP programme*. London: NAO. HC 1050, Session 2005–06, 25.07.2006.

7. National Research Council, 2010. *Achieving Effective Acquisition of Information Technology in the Department of Defense*. Washington, DC: The National Academies Press, p. 31. ISBN 978-0-309-14828-3. DOI: 10.17226/12823

8. United States Department of Defense, 2008. *Systems Engineering Guide for Systems of Systems, Version 1.0*. Washington, DC: Office of the Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering, p. 11

9. National Audit Office, 2021. *Improving the performance of major equipment contracts.* London: NAO. HC 298, p. 4.

10. National Audit Office, 2006. *Ministry of Defence: Delivering digital tactical communications through the Bowman CIP programme*. London: NAO. HC 1050, Session 2005–06, 25.07.2006.

11. National Research Council, 2010. *Achieving Effective Acquisition of Information Technology in the Department of Defense*. Washington, DC: The National Academies Press, p. 12, 16. ISBN 978-0-309-14828-3. DOI: 10.17226/12823

12. United States Government Accountability Office, 2025. *Weapon Systems Acquisition: DOD Needs Better Planning to Attain Benefits of Modular Open Systems*. GAO-25-106931. Washington, DC: GAO, p. 10

13. Open Systems Joint Task Force, 2004. *Program Manager's Guide: A Modular Open Systems Approach (MOSA) to Acquisition. Version 2.0.* Washington, DC: OSJTF, разд. 1, p. 3-4

14. United States Government Accountability Office, 2025. *Weapon Systems Acquisition: DOD Needs Better Planning to Attain Benefits of Modular Open Systems*. GAO-25-106931. Washington, DC: GAO, p. 10

15. United States Congress, 2016. *Requirement for modular open system approach in major defense acquisition programs; definitions.* 10 U.S.C. §4401. Pub. L. 114-328, §805, 23.12.2016; изм. 116-283, 118-159, 119-60; §4401(a) и (c)(1).

16. Ministry of Defence, 2025a. *Defence Industrial Strategy: Making Defence an Engine for Growth.* London: MOD. CP 1388.

17. United States Government Accountability Office, 2025. *Weapon Systems Acquisition: DOD Needs Better Planning to Attain Benefits of Modular Open Systems*. GAO-25-106931. Washington, DC: GAO, p. 10

18. United States Government Accountability Office, 2025. *Weapon Systems Acquisition: DOD Needs Better Planning to Attain Benefits of Modular Open Systems*. GAO-25-106931. Washington, DC: GAO, p. 9

19. United States Government Accountability Office, 2025. *Weapon Systems Acquisition: DOD Needs Better Planning to Attain Benefits of Modular Open Systems*. GAO-25-106931. Washington, DC: GAO, p. 2, 20, 26

20. National Audit Office, 2006. *Ministry of Defence: Delivering digital tactical communications through the Bowman CIP programme*. London: NAO. HC 1050, Session 2005–06, 25.07.2006.

21. National Audit Office, 2022. *The Ajax programme.* London: NAO. HC 1142, p. 8.

22. United States Government Accountability Office, 2025. *Weapon Systems Acquisition: DOD Needs Better Planning to Attain Benefits of Modular Open Systems*. GAO-25-106931. Washington, DC: GAO, p. 26

23. Ministry of Defence, 2025b. *PYRAMID Technical Standard Guidance V1.0.* PYD/TechStanGuide/V1.0, 24.02.2025, прил. D, pp. 481–489

24. Ministry of Defence, 2025c. PYRAMID: rapid adaptability for avionics systems. Guidance, 31.03.2025. Available from: https://www.gov.uk/guidance/pyramid-rapid-adaptability-for-avionics-systems

25. Ministry of Defence, 2023. MOD Update on the Land Environment Tactical Communication and Information Systems (LETacCIS). UK Parliament. HCWS137, 14.12.2023. Available from: https://questions-statements.parliament.uk/written-statements/detail/2023-12-14/hcws137

26. Ministry of Defence, 2023. MOD Update on the Land Environment Tactical Communication and Information Systems (LETacCIS). UK Parliament. HCWS137,

14.12.2023. Available from: https://questions-statements.parliament.uk/written-statements/detail/2023-12-14/hcws137; SYLVIA, N., 2024. Upgrading the British Army's Tactical Communications: What Next?. *RUSI* [online]. Available from: https://www.rusi.org/explore-our-research/publications/commentary/upgrading-british-armys-tactical-communications-what-next

27. Ministry of Defence, 2023. MOD Update on the Land Environment Tactical Communication and Information Systems (LETacCIS). UK Parliament. HCWS137, 14.12.2023. Available from: https://questions-statements.parliament.uk/written-statements/detail/2023-12-14/hcws137

28. POLLARD, L., 2026. Project Morpheus. *UK Parliament* [online]. UIN 19180, 02.09.2026. Available from: https://questions-statements.parliament.uk/written-questions/detail/2026-07-15/19180

29. National Audit Office, 2021. *Improving the performance of major equipment contracts.* London: NAO. HC 298, p. 37.

30. SYLVIA, N., 2024. Upgrading the British Army's Tactical Communications: What Next?. *RUSI* [online]. Available from: https://www.rusi.org/explore-our-research/publications/commentary/upgrading-british-armys-tactical-communications-what-next

31. Nettlefold, J., 2021. UK Multi-Domain Warfare Takes a Step Forward. *Battlespace* [online]. Available from: https://battle-updates.com/uk-multi-domain-warfare-takes-a-step-forward-by-julian-nettlefold

32. National Audit Office, 2006. *Ministry of Defence: Delivering digital tactical communications through the Bowman CIP programme*. London: NAO. HC 1050, Session 2005–06, 25.07.2006

33. National Audit Office, 2021. *Improving the performance of major equipment contracts.* London: NAO. HC 298, p. 37.

34. SYLVIA, N., 2024. Upgrading the British Army's Tactical Communications: What Next?. *RUSI* [online]. Available from: https://www.rusi.org/explore-our-research/publications/commentary/upgrading-british-armys-tactical-communications-what-next

35. Ministry of Defence, 2024. *Integrated Procurement Model: Driving pace in the delivery of Military Capability.* London: MOD

36. Ministry of Defence, 2025a. *Defence Industrial Strategy: Making Defence an Engine for Growth.* London: MOD. CP 1388, pp. 88-89

37. United States Congress, 2016. *Requirement for modular open system approach in major defense acquisition programs; definitions.* 10 U.S.C. §4401. Pub. L. 114-328, §805, 23.12.2016; изм. 116-283, 118-159, 119-60; §4401(a) и (c)(1)

ЛИТЕРАТУРА

ИВАНОВ, И. П., 2025. *Софтуерно-дефинирани радиокомуникационни системи.* София: Институт по отбрана „Професор Цветан Лазаров“. 215 с. ISBN 978-619-90024-8-3.

ЛЕВЕНЧУК, А., 2023. *Практическое системное мышление – 2023: Учебник.* [б. м.]: Издательские решения. 734 с. ISBN 978-5-4490-4439-6.

ЛЕВЕНЧУК, А., 2022. *Системная инженерия 2022.* Курс, версия от 24.08.2022. [Б. м.: б. и.]. 229 с.

ЛЕВЕНЧУК, А., 2024. *Системное мышление 2024. Том 2.* [б. м.]: Издательские решения. ISBN 978-5-0064-2855-3.

BOUDREAU, M.W., 2006. Acoustic Rapid COTS Insertion – Case Study. *Proceedings of the Third Annual Acquisition Research Symposium.* NPS-AM-06-071. Monterey: Naval Postgraduate School, pp. 185-186.

CARTLIDGE, J., 2024. Morpheus. UK Parliament. Written answer, UIN 8892. *UK Parliament* [online]. Available from: https://questions-statements.parliament.uk/written-questions/detail/2024-01-10/8892

CLARK, R.; ARMSTRONG, S., 2022. *Morpheus: The British Army's Next Procurement Failure?.* London: Henry Jackson Society.

CONWAY, M.E., 1968. How Do Committees Invent?. *Datamation magazine*, pp. 28–31. Available from: https://www.melconway.com/Home/Committees_Paper.html

ELMASRY, G.F., 2012. *Tactical Wireless Communications and Networks: Design Concepts and Challenges.* Chichester: John Wiley & Sons. ISBN 978-1-119-95176-6.

HENSHAW, M.J. de C. (ed.), 2011. *Assessment of Open Architectures within Defence Procurement.* Loughborough University. Issue 1.

RADOMAN, R.L.V.; HENSHAW, M.; KING, M.; RABBETS, T., 2025. Enabling Open Architecture in Military Systems: A Systemic and Holistic Analysis. *Systems,* vol. 13, no 3, p. 207. Available from: https://doi.org/10.3390/systems13030207.

RAGGETT, R.J. (ed.), 1982. *Jane's Military Communications 1982.* 3rd ed. London: Jane's Publishing Company. ISBN 0-86720-615-2.

RYAN, M.J.; FRATER, M.R., 2002. *Tactical Communications for the Digitized Battlefield.* Boston: Artech House. 372 pp. ISBN 1-58053-323-X.

ULRICH, K.T., 1995. The role of product architecture in the manufacturing firm. *Research Policy,* vol. 24, no 3, pp. 419-440. Available from: https://doi.org/10.1016/0048-7333(94)00775-3.

REFERENCES

BOUDREAU, M.W., 2006. Acoustic Rapid COTS Insertion – Case Study. *Proceedings of the Third Annual Acquisition Research Symposium.* NPS-AM-06-071. Monterey: Naval Postgraduate School, pp. 185-186.

CARTLIDGE, J., 2024. Morpheus. UK Parliament. Written answer, UIN 8892. *UK Parliament* [online]. Available from: https://questions-statements.parliament.uk/written-questions/detail/2024-01-10/8892

CLARK, R.; ARMSTRONG, S., 2022. *Morpheus: The British Army's Next Procurement Failure?.* London: Henry Jackson Society.

CONWAY, M.E., 1968. How Do Committees Invent?. *Datamation magazine*, pp. 28–31. Available from: https://www.melconway.com/Home/Committees_Paper.html

ELMASRY, G.F., 2012. *Tactical Wireless Communications and Networks: Design Concepts and Challenges.* Chichester: John Wiley & Sons. ISBN 978-1-119-95176-6.

HENSHAW, M.J. de C. (ed.), 2011. *Assessment of Open Architectures within Defence Procurement.* Loughborough University. Issue 1.

IVANOV, I.P., 2025. *Softuerno-definirani radiokomunikatsionni sistemi*. Sofia: Institut po otbrana „Profesor Tsvetan Lazarov". 215 s. ISBN 978-619-90024-8-3 [in Bulgarian].

LEVENCHUK, A., 2023. *Prakticheskoye sistemnoye myshleniye - 2023: Uchebnik.* [b. m.]: Izdatel‘skiye resheniya. 734 s. ISBN 978-5-4490-4439-6 [in Russian].

LEVENCHUK, A., 2022. *Sistemnaya inzheneriya 2022*. Kurs, versiya ot 24.08.2022. [B. m.: b. i.]. 229 s. [in Russian].

LEVENCHUK, A., 2024. *Sistemnoye myshleniye 2024*. Tom 2. [b. m.]: Izdatel’skiye resheniya. ISBN 978-5-0064-2855-3 [in Russian].

RADOMAN, R.L.V.; HENSHAW, M.; KING, M.; RABBETS, T., 2025. Enabling Open Architecture in Military Systems: A Systemic and Holistic Analysis. *Systems,* vol. 13, no 3, p. 207. Available from: https://doi.org/10.3390/systems13030207.

RAGGETT, R.J. (ed.), 1982. *Jane‘s Military Communications 1982.* 3rd ed. London: Jane‘s Publishing Company. ISBN 0-86720-615-2.

RYAN, M.J.; FRATER, M.R., 2002. *Tactical Communications for the Digitized Battlefield.* Boston: Artech House. 372 pp. ISBN 1-58053-323-X.

ULRICH, K.T., 1995. The role of product architecture in the manufacturing firm. *Research Policy,* vol. 24, no 3, pp. 419-440. Available from: https://doi.org/10.1016/0048-7333(94)00775-3.

CONDITIONS FOR THE SUCCESSFUL REALIZATION OF EVOLVING C5ISR SYSTEMS WITH OPEN ARCHITECTURE

Abstract. A C5ISR system is a continuously evolving system of systems. It is built up gradually from independent systems with different life cycles, and its unity is provided by the architecture. The normative response to this feature is the Modular Open Systems Approach in the United States and open architecture in the United Kingdom. In it, openness is a property of the architecture specification, and modularity a property of the system‘s construction. Mandating it, however, is not sufficient. The paper examines the problems that arise in realizing open architecture in a system of systems. By comparing successful and unsuccessful projects, it formulates the conditions for the successful realization of evolving C5ISR systems with open architecture.

Keywords: C5ISR; evolving system; Modular Open Systems Approach; open architecture

Dr. Ivan Ivanov, Assoc. Prof.
ORCID iD: 0009-0002-1304-1306
Defence Institute “Professor Tsvetan Lazarov”
2, Professor Tsvetan Lazarov Blvd.
1592 Sofia, Bulgaria
E-mail: i.p.ivanov@di.mod.bg

Dr. Anton Manchev
Defence Institute "Professor Tsvetan Lazarov"
2, Professor Tsvetan Lazarov Blvd.
1592 Sofia, Bulgaria
E-mail: a.manchev@di.mod.bg

Colonel Dr. Ivan Chakarov, Assoc. Prof.
ORCID iD: 0000-0002-6062-4806
Communication and Information Systems Department
Command and Staff Faculty
Rakovski National Defence College
82, Evlogi i Hristo Georgievi Blvd.
1504 Sofia, Bulgaria
E-mail: i.chakarov@rndc.bg

https://doi.org/10. 66334/annu26_6glan

ЛОКАЛНИ БЕЗЖИЧНИ МРЕЖИ, БАЗИРАНИ НА ТЕХНОЛОГИИ ЗА КЛЕТЪЧНИ СИСТЕМИ ОТ ШЕСТО ПОКОЛЕНИЕ (6G LAN): ОСОБЕНОСТИ, АРХИТЕКТУРА И ПЕРСПЕКТИВИ

доц. д-р Иван Иванов[1], доц. д-р Александър Колев[1], полковник доц. д-р Иван Чакъров[2]
[1]Институт по отбрана „Професор Цветан Лазаров“
[2]Военна академия „Георги Стойков Раковски“

Абстракт. В статията се разглежда развитието на локалните безжични мрежи в контекста на клетъчните комуникации от шесто поколение. Представят се концепцията за локални мрежи в 6G (6G Local Area Networks, 6G LAN), нейните особености и основните архитектурни подходи. Чрез съпоставка със съществуващите локални клетъчни решения се изясняват приемствеността и възможните промени в организацията на локалната комуникация. Обсъждат се перспективите за по-тясно обвързване на комуникацията, обработката на информация и предоставянето на услуги, както и предпоставките и ограниченията за практическото им реализиране. Анализът очертава направления за развитие на 6G LAN, при които архитектурните решения се оценяват според изискванията на приложенията и условията на използване.

Ключови думи: 6G; локални безжични мрежи; 6G LAN; клетъчни комуникации; непублични мрежи; мрежова архитектура

1. Увод

Шестото поколение клетъчни комуникации (6G) се развива в рамката IMT-2030 (International Mobile Telecommunications for 2030 and beyond). Препоръка M.2160-0 на Сектора по радиосъобщения на Международния съюз по далекосъобщения (ITU-R) определя общите ѝ цели и добавя към свързаността по-тясно взаимодействие между комуникацията, изкуствения интелект и радиосензорното наблюдение (ITU-R 2023). Обсъждат се и услуги, които изискват съгласувана работа на комуникационни и изчислителни ресурси. Възможните направления за военно приложение са разгледани в отделна публикация (Ivanov 2026).

6G все още не е завършен стандарт: проучванията в 3GPP (3rd Generation Partnership Project) са включени в Release 20, а Release 21 е предвиден като първи нормативен пакет за 6G[1]. По тази причина трябва да се разграничават вече реализираните възможности, архитектурните предложения и очакваните бъдещи характеристики. Това е особено важно за локалните мрежи, защото част от обсъжданите за тях възможности вече имат основа в съществуващите технологии. В този контекст се оформя направлението 6G Local Area Networks (6G LAN) – локални мрежи за ограничено пространство или обект, изградени с технологиите на шестото поколение. Интересът към него е свързан с организирането на комуникацията и обработката близо до приложенията и с взаимодействието на локалната система с по-голямата мрежа. Както самото 6G, и 6G LAN се разглежда тук като архитектурно направление, а не като установен модел на локална мрежа.

Доминиращата технология за безжични локални мрежи е фамилията стандарти IEEE 802.11 (Wi-Fi) (Goldsmith 2005, p. 12, 558), а прегледът на нейното развитие е извън обхвата на статията. Тук се разглеждат локалните мрежи, изградени с клетъчни технологии: частните мрежи от пето поколение (5G) пренасят тези технологии в ограничена среда със собствени услуги и управление (Prados-Garzon et al. 2021). Следователно „локална“ и „клетъчна“ мрежа не са противоположни понятия – първото описва обхвата и организацията на системата, второто – технологията на достъпа. Сравнението с 6G LAN трябва да отчита и радиоинтерфейса, и разполагането на функциите, и начина на вземане на управляващите решения. Статията търси отговор на въпроса какво добавя подмрежовият подход и при какви условия различната организация на функциите носи практическа полза. Отговорът се търси чрез съпоставка с наличните решения, така че перспек-

тивите да се обсъждат като отговор на конкретни потребности, а не като следствие от смяната на поколението.

2. Локални мрежи на основата на 5G

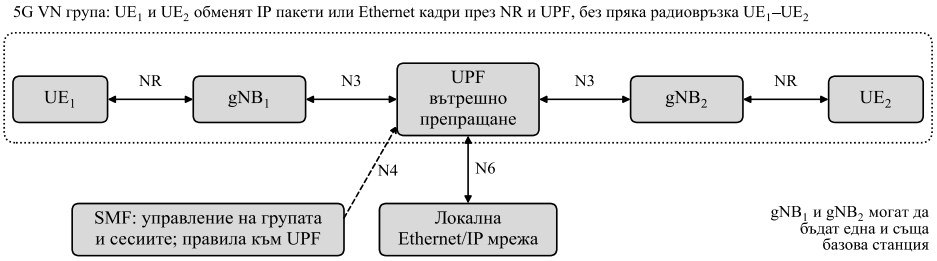
Клетъчната технология не е ограничена до обществена мрежа с национално покритие. Непубличната мрежа (Non-Public Network, NPN) е 5G система за непублично ползване. Тя е самостоятелна (Stand-alone Non-Public Network, SNPN), когато не разчита на мрежови функции на обществена мобилна мрежа, или интегрирана с обществена мрежа (Public Network Integrated NPN, PNI-NPN), когато се разгръща с нейна поддръжка[2]. Разграничението е по ползване и зависимост, а не по размер на покритието – непубличните мрежи са предназначени за изключително ползване от едно предприятие или държавна организация (Prados-Garzon et al. 2021). Сред тези, които биха имали полза от тях, изрично са посочени и военните бази (Wen et al. 2022).

Локалната 5G мрежа обединява базови станции (gNodeB, gNB), крайни устройства (User Equipment, UE), ядро и приложни сървъри; радиовръзката UE–gNB използва NR (New Radio)[3]. В самостоятелната мрежа цялата 5G система радиодостъпът и ядрото е в логическия периметър на обекта (Wen et al. 2022). Функцията за пренос на потребителските данни (User Plane Function, UPF) се разполага в обекта заедно с изчисленията в периферията на мрежата (edge computing), а управляващите функции на ядрото могат частично да са извън него (Prados-Garzon et al. 2021). При интегрираните варианти обществената мрежа поема общ радиодостъп, управлението или цялата мрежа; колкото по-дълбока е интеграцията, толкова по-ниски са разходите, но и контролът и изолацията (Wen et al. 2022). Насочването на трафика към близка мрежа за данни е стандартен механизъм – ядрото избира UPF близо до устройството (3GPP 2024b, §5.13), а рамката MEC (Multi-access Edge Computing) определя платформа и управление на приложенията близо до достъпа (ETSI 2020).

Услугата от тип локална мрежа (5G LAN-type service) е различна от инфраструктурата: частна комуникация по IP или Ethernet между участниците в 5G виртуална мрежа (5G Virtual Network, 5G VN) (3GPP 2024b, §5.29; Phan et al. 2026). Частната мрежа определя организацията и ползвателите, а LAN-type — предоставяната групова услуга. Трафикът между участниците се препраща през мрежа за данни по референтната точка N6, между от-

делни UPF по N19 или локално в една UPF, когато тя обслужва сесиите на всички участници (3GPP 2024b, §5.29.4). Групата може да обхваща различни клетки и местоположения, затова „LAN-type“ не означава физически малка мрежа. Сесиите за пренос на протоколни единици данни (Protocol Data Unit, PDU) от тип Ethernet пренасят Ethernet кадри, включително на устройства, свързани локално към терминала (3GPP 2024b, §5.6.10.2). Фигура 1 показва пътя на полезните данни при обща UPF, без пълната сигнализация.

За индустриалните мрежи 5G системата се интегрира с TSN (Time-Sensitive Networking) като логически мост, чиито входове и изходи се осигуряват от преобразуватели от страната на устройството и на мрежата (DS-TT и NW-TT)[4]. Локалните и частните 5G мрежи все още са в начален етап (Wen et al. 2022). Самостоятелните изискват високи капиталови и експлоатационни разходи, докато интегрираните снижават прага за навлизане (Prados-Garzon et al. 2021). Практическото внедряване на LAN-type услугата също се оценява като ограничено (Phan et al. 2026). Така локалната мрежа върху 5G е съществуваща архитектура, а локалността на функциите, поддръжката на Ethernet и груповите услуги се оценяват поотделно, вместо да се приписват на бъдещото поколение.



Фигура 1. 5G LAN-type услуга при обща UPF

3. Особености и архитектура на 6G LAN

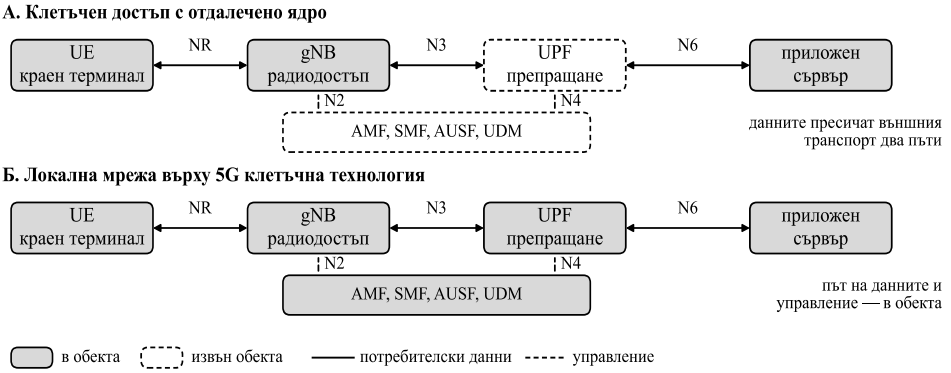
Под 6G LAN се разбира локална мрежа, изградена с технологиите на шестото поколение, която обслужва ограничено пространство или конкретен обект – производствен участък, кампус, сграда или превозно средство. Тя се разграничава от широкообхватната обществена мрежа, която покрива градове и региони и обслужва подвижни потребители. Функционално 6G LAN е най-близо до днешните частни 5G мрежи, но е предназначена

за по-строги изисквания към закъснението, детерминираността и скоростта на предаване. Такива мрежи обединяват подмрежи с различни спектър, обхват и услуги в потребителски, индустриални, офисни и автомобилни приложения и съществуват съвместно с обществените мрежи, което може да наложи и нова регулация[5].

Най-разработената форма на тази идея са подмрежите in-X (in-X subnetworks), при които „X“ означава обекта, в който е разположена клетката – производствен модул, робот, превозно средство, сграда или дори човешкото тяло. Това са маломощни клетки с малък обхват за услуги, които досега разчитат на кабелни връзки и могат да бъдат критични за живота (Berardinelli et al. 2021). Голяма част от трафика им не напуска обекта – контролерът, сензорите и изпълнителните механизми обменят данни локално, а към широката мрежа отиват обобщена информация и управление. В архитектурните разработки на проекта 6G-SHINE[6] подмрежата е описана чрез роли за управление на подмрежата, радиоресурсите, изчислителните задачи и шлюзовата свързаност. Тя се разглежда като организирано цяло със собствени вътрешни взаимодействия и връзки към външната среда, а не като клетка с намален радиус.

Кое прави една локална мрежа „6G“ не е еднозначно определено. Сред обсъжданите технологии са обхватите sub-THz и THz за къси връзки, изчисленията в периферията на мрежата (edge computing) и изкуственият интелект за управление на ресурсите[7], както и интегрираните комуникации и сензорика (ISAC), въведени в рамката IMT-2030[8]. Нито една от тези технологии обаче не е задължителен признак. Затова 6G LAN е по-скоро изследователска категория, отколкото отделен вид мрежа със собствена спецификация. Тя обединява развитието на непубличните мрежи и на услугата 5G LAN-type, подмрежите in-X, локалната обработка и включването им в по-широка „мрежа от мрежи“[9].

За съпоставката се използват три референтни конфигурации: А – клетъчен достъп с отдалечено ядро; Б – частна 5G мрежа с локално ядро; В – локална подмрежа по концепцията 6G LAN. „Локално“ означава вътре в експлоатационната граница на един обект. За А и Б се разглежда една и съща услуга на сървър в обекта, така че разликите да идват от маршрута на данните, а не от мястото на приложението. Фигура 2 показва местата на функциите и пътищата на данните в конфигурации А и Б. Интерфейсите N2 (gNB–AMF) и N4 (SMF–UPF) пренасят управление, а N3 (gNB–UPF) и N6 – потребителски данни.



Фигура 2. Път на данните и места на управлението в две съпоставими реализации

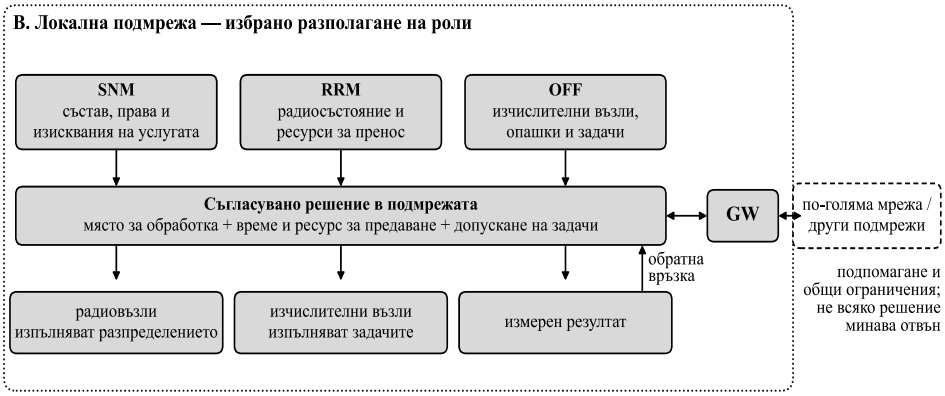
При конфигурация А крайното устройство UE и базовата станция gNB са в обекта, а UPF и основните управляващи функции са извън него – функцията за управление на достъпа и мобилността (Access and Mobility Management Function, AMF), функцията за управление на сесиите (Session Management Function, SMF), сървърната функция за удостоверяване (Authentication Server Function, AUSF) и функцията за унифицирано управление на данните (Unified Data Management, UDM)[10]. Трафикът от терминала излиза през отдалечената UPF и се връща в обекта към локалния сървър. Разпределянето на радиоресурсите остава в gNB и не се извършва от ядрото за всеки пакет[11]. Предимството на А е споделената инфраструктура и централизираното обслужване на много обекти, а ограничението за локалната услуга е външният участък в пътя на данните.

При конфигурация Б базовата станция, ядрото, абонатните данни и приложният сървър са в обекта. Това е локална мрежа върху 5G, независимо дали е активирана LAN-type услугата. Радиопротоколите са същите като при А, но полезният трафик и управлението не напускат локалната граница. Ethernet интеграцията се проверява отделно[12]. Конфигурация Б е практически наличната основа за сравнение с В (Prados-Garzon et al. 2021).

Между А и Б има важен междинен вариант – локална UPF при отдалечени управляващи функции. Тогава данните остават в обекта, но някои операции продължават да изискват външното ядро. Затова локалният път на данните не е достатъчен критерий за локална автономност.

Конфигурация В използва логическите роли от архитектурата на 6G-SHINE, без да ги отъждествява с отделни устройства – управление на

подмрежата (Subnetwork Management, SNM), управление на радиоресурсите (Radio Resource Management, RRM), прехвърляне на изчислителни задачи (Compute Offloading, OFF) и шлюзова свързаност (Gateway, GW). Ролите могат да се изпълняват от един или от няколко възела. Фигура 3 представя информационните зависимости, необходими за съгласуването им в подмрежата.



Фигура 3. Модел на конфигурация В с локални роли

Подмрежата е единица за съгласуване на локалната услуга, наличните ресурси и външните взаимодействия. Ролите обменят състояние и решения, без това да налага един централен контролер или пълна децентрализация. Блокът за съгласувано решение на фигурата означава именно това взаимодействие, а не стандартизирана 6G функция. Сходен управляващ слой може да се развие и над Б, затова за В е съществено доколко тези взаимодействия са последователно организирани и какъв резултат дават при съпоставими ресурси.

4. Сравнителен анализ на архитектурните възможности

При еднакви устройства, трафик и приложна задача сравнението трябва да отделя влиянието на широчината на канала, радиосредата, мощността и изчислителната производителност. При услуга „заявка–обработка–отговор“ общото време включва доставката на заявката и отговора, изчакването пред изчислителния ресурс и самото изпълнение на задачата. Преминаването от А към Б или В отстранява отдалечения участък от комуникационния път и може да намали транспортното закъснение, но пре-

товарен локален сървър може да изгуби спечеленото с по-дълго изчакване или изпълнение. Между Б и В този ефект не е предварително установен, защото и двете вече могат да имат локален път. Следователно локализацията трябва да се отчита за отделен механизъм, а не като доказателство за ново поколение.

Съвместното разполагане на сървър и радиодостъп не означава съвместно управление. Ако задачата закъснява поради изчислителна опашка, допълнителен радиоресурс не отстранява причината. Решението трябва да отчита свободния процесорен ресурс, размера и крайния срок на задачата и състоянието на връзките, за да се съгласуват допускането на задачи, мястото на обработка и моментите на предаване. MEC архитектурата вече включва управление на приложения и ресурси[13], а в архитектурата на 6G-SHINE са изследвани взаимодействия на равнище подмрежа. Перспективата при В е по-добро съгласуване на преноса и обработката или по-проста интеграция при еднакви ресурси. За това са необходими актуални измервания, съвместими описания на задачите и управляващи решения, които въздействат едновременно върху комуникацията и изчисленията.

Радиовръзките на малки разстояния позволяват пространствено повторно използване на спектъра, но с броя на подмрежите растат взаимните смущения (Berardinelli et al. 2021). В проекта 6G-SHINE[14] чрез симулации са оценени централизирани и разпределени методи за честотно разпределение и управление на мощността. Резултатите подкрепят развитието на алгоритми при конкретните допускания, но не доказват общо превъзходство спрямо частна 5G мрежа. Сравнението трябва да разглежда кой разполага с информация за съседите, как се договарят ограниченията и колко служебен обмен струва координацията.

Агрегирането на устройства в подмрежа може да намали подробността на информацията към външната мрежа, но не премахва вътрешната координация. По-малкият външен служебен обмен не означава по-малък общ обмен, защото към него се добавят вътрешната координация и поддържането на съгласувано състояние. Управляваната група с шлюз не е изцяло нова идея – в Release 18 е определена поддръжка на персонални мрежи от устройства на интернет на нещата (Internet of Things, IoT), означавани като Personal IoT Network (PIN), включително управляващи и шлюзови роли[15]. При Б и В трябва да се различават продължаването на установен трафик, новото удостоверяване и възстановяването след отказ. Автономност за дадена операция има само когато нужните функции, ключове, състояние и

ресурси са достъпни локално, а съсредоточаването им в един координатор може да създаде единична точка на отказ.

Локалният път намалява участието на външни компоненти в преноса, но сигурността зависи и от удостоверяването, защитата на данните и управлението на правата. Общото управление на комуникация и изчисления добавя интерфейси и правомощия, които също трябва да се защитят. За В важен въпрос е съвместимостта на взаимодействията между ролите, защото нестандартизираните решения увеличават зависимостта от конкретна реализация.

5. Перспективи за развитие и приложимост

Перспективите на 6G LAN трябва да се търсят в съчетаването на архитектурни механизми, а не в едно изолирано свойство като малък обхват или локален сървър. Таблица 1 обобщава условията, при които конфигурация В би могла да даде допълнителна стойност; оценката е качествена и не е измерено класиране на технологии.

Таблица 1. Условия за потенциални предимства на конфигурация В спрямо архитектурните алтернативи

Проверяван ефект	***Спрямо А***	***Спрямо Б***	***Необходима проверка***
По-кратък път на данните	Възможен чрез отпадане на външния транспорт	Не е отличителен – пътят вече може да е локален	Общото време, включително опашките и изчисленията
Съгласувано управление	Не следва само от локализацията	Потенциален ефект; възможен и чрез разширения	Обща цел, актуални измервания и цена на интеграцията
Координация на подмрежи	Може да намали зависимостта от отдалечени решения	Няма предварително доказано превъзходство	Еднакъв спектър, трафик и отчетен служебен обмен
Работа без външна връзка	Разлика за избраните в А пътища и операции	Не е отличителна при локално обезпечени функции	Достъпност на права, ключове, състояние и резерви
По-ниска сложност и разходи	Не следва от по-малкия обхват	Не е установена без конкретни реализации	Компоненти, експлоатация, резервиране и съвместимост

Една възможна посока е постепенното развитие върху съществуващите локални 5G системи, в които локалният пренос, частната организация и близката обработка вече имат технологична основа[16,17]. Към тях могат да се добавят взаимодействия за управление на подмрежата, без да се подменят едновременно всички компоненти, като ефектите от разполагането, от съгласуването и от промените в радиоинтерфейса се оценяват поотделно.

Друго направление е организирането на локалната система около изискванията на услугата. Когато преносът и обработката споделят общ времеви бюджет, решенията за достъп до радиосредата, разполагане на задачите и използване на изчислителни ресурси могат да се съгласуват. Архитектурните предложения на 6G-SHINE дават основа за такова изследване. Ползата зависи от актуалността на информацията и от разхода за координация, а при обикновен локален достъп допълнителният управляващ слой може да е излишен. Трето направление са взаимодействията между подмрежи, които в ограничено пространство трябва да съгласуват ресурсите си, без да губят самостоятелността на вътрешните си услуги. Това насочва вниманието към интерфейсите, обмена на състояние и разпределянето на отговорностите между локалното и външното управление.

Приложимостта е най-голяма там, където локалният обмен е част от общ процес на измерване, обработка и действие. Индустриалните приложения с определени времеви изисквания дават установена основа за анализ[18] (Prados-Garzon et al. 2021), а в отбраната и сигурността стационарните и развръщаемите информационни среди (Ivanov 2026) поставят допълнителни изисквания към границите на доверие и външните зависимости. Практическата оценка на тези перспективи изисква симулации и експерименти при съпоставими условия, включително при прекъсвания и откази. Настоящият анализ определя архитектурните зависимости за такава проверка и не представя измерени показатели за закъснение, надеждност, енергопотребление или разходи.

6. Заключение

6G LAN очертава направление за развитие на локалните безжични мрежи чрез организацията на локалните функции и взаимодействието им с по-широката среда. Локалните 5G системи със собствен радиодостъп и ядро вече съществуват и не се свеждат до LAN-type услугата, чието внедряване е ограничено. Те показват, че локалният обмен, близката обработка и самостоятелното управление не са изключителни свойства на

бъдещото поколение. Перспективите на 6G LAN са в съгласуването на комуникацията и изчисленията, управлението според услугите и взаимодействието между подмрежи. Реализирането им зависи от съвместимостта на функциите, сложността на управлението и доказуемата полза при конкретни условия, която трябва да се установи чрез съпоставка с локалните 5G системи.

БЕЛЕЖКИ

1. 3GPP, 2026. *Release 21*. 3GPP. Page updated after the June 2026 TSG plenaries. Available from: https://www.3gpp.org/specifications-technologies/releases/release-21.

2. 3GPP, 2024b. *System architecture for the 5G System (5GS)*. TS 23.501 V18.6.0, Release 18. ETSI TS 123 501, July 2024. ETSI. Available from: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/18.06.00_60/ts_123501v180600p.pdf.

3. 3GPP, 2025. *NR; NR and NG-RAN Overall description; Stage-2*. TS 38.300 V18.5.0, Release 18. ETSI TS 138 300, April 2025. ETSI. Available from: https://www.etsi.org/deliver/etsi_ts/138300_138399/138300/18.05.00_60/ts_138300v180500p.pdf.

4. 3GPP, 2024b....

5. IEEE COMMUNICATIONS SOCIETY, 2025. *6G Local Area Networks*. Call for papers, special issue of IEEE Wireless Communications. Available from: https://www.comsoc.org/publications/magazines/ieee-wireless-communications/cfp/6g-local-area-networks.

6. 6G-SHINE, 2025b. *In-X Subnetwork Architectures and Integration into 6G "Networks of Networks"*. Deliverable D2.4, V1.0, 28 February 2025. Available from: https://6gshine.eu/wp-content/uploads/2025/02/6GSHINE_D2.4_Deliverable_v1.0_Disclaimer.pdf.

7. IEEE COMMUNICATIONS SOCIETY, 2025…

8. ITU-R, 2023. *Framework and overall objectives of the future development of IMT for 2030 and beyond*. Recommendation ITU-R M.2160-0. Geneva: ITU. Available from: https://www.itu.int/rec/R-REC-M.2160-0-202311-I/en.

9. 6G-SHINE, 2025b…

10. 3GPP, 2024b…

11. 3GPP, 2025…

12. 3GPP, 2024b…

13. ETSI, 2020. *Multi-access Edge Computing (MEC); Framework and Reference Architecture*. ETSI GS MEC 003 V2.2.1, December 2020. ETSI. Available from: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/02.02.01_60/gs_MEC003v020201p.pdf.

14. 6G-SHINE, 2025a. *Final Results on the Management of Radio Resources in Subnetworks in the Presence of Legitimate and Malicious Interferers*. Deliverable D4.3, V1.0, 30 June 2025. Available from: https://6gshine.eu/wp-content/uploads/2025/11/D4.3_Final-results-on-the-management-of-radio-resources-in-subnetworks_v1.0.pdf.

15. 3GPP, 2024a. *Application layer support for Personal IoT Network*. TS 23.542 V18.3.0, Release 18. ETSI TS 123 542, April 2024. ETSI. Available from: https://www.etsi.org/deliver/etsi_ts/123500_123599/123542/18.03.00_60/ts_123542v180300p.pdf.

16. ETSI, 2020…

17. 3GPP, 2024b…

18. 3GPP, 2024b…

REFERENCES

BERARDINELLI, G.; BARACCA, P.; ADEOGUN, R. O. et al., 2021. Extreme Communication in 6G: Vision and Challenges for "in-X" Subnetworks. *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2516 – 2535. DOI: 10.1109/OJCOMS.2021.3121530.

GOLDSMITH, A., 2005. *Wireless Communications*. Cambridge: Cambridge University Press.

IVANOV, I., 2026. 6G Technology for Military Communications (IMT-2030). In: *Godishna universitetska nauchna konferentsia*, [15-16 Oct. 2026]. Veliko Tarnovo: NVU „Vasil Levski".

PHAN, L.-A.; PESCH, D.; ROEDIG, U. & SREENAN, C. J., 2026. The Future of Industrial Connectivity: The 5G LAN-Type Service. *IT Professional*, vol. 28, no 2, pp. 76 – 82. DOI: 10.1109/MITP.2026.3652039.

PRADOS-GARZON, J.; AMEIGEIRAS, P.; ORDONEZ-LUCENA, J.; MUÑOZ, P.; ADAMUZ-HINOJOSA, O. & CAMPS-MUR, D., 2021. 5G Non-Public Networks: Standardization, Architectures and Challenges. *IEEE Access*, vol. 9, pp. 153893 – 153908. DOI: 10.1109/ACCESS.2021.3127482.

WEN, M.; LI, Q.; KIM, K. J.; LÓPEZ-PÉREZ, D.; DOBRE, O.A.; POOR, H.V.; POPOVSKI, P. & TSIFTSIS, T.A., 2022. Private 5G Networks: Concepts, Architectures, and Research Landscape. *IEEE Journal of Selected Topics in Signal Processing*, vol. 16, no 1, pp. 7 – 25. DOI: 10.1109/JSTSP.2021.3137669.

LOCAL WIRELESS NETWORKS BASED ON TECHNOLOGIES OF SIXTH-GENERATION CELLULAR SYSTEMS (6G LAN): FEATURES, ARCHITECTURE AND PROSPECTS

Abstract. The paper examines the development of local wireless networks in the context of sixth-generation cellular communications. It presents the concept of 6G local area networks (6G LAN), its distinctive features, and the main architectural approaches. A comparison with existing local cellular solutions clarifies both continuity with established technologies and possible changes in the organization of local communication. The prospects for closer integration of communication, information processing, and service delivery are discussed, together with the prerequisites and limitations for their practical implementation. The analysis

outlines development directions for 6G LAN in which architectural choices are assessed against application requirements and operating conditions.

Keywords: 6G; local wireless networks; 6G LAN; cellular communications; non-public networks; network architecture.

Dr. Ivan Ivanov, Assoc. Prof.
ORCID iD: 0009-0002-1304-1306
Defence Institute “Professor Tsvetan Lazarov”
2, Professor Tsvetan Lazarov Blvd.
1592 Sofia, Bulgaria
E-mail: i.p.ivanov@di.mod.bg

Dr. Alexander Kolev, Assoc. Prof.
ORCID iD: 0000-0002-9211-2717
Defence Institute “Professor Tsvetan Lazarov”
2, Professor Tsvetan Lazarov Blvd.
1592 Sofia, Bulgaria
E-mail: a.kolev@di.mod.bg

Colonel Dr. Ivan Chakarov, Assoc. Prof.
ORCID iD: 0000-0002-6062-4806
Command and Staff Faculty
Rakovski National Defence College
82, Evlogi i Hristo Georgievi Blvd.
1504 Sofia, Bulgaria
E-mail: i.chakarov@rndc.bg

https://doi.org/10. 66334/annu26_publicpriv

ПУБЛИЧНО-ЧАСТНО ПАРТНЬОРСТВО ПРИ ЗАЩИТАТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА: СРАВНИТЕЛЕН АНАЛИЗ И ПРЕДЛОЖЕНИЯ ЗА НОРМАТИВНО РЕГУЛИРАНЕ В РЕПУБЛИКА БЪЛГАРИЯ

Иван Кутелов
Военна академия „Георги Стойков Раковски“

Абстракт. Докладът анализира публично-частното партньорство като инструмент за защита на критичната инфраструктура в условията на преобладаваща частна собственост върху стратегическите сектори. На базата на сравнителен анализ на моделите на Съединените американски щати (CISA, ISACs, NSM-22) и на Федерална република Германия (BSI и BBK, KRITIS-DachG, UP KRITIS) се доказва, че оптималният подход е хибриден – комбинация от минимални задължителни стандарти, стимули и институционализирано сътрудничество. За България се идентифицират системни дефицити: фрагментирана нормативна рамка, липса на национален координатор и на механизми за информационно споделяне, както и нетранспонирана Директива за устойчивост на критичните субекти, поради което страната е изправена пред Съда на Европейския съюз. Формулират се предложения

за законодателна реформа, единен координационен орган и секторни центрове за споделяне на информация.

Ключови думи: публично-частно партньорство; критична инфраструктура; национална сигурност; нормативна уредба; информационно споделяне; хибриден модел

I. Увод

Защитата на критичната инфраструктура (КИ) е един от фундаментите на националната сигурност, а нейното нарушаване – вследствие на кибератаки, физически диверсии или природни бедствия – може да предизвика каскадни негативни ефекти върху икономиката, държавното управление и обществената безопасност. Особеност на българския контекст е, че над 90% от бизнеса, включително стратегически активи в комуникациите, енергетиката и комуналните услуги, е в частни ръце. Държавата обаче все още не разполага със специализиран закон за защита на КИ, нито с изградени оперативни платформи за сътрудничество с частните оператори – състояние, определяно от експертите като своеобразен „сигурностен вакуум“[1, 2].

Настоящият доклад си поставя за цел да анализира приложимостта и потенциала на публично-частното партньорство (ПЧП) при защитата на КИ в Република България. На основата на сравнителен институционален анализ на утвърдените и действащи модели в САЩ и Германия се извеждат ключовите уроци за българската практика и се формулират конкретни предложения за изграждане на устойчив хибриден модел за сигурност. Изследването се базира на детайлен преглед на националното и международното законодателство, официалните държавни стратегически документи и съвременни научни изследвания в областта на критичната устойчивост.

II. Теоретични основи на публично-частното партньорство

2.1. Икономическа обоснованост

Необходимостта от публично-частно партньорство при защитата на критичната инфраструктура произтича пряко от публичния характер на сигурността като стока. Сигурността за частните компании се възприема основно като разход, което я прави неконкурентна. Това, по своята същност, поражда класическия пазарен дефект, известен като проблема на „свободния ездач“. Преодоляването на тази бариера пред колективното действие

изисква специфични институционални решения, които да противодействат на естественото подинвестиране в сигурност от страна на частните субекти (Samuelson 1954; Olson 1965).

В киберсигурността тези проблеми се задълбочават допълнително от информационната асиметрия и наличието на положителни външни ефекти, които свободният пазар не може самостоятелно да усвои. Държавата не разполага с целия необходим финансов и оперативен ресурс да действа напълно самостоятелно, докато частният сектор няма достатъчно икономически стимули да поеме цялата тежест по осигуряване на колективната устойчивост. Поради това ПЧП се налага като обективна функционална необходимост, при която водещият научен и практически въпрос е как именно да бъде структурирано това взаимодействие.

В българската научна литература същата теоретична логика е развита в контекста на противодействието на съвременните хибридни заплахи. Както посочва Стоилов, асиметричният характер на тези заплахи изисква разширяване на обхвата от държавни и надкорпоративни инструменти: *Самият характер на заплахата обаче изисква по-широк обхват от инструменти като добре обучена полиция, функциониращ граничен контрол, ефективни антикорупционни агенции и прозрачност в енергийния сектор и финансирането на партиите* (Stoilov 2015, p. 65).

Защитата на КИ по своята сложност надхвърля капацитета на който и да е изолиран държавен орган и изисква изграждането на дългосрочно, нормативно закрепено сътрудничество с частните оператори.

2.2. Модели на публично-частното партньорство и хибридния подход

Европейската агенция за киберсигурност (ENISA) класифицира четири основни модела за реализиране на ПЧП в сектора на сигурността[3]:

• *Институционален модел* – основан на изграждането на общи съвместни структури (като агенцията RIA в Естония или RCB в Полша);

• *Оперативен модел* – изграден около съвместни оперативни дейности и реакция при конкретни кризисни казуси;

• *Финансов модел* – базиран на споделено или съвместно финансиране;

• *Информационен модел* – фокусиран върху организиран обмен на информация за заплахи и уязвимости (какъвто е моделът на секторните центрове ISACs в САЩ).

Практическият опит показва, че разчитането на чисто доброволни партньорства не генерира задоволителни нива на защита. Този извод се

потвърждава изрично в Националната стратегия за киберсигурност на САЩ от 2023 г., където се отчита, че пазарът не успява да стимулира и възнагради в достатъчна степен операторите, инвестиращи в проактивна колективна сигурност[4]. В резултат на това за най-ефективно съвременно решение се приема хибридният модел, който ефективно съчетава въвеждането на минимални задължителни стандарти със система от стимули и институционализирано сътрудничество.

Методологическа основа за подобен трансфер и взаимодействие е общността на управленските принципи, валидни и за двата сектора: *Управлението на една организация представлява сложна и отговорна дейност, независимо от това дали тази организация е държавна или частна, военна или гражданска, малка, средна или голяма, дали е създадена със стопанска или нестопанска цел* (Stoilov 2022, p. 14).

Тази универсална общност на управленските принципи прави изграждането на хибридни модели за взаимодействие между държавните органи и частния бизнес напълно постижимо в организационно отношение

III. Състояние и дефицити на българския модел

3.1. Фрагментирана нормативна и институционална рамка

Отменението през 2009 г. Закон за управление при кризи възлагаше на Министерския съвет приемането на Национална програма за защита на КИ, но не определяше конкретен орган за оперативна координация с частните оператори. Понастоящем рамковото регулиране се съдържа в Закона за защита при бедствия(ЗЗБ)[5] (Stoyanov 2025). Наредба № 256 от 2012 г. (издадена на основание чл. 8а от ЗЗБ) изцяло възлага оценката на риска на самите оператори, без да въвежда общи задължителни стандарти или работещ санкционен механизъм[6] (Stoyanov 2025). Единствената всеобхватна секторна наредба[7] има силно ограничен териториален и функционален обхват, тъй като регулира единствено физическата сигурност в банковия сектор (Stoyanov 2025).

През февруари 2026 г. България транспонира европейската Директива NIS2 чрез ключови изменения в Закона за киберсигурност, въвеждайки задължително докладване на инциденти и доброволни механизми за споделяне на информация[8, 9]. Директивата за устойчивост на критичните субекти (CER) обаче все още не е транспонирана в националното ни законодателство. Поради това забавяне на 29 април 2026 г. Европейската комисия официално сезира Съда на ЕС по дело INFR(2024)0258[10]. В същото време подготвеният от Министерство на вътрешните работи (МВР) проект на За-

кон за устойчивост на критичните субекти (ЗУКС) все още се намира на етап обсъждане и не е приет от законодателния орган[11].

В България функциите по защита на КИ са силно разпръснати и разпределени между Министерството на иновациите и дигиталната трансформация (което от май 2026 г. е официален правоприемник на Министерството на електронното управление), Държавна агенция „Национална сигурност“, МВР и отделните секторни регулатори. Към момента нито една държавна институция не притежава ясен и цялостен правен мандат за секторна координация[12]. Докато САЩ разполагат с единен оперативен координатор в лицето на CISA, а Германия прилага доказана двустълбова институционална архитектура (BSI за киберсигурност и BBK за физическа устойчивост), в България отсъства национален оперативен център за контакт и координация с частните оператори.

3.2. Правни, икономически и поведенчески бариери

Специфика на националния контекст е, че ключови стратегически сектори у нас са чуждестранна собственост. Две от трите електроразпределителни дружества са собственост на големи чуждестранни инвеститори, а третото премина под контрола на български холдинг едва през 2021 г. Липсата на ефективни правни лостове за въздействие върху частните собственици е детайлно анализирана от д-р Бойко Митев, председател на Българската асоциация „Корпоративна сигурност“ (БАКС):

...всяка компания се оправя сама за себе си и между тях няма взаимодействие, поради което се явява спешно необходимо изграждането на „надкорпоративно, национално равнище на управление на кризисни ситуации и сигурност[13].

Бариерите пред ефективното партньорство обаче не са единствено от нормативен характер. Липсата на изградено взаимно доверие между държавните органи и частния бизнес (Mladenova 2024) е трайно идентифицирана в редица международни емпирични изследвания: 40% от анкетираните организации посочват именно „установяването на доверие“ като най-съществена бариера пред партньорството, а 20% отчитат липсата на реципрочност от страна на държавата (Koepke 2017). Доверието при споделяне на информация за заплахи задължително трябва да бъде двупосочен процес. Дори въвеждането на законови гаранции няма да стимулира реалния обмен на данни, ако регулациите не адресират директно страховете на бизнеса от репутационни вреди и загуба на пазарен дял[14].

IV. Сравнителен анализ на моделите на САЩ и Германия

4.1. Моделът на САЩ

Американският модел за защита на критичната инфраструктура е изграден върху концепцията за задължителна и централизирана институционална координация. Ключовият орган (Агенцията за киберсигурност и сигурност на инфраструктурата (CISA) е създаден със закон през 2018 г.[15]. С приемането на Националния меморандум за сигурност NSM-22 от 30 април 2024 г. CISA се утвърждава като национален оперативен координатор за цялата КИ, като успоредно с това се определят конкретни държавни ведомства като Агенции за управление на секторния риск (SRMA) за всеки от 16-те идентифицирани критични сектора[16, 17].

Информационният обмен с бизнеса е институционализиран чрез мрежа от над 23 секторни центъра за споделяне и анализ на информация (ISACs), създадени въз основа на препоръките на Президентската комисия PCCIP и Директива PDD-63, които днес са обединени в Национален съвет на ISACs[18, 19, 20]. От 2023 г. насам САЩ плавно преминават от чисто доброволно сътрудничество към регулиран модел с минимални задължителни изисквания за устойчивост[21]. Законът CIRCIA от 2022 г. въвежда строго задължение за операторите да докладват за значими киберинциденти на държавните органи в рамките на 72 часа[22]. Тези реформи отразяват официалните констатации на комисията CSC 2.0, според които доброволните партньорства не генерират достатъчни нива на национална защита и сигурността изисква целенасочена комбинация от строга регулация, финансови стимули и съвместни оперативни процеси[23].

4.2. Моделът на Германия

Във Федерална република Германия се изгражда стабилна и ефективна двустълбова институционална архитектура. Федералната служба за информационна сигурност (BSI) отговаря пряко за киберсигурността, докато Федералната служба за гражданска защита и помощ при бедствия (BBK) поема контрола над физическата устойчивост на критичните обекти в съответствие с новия закон за КИ (KRITIS-Dachgesetz), влязъл в сила на 17 март 2026 г.[24, 25].

Новия закон задължава операторите на критични съоръжения периодично да провеждат всеобхватни анализи на риска под прекия надзор на BBK, въвежда лична отговорност за ръководните кадри при неизпълнение на мерките (§ 20) и предвижда строги административни санкции, достигащи до 1 млн. евро при сериозни системни нарушения (§ 24)[26, 27]. Паралелно

с тези регулации, в страната успешно функционират утвърдени доброволни структури: публично-частната платформа UP KRITIS (създадена през 2007 г.), която към 2024 г. обединява над 900 държавни и частни членове[28, 29], и германският Алианс за киберсигурност, чиито участници надхвърлят 8800 организации към 2026 г.[30].

4.3. Уроци за България

Задълбоченото сравнение на американския и германския подход позволява извеждането на три ключови извода, които да послужат като основа за българските реформи:

1. Баланс между задължение и партньорство. И двата модела показват, че успешната защита на КИ е невъзможна без прецизен баланс – съчетаване на минимални задължителни държавни стандарти с гъвкави, работещи доброволни платформи за оперативна подкрепа.

2. Нужда от единен координатор. Наличието на централизиран национален орган е задължително условие за оперативна съвместимост, бърз обмен на данни за заплахи и преодоляване на междуведомствената фрагментация.

3. Правни гаранции за обмен на данни. Информационното споделяне изисква сигурна правна рамка и дългосрочно доверие. Важността на този урок се доказва от сериозния дебат около изтичането на законовите срокове на Закона за споделяне на информация за киберсигурност (CISA 2015) в САЩ през септември 2025 г.[31].

За България, която вече направи първата крачка със задължителното транспониране на Директива NIS2 чрез измененията в Закона за киберсигурност, следващата логична стъпка е да надгради тази нормативна база с реални, законово гарантирани механизми за практическо сътрудничество и обмен на информация.

V. Предложения за изграждане на хибриден модел в България

5.1. Основни мерки за нормативно и институционално изграждане

На базата на направения сравнителен анализ и идентифицираните системни дефицити в нормативната и институционална рамка за защита на КИ се налага като най-подходящо въвеждането на четири ключови мерки за изграждане на устойчив хибриден модел в Република България:

1. Приемане на специален Закон за устойчивост на критичните субекти. Този нормативен акт трябва да стъпи върху разработения от МВР проект от 2025 г., като напълно и прецизно транспонира изискванията на

европейската Директива CER[32, 33]. Законът следва да въведе ясни, минимални задължителни стандарти за физическа сигурност и киберзащита, съчетани с прецизна система от административни санкции при неспазване на предписанията (по образеца на германския KRITIS-DachG).

2. Създаване на единен Национален оперативен координатор за КИ. Необходимо е изграждането на централизиран държавен орган (агенция или център), който да консолидира фрагментираните към момента ведомствени функции и да служи като единна точка за контакт и оперативна съвместимост за всички частни и държавни оператори (по примера на американската CISA).

3. Институционализиране на секторни центрове за обмен на информация (ISACs). Предлага се изграждането на защитени секторни платформи за двупосочно споделяне на данни за заплахи и уязвимости. Изключително важно е законът да предостави ясни правни защити за споделящите субекти – включително ограничаване на гражданската отговорност при споделяне на информация „при добра съвест“ и категорични гаранции за защита на търговската тайна и конкурентно чувствителните данни. Без тези нормативни гаранции е невъзможно да се преодолеят страховете на бизнеса от репутационни щети и да се изгради необходимото доверие[34] (Koepke 2017).

4. Въвеждане на икономически стимули за инвестиции в сигурността. Държавата трябва да подкрепи частните оператори чрез механизми – като данъчни облекчения за сертифицирани инвестиции в сигурност и въвеждане на задължителни изисквания за устойчивост на веригата за доставки в процедурите за публични поръчки.

5.2. Правна допустимост на договорния модел на публично-частното партньорство

Българското право вече е съдържало успешен прецедент за допускане на частни субекти до управлението и изпълнението на функции, които традиционно се приемат за изключителен прерогатив на държавата. По повод приемането на Закона за публично-частното партньорство от 2013 г., който впоследствие беше отменен, авторите Симеонов и Стоилов констатират: *С този изцяло нов за страната нормативен акт се създава юридическа възможност търговски дружества да бъдат допуснати до управлението и стопанисването на места за лишаване от свобода, социални домове и други подобни институции, които до момента са изцяло под контрола на държавните органи. В основата на сътрудничеството между държава-*

та и частните субекти е договор за публично-частно партньорство, чиито параметри Законът определя (Simeonov & Stoilov 2019, p. 88).

От 03.09.2026 г. Министерството на икономиката, инвестициите и индустрията е публикувало за обществени консултации законопроект, който има за цел да създаде единна национална политика за публично-частните партньорства и да определи правилата за сътрудничество между публичен партньор и частен партньор в рамките публично-частното партньорство.

Следователно пренасянето и разширяването на тази договорна рамка към ПЧП в областта на защитата на критичната инфраструктура е изцяло въпрос на политическа воля и последващо нормативно оформление, а не на принципна или непреодолима конституционно-правна пречка у нас.

VI. Заключение

Настоящият доклад показва по категоричен начин, че публично-частното партньорство не е просто алтернативна стратегия, а обективна функционална необходимост за гарантиране на сигурността на критичната инфраструктура, чиито основни стратегически активи днес са концентрирани в частния сектор. Проведеният сравнителен институционален анализ на моделите на САЩ и Германия показва, че високи нива на национална устойчивост се постигат единствено чрез балансирано съчетаване на задължителни минимални стандарти за сигурност, дефиниране на единен национален оперативен координатор и изграждане на институционализирани платформи за обмен на информация, които се базират на ясни правни гаранции за бизнеса и взаимно дългосрочно доверие[35, 36] (Koepke 2017).

За преодоляване на системните дефицити и премахване на съществуващия „сигурностен вакуум“ у нас се предлага изграждането на цялостен национален хибриден модел за сигурност. Реализирането му изисква спешното приемане на специален Закон за устойчивост на критичните субекти, определянето на централизиран държавен координационен орган, изграждането на защитени секторни центрове за информационен обмен (ISACs) и въвеждането на пакет от икономически и нормативни стимули за частните оператори. Теоретичните, организационните и управленските предпоставки за тази реформа у нас са детайлно аргументирани и налице. За превръщането им в реална институционална практика обаче е необходима консолидирана държавна политическа воля. Преходът от „споделен риск“ към споделена и правно гарантирана отговорност е единственият път за осигуряване на дългосрочната национална устойчивост и защита на жизненоважните за обществото сектори.

БЕЛЕЖКИ

1. MITEV, B., 2023. Interview for Bloomberg TV Bulgaria, 20 November. [online]. Available from: https://www.bloombergtv.bg/a/19-svetat-e-biznes/124098-balgariya-ima-speshna-nuzhda-ot-zakon-za-zashtita-na-kritichnata-infrastruktura. [Last viewed: 19 July 2026]. [in Bulgarian].

2. PAVLOV, N., 2007. *Analiz na normativnata uredba po zashtita na kritichnata in frastruktura.* [online]. Available from: https://nikipavlov.files.wordpress.com/2011/05/analiz_normativna_uredba_cip_statija_v-final_2007.pdf. [Last viewed: 19 July 2026]. [in Bulgarian].

3. ENISA, 2017. *Public Private Partnerships (PPP): Cooperative Models.* Heraklion: European Union Agency for Network and Information Security. [online]. Available from: https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models. [Last viewed: 19 July 2026].

4. THE WHITE HOUSE, 2023. *National Cybersecurity Strategy.* Washington, DC: The White House, March 2023. [online]. Available from: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. [Last viewed: 19 July 2026].

5. MINISTERSKI SAVET, 2006. Zakon za zashtita pri bedstviya. *Darzhaven vestnik*, br. 102 ot 19.12.2006. [in Bulgarian].

6. NAREDBA № 256, 2012. Naredba za reda, nachina i kompetentnite organi za ustanovyavane na kritichnite infrastrukturi, tyahnata uyazvimost i riskovete za tyah [prieta s RMS № 256 ot 17.10.2012]. *Darzhaven vestnik*, br. 81 ot 23.10.2012. [in Bulgarian].

7. MVR i BNB, 2016. *Naredba № 8121z-444 za organizatsiyata i kontrola po obezpechavaneto na sigurnostta na bankite.* [03 May 2016]. [in Bulgarian].

8. MINISTERSKI SAVET, 2026. Zakon za izmenenie i dopalnenie na Zakona za kibersigurnost. *Darzhaven vestnik*, br. 17 ot 13.02.2026 [v sila ot 17.02.2026]. [in Bulgarian].

9. KINSTELLAR, 2026. Bulgaria‘s long road to NIS2 is over. *Kinstellar*, 17 June [online]. Available from: https://www.kinstellar.com/news-and-insights/detail/4093/bulgarias-long-road-to-nis2-is-over. [Last viewed: 19 July 2026].

10. EUROPEAN COMMISSION, 2026. April infringements package: key decisions (referral to the Court of Justice in case INFR(2024)0258), 29 April 2026. [online]. Available from: https://malta.representation.ec.europa.eu/news/april-infringements-package-key-decisions-2026-04-29_en [last viewed: 19 July 2026].

11. MVR, 2025. *Draft Law on the Resilience of Critical Entities (public consultation 27.05–26.06.2025).* Portal for Public Consultations. [online]. Available from: https://www.strategy.bg/bg/public-consultations/11134. [Last viewed: 19 July 2026]. [in Bulgarian].

12. NATIONAL REVENUE AGENCY, 2024. *Doklad za sastyanieto na natsionalnata sigurnost na Republika Balgariya prez 2024 g.* Sofia: Parliament of the Republic of Bulgaria. [online]. Available from: https://www.parliament.bg/bills/51/51-602-00-7.pdf. [Last viewed: 19 July 2026]. [in Bulgarian].

13. MITEV, B., 2023. Interview for Bloomberg TV Bulgaria, 20 November. [online]. Available from: https://www.bloombergtv.bg/a/19-svetat-e-biznes/124098-balgariya-ima-speshna-nuzhda-ot-zakon-za-zashtita-na-kritichnata-infrastruktura. [Last viewed: 19 July 2026]. [in Bulgarian].

14. CSC 2.0, 2023. *Revising Public-Private Collaboration to Protect U.S. Critical Infrastructure.* Washington, DC: Cyberspace Solarium Commission 2.0. [online]. Available from: https://cybersolarium.org/wp-content/uploads/2023/06/CSC2.0_Report_SRMA.pdf. [Last viewed: 19 July 2026].

15. U.S. CONGRESS, 2018. Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168. [online]. Available from: https://www.congress.gov/bill/115th-congress/house-bill/3359. [Last viewed: 19 July 2026].

16. NDAA FY2021, 2021. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 3288. [online]. Available from: https://www.congress.gov/bill/116th-congress/house-bill/6395. [Last viewed: 19 July 2026].

17. NSM-22, 2024. National Security Memorandum on Critical Infrastructure Security and Resilience. Washington, DC: The White House, 30 April 2024. [online]. Available from: https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/. [Last viewed: 19 July 2026].

18. PCCIP, 1997. *Critical Foundations: Protecting America's Infrastructures.* Washington, DC: President's Commission on Critical Infrastructure Protection, October 1997.

19. PDD-63, 1998. Presidential Decision Directive/NSC-63: Critical Infrastructure Protection. Washington, DC: The White House, 22 May 1998. [online]. Available from: https://irp.fas.org/offdocs/pdd/pdd-63.htm. [Last viewed: 19 July 2026].

20. NCI, n. d. National Council of ISACs: About NCI. [online]. Available from: https://www.nationalisacs.org/about-nci. [Last viewed: 19 July 2026].

21. THE WHITE HOUSE, 2023. *National Cybersecurity Strategy.* Washington, DC: The White House, March 2023. [online]. Available from: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. [Last viewed: 19 July 2026].

22. CIRCIA, 2022. *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, Pub. L. no. 117 – 103, div. Y. [online]. Available from: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-for-critical-infrastructure-act-2022-circia. [Last viewed: 19 July 2026].

23. CSC 2.0, 2023. *Revising Public-Private Collaboration to Protect U.S. Critical Infrastructure.* Washington, DC: Cyberspace Solarium Commission 2.0. [online]. Available from: https://cybersolarium.org/wp-content/uploads/2023/06/CSC2.0_Report_SRMA.pdf. [Last viewed: 19 July 2026].

24. KRITIS-DACHG, 2026. Gesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz), BGBl. 2026 I Nr. 66, in Kraft seit 17.03.2026. [online]. Available from: https://www.gesetze-im-internet.de/kritisdachg/BJNR0420B0026.html. [Last viewed: 19 July 2026].

25. A&O SHEARMAN, 2026. *Germany: New Act transposing NIS2 and CER adopted* [online]. Available from: https://www.aoshearman.com. [Last viewed: 14 July 2026].

26. Ibidem.

27. KRITIS-DACHG, 2026. Gesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz), BGBl. 2026 I Nr. 66, in Kraft seit 17.03.2026. [online]. Available from: https://www.gesetze-im-internet.de/kritisdachg/BJNR0420B0026.html. [Last viewed: 19 July 2026].

28. CIP ASSOCIATION, 2024. Germany‘s critical infrastructure protection (KRITIS). *Critical Infrastructure Protection Association* [online]. Available from: https://www.cip-association.org/germanys-critical-infrastructure-protection-kritis/. [Last viewed: 19 July 2026].

29. BSI, n. d. *UP KRITIS.* Bundesamt für Sicherheit in der Informationstechnik [online]. Available from: https://www.bsi.bund.de/EN/Themen/Regulierte-Wirtschaft/UP-KRITIS/up-kritis_node.html. [Last viewed: 19 July 2026].

30. ALLIANZ FÜR CYBER-SICHERHEIT, 2026. Die Allianz für Cyber-Sicherheit [online]. Available from: https://www.allianz-fuer-cybersicherheit.de/. [Last viewed: 14 July 2026].

31. CYBERSECURITY INFORMATION SHARING ACT, 2015. Pub. L. No. 114 – 113, div. N, 129 Stat. 2936.

32. MVR, 2025. *Draft Law on the Resilience of Critical Entities (public consultation 27.05–26.06.2025).* Portal for Public Consultations. [online]. Available from: https://www.strategy.bg/bg/public-consultations/11134. [Last viewed: 19 July 2026]. [in Bulgarian].

33. EU, 2022. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER Directive). *Official Journal of the European Union*, OJ L 333, pp. 164 – 198. [online]. Available from: https://eur-lex.europa.eu/eli/dir/2022/2557/oj. [Last viewed: 19 July 2026].

34. CSC 2.0, 2023. *Revising Public-Private Collaboration to Protect U.S. Critical Infrastructure.* Washington, DC: Cyberspace Solarium Commission 2.0. [online]. Available from: https://cybersolarium.org/wp-content/uploads/2023/06/CSC2.0_Report_SRMA.pdf. [Last viewed: 19 July 2026].

35. KRITIS-DACHG, 2026. Gesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz), BGBl. 2026 I Nr. 66, in Kraft seit 17.03.2026. [online]. Available from: https://www.gesetze-im-internet.de/kritisdachg/BJNR0420B0026.html. [Last viewed: 19 July 2026].

36. NSM-22, 2024. National Security Memorandum on Critical Infrastructure Security and Resilience. Washington, DC: The White House, 30 April 2024. [online]. Available from: https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/. [Last viewed: 19 July 2026].

37. ASPR, 2016. *Healthcare and Public Health Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan.* Washington, DC: U.S. Department of

Health and Human Services, Office of the Assistant Secretary for Preparedness and Response.

38. BACS, 2010. *Bulgarian Association „Corporate Security"* [online]. Available from: https://bacsbg.com/. [Last viewed: 19 July 2026]. [in Bulgarian].

39. CISA, 2024. *Critical Infrastructure Outreach.* Washington, DC: Cybersecurity and Infrastructure Security Agency. [online]. Available from: https://www.dhs.gov/sites/default/files/2024-12/2024_1023_cisa_critical_infrastructure_outreach.pdf. [Last viewed: 19 July 2026].

40. CISA, 2024. *Joint Cyber Defense Collaborative (JCDC) Fact Sheet.* Washington, DC: Cybersecurity and Infrastructure Security Agency. [online]. Available from: https://www.cisa.gov/sites/default/files/publications/JCDC%20Fact%20Sheet.pdf. [Last viewed: 19 July 2026].

41. CISA, 2025. *JCDC AI Cybersecurity Collaboration Playbook.* Washington, DC: Cybersecurity and Infrastructure Security Agency. [online]. Available from: t tps://www.cisa.gov/sites/default/files/2025-01/JCDC%20AI%20Playbook.pdf. [Last viewed: 19 July 2026].

42. CONSULTANCY.EU, 2023. Vivacom buys Telnet and Networx following Bulgarian antitrust saga. *Consultancy.eu*, 1 September. [online]. Available from: https://www.consultancy.eu/news/9316/vivacom-buys-telnet-and-networx-following-bulgarian-antitrust-saga. [Last viewed: 19 July 2026].

43. CRS, 2026. *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress*, R48878. Washington, DC: Congressional Research Service. [online]. Available from: https://www.congress.gov/crs_external_products/R/PDF/R48878/R48878.2.pdf. [Last viewed: 19 July 2026].

44. CSC 2.0, 2025. *2025 Annual Report on Implementation.* Washington, DC: Cyberspace Solarium Commission 2.0. [online]. Available from: https://cybersolarium.org/annual-assessment/2025-annual-report-on-implementation/. [Last viewed: 19 July 2026].

45. CYBERSECURITY DIVE, 2025. CISA Joint Cyber Defense Collaborative contract lapse. *Cybersecurity Dive*, 15 July. [online]. Available from: https://www.cybersecuritydive.com/news/cisa-joint-cyber-defense-collaborative-contract-lapse/756231/. [Last viewed: 19 July 2026].

46. ENISA, 2018. *Information Sharing and Analysis Centres (ISACs): Cooperative Models.* Heraklion: European Union Agency for Network and Information Security. [online]. Available from: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models. [Last viewed: 19 July 2026].

47. EO 13636, 2013. Executive Order 13636: Improving Critical Infrastructure Cybersecurity. *78 Federal Register 11739*, 19 February 2013.

48. EU, 2016. DIRECTIVE (EU) 2016/1148, 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, OJ L 194, pp. 1 – 30. [online]. Available from: https://eur-lex.europa.eu/eli/dir/2016/1148/oj. [Last viewed: 19 July 2026].

49. EU, 2022. DIRECTIVE (EU) 2022/2555, 2022. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2). *Official*

Journal of the European Union, OJ L 333, pp. 80 – 152. [online]. Available from: https://eur-lex.europa.eu/eli/dir/2022/2555/oj. [Last viewed: 19 July 2026].

50. IISS, 2023. Germany. In: *Cyber Capabilities and National Power: A Net Assessment,* vol. II. London: International Institute for Strategic Studies.

51. MYRA SECURITY, n. d. *BSI and critical infrastructure protection in Germany* [online]. Available from: https://www.myrasecurity.com/de/knowledge-hub/bsi/. [last viewed: 19 July 2026].

52. OSW, 2026. Germany: New law for protection of critical infrastructure. *OSW Analysis*, 4 February 2026. Warsaw: Centre for Eastern Studies.

53. PPD-21, 2013. Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. Washington, DC: The White House, 12 February 2013. [online]. Available from: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. [Last viewed: 19 July 2026].

54. SCHOENHERR, 2026. Bulgaria implements NIS 2 Directive: Key changes to the Cybersecurity Act. *Schoenherr*, 18 March. [online]. Available from: https://www.schoenherr.eu/content/bulgaria-implements-nis-2-directive-key-changes-to-the-cybersecurity-act. [Last viewed: 19 July 2026].

55. SECURITY TODAY, 2026. Incident Response: BSI, CERT und DCSO - Deutschland Reboot 2026. *Security Today*, 22 January. [online]. Available from: https://www.securitytoday.de/2026/01/22/incident-response-bsi-cert-dcso-deutschland-reboot-2026/. [Last viewed: 19 July 2026].

56. THE WHITE HOUSE, 2024. *National Cybersecurity Strategy Implementation Plan – Version 2.* Washington, DC: The White House, May 2024. [online]. Available from: https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf. [Last viewed: 19 July 2026].

57. U.S. GAO, 2021. *Cybersecurity and Infrastructure Security Agency: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation*, GAO-21-236. Washington, DC: U.S. Government Accountability Office. [online]. Available from: https://www.gao.gov/products/gao-21-236. [Last viewed: 19 July 2026].

58. MINISTERSKI SAVET, 2005. Zakon za upravlenie pri krizi. *Darzhaven vestnik*, br. 19 ot 01.03.2005, otm. br. 35 ot 12.05.2009. [in Bulgarian].

59. ANDERSON, R. & MOORE, T., 2006. The economics of information security. *Science*, vol. 314, no. 5799, pp. 610 – 613. doi: 10.1126/science.1130992.

60. DUNN CAVELTY, M. & SUTER, M., 2012. The art of CIIP strategy: Taking stock of content and processes. In: LOPEZ, J.; SETOLA, R. & WOLTHUSEN, S. D. (eds.) Critical Infrastructure Protection. *Lecture Notes in Computer Science*, vol. 7130., pp. 15 – 38. Berlin, Heidelberg: Springer. doi: 10.1007/978-1-4471-4763-3_4.

REFERENCES

KOEPKE, P., 2017. Cybersecurity Information Sharing Incentives and Barriers. Cambridge, MA: MIT Sloan School of Management, Cybersecurity Interdisciplinary Systems Laboratory, Working Paper CISL# 2017-13. [online]. Available from: https://cams.mit.edu/wp-content/uploads/2017-13.pdf. [Last viewed: 19 July 2026].

MLADENOVA, M., 2024. Korporativna i natsionalna sigurnost – parametri na relatsiyata. *Nauchni trudove na Voenna akademia „G. S. Rakovski“,* vol. 1, pp. 1 – 15. Sofia: *Voenna akademia „G. S. Rakovski“*. [in Bulgarian].

OLSON, M., 1965. *The Logic of Collective Action: Public Goods and the Theory of Groups.* Cambridge, MA: Harvard University Press.

OSTROM, E., 1990. *Governing the Commons: The Evolution of Institutions for Collective Action.* Cambridge: Cambridge University Press.

SAMUELSON, P. A., 1954. The pure theory of public expenditure. *The Review of Economics and Statistics*, vol. 36, no. 4, pp. 387 – 389. doi: 10.2307/1925895.

SIMEONOV, T. & STOILOV, P., 2019. *Dejnostta na chastnite voenni kompanii i kompanii za sigurnost v savremennite vaorazheni konflikti – predizvikatelstvo kam mezhdunarodnoto pravo i natsionalnoto zakonodatelstvo*, vol. 126, no. 1 – 2, pp. 77 – 89. [in Bulgarian].

STOILOV, P., 2015. Hibridna vojna – hibridna reaktsia? *Godishnik na Voenna akademia „G. S. Rakovski“, Fakultet „Komandno-shtaben“*, vol. 1, pp. 61 – 68. Sofia: Voenna akademia „G. S. Rakovski“. [in Bulgarian].

STOILOV, P., 2022. *Administrativen menidzhmant v otbranata*. Sofia: Reklamno-izdatelska kashta DioMira. [in Bulgarian].

STOYANOV, K., 2025. *Upravlenie na sigurnostta na kritichnata infrastruktura pri krizi: avtoreferat na disertatsionen trud.* Shumen: Shumen University „Episkop Konstantin Preslavski“. [online]. Available from: https://www.shu.bg/wp-content/uploads/file-manager-advanced/users/razvitie/as/2025/ONS_DOKTOR/. [Last viewed: 19 July 2026]. [in Bulgarian].

PUBLIC-PRIVATE PARTNERSHIP IN CRITICAL INFRASTRUCTURE PROTECTION: A COMPARATIVE ANALYSIS AND PROPOSALS FOR BULGARIA

Abstract. The report examines public-private partnership as a mechanism for protecting critical infrastructure. Based on the theory of public and common goods and the comparative institutional experience of the United States and Germany, deficits in the Bulgarian legal and institutional framework are identified: the lack of a special law and a single coordination center, the un-

transposed CER Directive and the fragmentation of responsibilities. A doctrinal model is proposed, structured around the logic threat – vulnerability – resilience, as well as four measures: adoption of a Law on Critical Infrastructure Management; a single national coordination center; mandatory partnership mechanisms; and institutionalization of public-private platforms for information exchange, training and joint exercises.

Keywords: public-private partnership; critical infrastructure; national security; regulatory framework; information sharing; hybrid model

Ivan Kutelov, **PhD Student**
ORCID iD: 0009-0000-5947-1745
Scientific Section “Strategic Security and Defense Studies”
Defence Advanced Research Institute
Rakovski National Defence College
82, Evlogi i Hristo Georgievi Blvd.
1504 Sofia, Bulgaria
E-mail: ikutelov@gmail.com

https://doi.org/10. 66334/annu26_digiextrem

ДИГИТАЛНИТЕ ИЗМЕРЕНИЯ НА КРАЙНОДЕСНИЯ ЕКСТРЕМИЗЪМ: ОНЛАЙН РАДИКАЛИЗАЦИЯ, ДЕЗИНФОРМАЦИЯ И РИСКОВЕ ЗА ВЪТРЕШНАТА СИГУРНОСТ НА БЪЛГАРИЯ

Ивелина Дундакова, докторант
Военна академия „Георги Стойков Раковски“

Абстракт. В статията се търси отговор как дигиталната среда преструктурира социализацията, нормализирането и мобилизацията при крайнодесния екстремизъм и при какви условия взаимодействието му с дезинформацията придобива значение за вътрешната и националната сигурност на България. Върху качествен преглед на литературата, европейските институционални оценки и публично достъпните български данни е изградена аналитична рамка с четири измерения: групова идентичност и конструиране на заплаха; отношение към насилието; мрежова и субкултурна организация; проницаемост между дигиталната и физическата среда. Българските данни и Пловдивският случай служат като проверка на границите на рамката и показват дигитална организация и публичност на насилието при все още недоказана идеологическа компонента. Изводът е, че рискът нараства, когато предразполагащите условия се наслагват с конкретна цел, готовност и

възможност за действие; статията очертава и три направления за практиката в областта на сигурността.

Ключови думи: крайнодесен екстремизъм; онлайн радикализация; дезинформация; вътрешна сигурност; България; Пловдивски случай

I. Увод

Дигиталната среда промени не само разпространението на политически и идеологически послания, но и условията, в които се формират идентичности, общности и готовност за действие. Платформите предлагат различни възможности за достигане до аудитории, групова идентификация и транснационални връзки, така че интернет е част от социалната среда, в която идеите се тълкуват, приспособяват и – при определени условия – придобиват мобилизационен потенциал (Kakavand 2024; Matlach & Hammer 2024; Zhang & Davis 2024).

Досегът с радикално съдържание сам по себе си не поражда екстремистки убеждения и не позволява надеждна прогноза за насилие (Odağ et al. 2019; Whittaker 2022; Kenyon et al. 2023). Публикацията се насочва към механизмите, чрез които дигиталната среда влияе върху социализацията, нормализирането и мобилизацията, и към условията, при които взаимодействието им с дезинформацията придобива значение за вътрешната и националната сигурност на България. Работната теза е, че рискът нараства, когато изключваща групова идентичност, възприета заплаха, социално подкрепление, институционално недоверие и легитимиране на насилието се наслагват, особено ако към тях се прибавят конкретна цел, мобилизационна готовност и възможност за действие. Дезинформацията може да усилва и свързва тези процеси, но не е самостоятелна причина за радикализация или насилие.

Изследването е качествено и се опира на академична литература, европейски институционални оценки, български изследвания и публично достъпна информация. Единичният случай служи за аналитична проверка. При незавършено наказателно производство символиката, публикацията или обвинението сами по себе си не установяват мотив, принадлежност или причинна връзка. Ролята на дезинформацията не може да бъде проверена самостоятелно, затова в рамката тя фигурира като усилващ фактор, а не като емпирично доказана причина.

II. Понятийна и аналитична рамка

Рамката се ограничава до онези характеристики на крайнодесния екстремизъм, които имат пряко значение за дигиталната среда и за оценката на риска за вътрешната сигурност, а по-широкият политологичен дебат остава теоретичен фон (Mudde 2019; Pirro 2023). Централният въпрос е по какви признаци идеологическата позиция, субкултурната принадлежност или провокативното съдържание могат да бъдат отграничени от процесите, в които се оформя екстремистка мобилизация и нараства рискът от насилствено или друго обществено опасно поведение.

Понятието „крайнодесен екстремизъм“ се използва тук като аналитична категория, а не като политически етикет. Първият от разглежданите белези на крайнодесния екстремизъм е конструирането на противопоставянето „ние – те“, при което определени групи се представят като заплаха за идентичността, сигурността или бъдещето на общността. Нативизмът в смисъла на Кас Мюде е важен ориентир, но не е достатъчен критерий (Mudde 2007; Mudde 2019). Разграничението има и нормативна страна: националистическата, консервативната, антиимиграционната, популистката или антиелитната позиция още не е основание за извод за екстремизъм, а по-показателни са системното делегитимиране на демократичния и правния ред, дехуманизацията или демонизирането на групи и разширяването на допустимите действия към принуда, саморазправа или насилие.

Дезинформацията също не е определящ елемент на понятието. Европейският план за действие срещу дезинформацията я дефинира по-широко – като проверимо невярна или подвеждаща информация, създавана или разпространявана с цел изгода или умишлена заблуда и способна да причини обществена вреда[1]. За анализа е по-важна функцията ѝ – тя може да подсилва образа на заплахата, противопоставянето „ние – те“ и представата, че институциите са нелегитимни.

Вторият признак и ключова аналитична граница е отношението към насилието. Работната европейска дефиниция за насилствен десен екстремизъм (VRWE) включва използване, подбуждане, заплаха, легитимиране или подкрепа на насилие и омраза за политически или идеологически цели, когато мотивацията е свързана с отхвърляне на демократичния ред и основните права, и е центрирана върху националистически идеи, основани на противопоставяне и отхвърляне на определени групи, расизъм или ксенофобия[2]. Тя насочва вниманието отвъд вече извършеното насилие към

момента, в който радикалната или поляризираща позиция започва да представя насилието като оправдано, необходимо или допустимо.

Терминът „онлайн радикализация“ също не се разбира като самостоятелен и праволинеен интернет процес (Whittaker 2022; Odağ et al. 2019; Kenyon et al. 2023) – той обозначава дигитално медиирани процеси на социализация, идентификация, нормализиране и мобилизация, които се преплитат с офлайн отношения и обстоятелства. Връзката е двупосочна – онлайн принадлежности могат да се превърнат в действие, а физическите действия да бъдат заснети, разпространени и натоварени с нов смисъл онлайн.

Мрежовият характер на дигиталната среда налага и методологично ограничение – сходството не доказва организационна връзка. Общите символи, речникът или наративите сочат идейна или субкултурна близост, но не и членство, координация или мотив, макар че липсата на формална организация не изключва подражание. Затова рамката проследява четири свързани измерения: групова идентичност и конструиране на заплаха; отношение към насилието; мрежова и субкултурна организация; проницаемост между дигиталната и физическата среда. Дезинформацията може да пресича всяко от тях като усилващ механизъм, без да бъде критерий за екстремизъм. Механизмите в параграф III показват как тези измерения се оформят в дигитална среда, а равнищата в параграф V – как отношението към насилието преминава в поведенчески риск.

Работната теза от увода насочва към разграничаване на две групи условия: предразполагащи (групова идентичност, възприета заплаха, социално подкрепление, институционално недоверие, легитимиране на насилието) и приближаващи действието (конкретна цел, мобилизационна готовност, възможност за действие), като мобилизационният потенциал е свойство на средата, докато мобилизационната готовност се отнася до индивида или групата.

III. Механизми на дигиталната трансформация на крайнодесния екстремизъм

За да се разбере дигиталното измерение на крайнодесния екстремизъм, е полезно да се проследят механизмите, които свързват индивиди, съдържание и поведение, отколкото анализът да се ограничи до конкретна платформа или технологични канали. Първият механизъм е мрежовата организация. Съвременният крайнодесен екстремизъм трудно се побира

в модела на формална, йерархична и централизирана организация – той може да включва автономни формации, субкултурни среди и „мрежи от мрежи“ без единен център (Castelli Gattinara & Pirro 2019). Дигиталната среда улеснява поддържането на такова пространство и отнема на формалното членство значението му на единствен маркер за принадлежност.

На второ място стои социализацията чрез принадлежност и статус. Понятието „радикални контрастни общества“ (Koehler 2014/2015) показва как идеологическите послания се преплитат със социалното признание и могат да улесняват прехода от символна идентификация към активизъм. Самото недоволство обяснява малко – решаващ е колективният разказ: кои са „нашите“, кой е заплахата и какво действие изглежда допустимо.

Третият механизъм е многоплатформената циркулация. Платформите се различават по видимост, достъпност, устойчивост на съдържанието, свързаност и модерация, а съдържание, аудитории и връзки се придвижват между тях (Kakavand 2024; Matlach & Hammer 2024). Затова въпросът коя платформа „радикализира“ е по-маловажен от проследяването на движението между различните среди.

Четвъртият механизъм е нормализацията. Когато радикални идеи и естетика, свързана с насилие, се повтарят във визуални послания и иронични публикации, с времето могат да започнат да изглеждат обичайни. Това само по себе си обаче не доказва радикализация или готовност за насилие (Crawford et al. 2021; Nangle & D’Haenens 2026; de Jonge & Gaufman 2022). Кодираните символи и модата също могат да имат различни значения – да бъдат израз на стил, знак за принадлежност или послание, разпознаваемо само за определена публика (Miller-Idriss 2018). Затова значението им трябва да се преценява според контекста.

Тези механизми се свързват чрез образа на заплахата – щом обществената промяна се представи като извънредна криза, по-твърдите действия започват да изглеждат съразмерни и адекватни (Wodak 2021). В разказ за опасност, предателство или необходимост от „защита“ именно дезинформацията получава усилваща функция.

IV. Крайнодесен екстремизъм, дезинформация и риск за националната сигурност

Емпиричните изследвания откриват връзки между радикално десни нагласи, медийно потребление и излагането на дезинформация, но не и причинна връзка с насилствен екстремизъм. В изследване на 594 учас-

тници в Германия по-честият досег с дезинформация съвпада с по-високи популистко-радикално десни нагласи, но резултатът засяга нагласите и медийното поведение, а не насилието (Christner et al. 2025). Анализ на 4876 публикации в ирландска крайнодясна Telegram група показва как американско крайнодясно и QAnon съдържание се приспособява към местния контекст (Fattibene et al. 2024). Преносът на идеи през националните граници не заличава националната специфика. Дали и как съдържанието, адаптирано към местния контекст, придобива мобилизационно значение, остава отделен въпрос, на който тези изследвания не дават отговор.

Регионален контекст към този въпрос предлага анализът на Центъра на ЕС за знания в областта на превенцията на радикализацията от 2026 г., посветен на Западните Балкани. В него онлайн радикализацията и дезинформацията се разглеждат на фона на междуетническо напрежение, чуждо информационно въздействие и институционални уязвимости[3]. Близостта на региона прави анализа полезен за българския контекст, но не оправдава автоматичното пренасяне на изводите му върху България.

Към тази картина се добавя и проблематиката на чуждестранното манипулиране на информация и вмешателство (Foreign Information Manipulation and Interference – FIMI). Според Европейската служба за външна дейност то може да експлоатира чувствителни идентичностни теми, да задълбочава поляризацията и да подкопава общественото доверие[4]. Манипулативен наратив може да съвпадне със съществуващ образ на врага, без това да доказва контрол или общ организационен източник. Връзката между дезинформацията, крайнодесния екстремизъм и сигурността е взаимодействие между информационни, социални и поведенчески равнища, а не линейна верига.

V. От дигитална социализация към риск от насилие

Онлайн социализацията сама по себе си не води до насилие (Odağ et al. 2019; Kenyon et al. 2023). За да се проследи кога може да възникне риск от насилствено действие, е полезно да се разграничат три взаимосвързани равнища. На когнитивно равнище поляризиращи и конспиративни представи очертават заплаха; на социално – принадлежността, статусът и подкрепата от групата укрепват идентичността, докато на мобилизационно ниво се търсят признаци за възможно преминаване към действие: оправдаване на насилието, конкретна цел, подготовка или предварително заявяване на намерения.

Особено важно е това разграничение при младежките онлайн субкултури, където последователната политическа идеология невинаги е водеща. Според доклада на Европол EU TE-SAT 2025 от 449 заподозрени, арестувани в ЕС през 2024 г. за престъпления, свързани с тероризъм, 133 са на възраст 12 – 20 години, 70 са непълнолетни, а 12 от тях са свързани с крайнодесен тероризъм и насилствен екстремизъм[5]. Тези данни показват участието на млади лица, но не и мащаба на крайнодясната радикализация. Документ 15477/25 на Координатора на Европейския съюз за борба с тероризма добавя понятието „нихилистично екстремистко насилие“, при което статусът и груповото признание могат да тежат повече от доктрината[6]. Същият документ откроява и „перформативното“ насилие – заснемането и разпространението носят статус и признание, така че физическият акт е едновременно и комуникационно съдържание[7]. Децентрализираната форма не изключва подготовка за насилие – Европол отчита транснационални онлайн мрежи, самостоятелни извършители и малко структурирани офлайн групи[8].

VI. Българският контекст като емпирична проверка

Наличните български данни не позволяват нито да се измери мащабът на крайнодясната радикализация, нито да се докаже причинна връзка между дезинформация, идентификация и насилие. Те обаче позволяват да се проследят отделни елементи от рамката (досега с агресивно съдържание), структурата на дигиталните мрежи, локализацията на антисистемни наративи и взаимодействието между онлайн комуникацията и груповото поведение. Национално представително изследване на Центъра за изследване на демокрацията сред 1018 младежи на 14 – 19 години установява, че 52% са срещали онлайн съдържание, призоваващо към агресия и омраза, а 12 – 16% одобряват отделни агресивни послания[9]. Това е досег и резонанс, не крайнодясна идентичност или готовност за насилие. Мониторинг на 42 българоезични Telegram канала между януари и март 2026 г., обхванал 48 685 публикации, показва интензивно препредаване на антизападни, конспиративни, антисистемни и прокремълски послания (Dzhekova et al. 2026). Това не доказва организационна връзка с крайнодесни групи, но очертава комуникационна инфраструктура за циркулация и локализация на сходни образи на (и разкази за) врага. Аналитична бележка № 167 на Центъра за изследване на демокрацията свързва младежкото насилие с вредни онлайн среди,

култура на саморазправа и стремеж към статус[10], което води към Пловдивския случай.

6.1. Пловдивският случай като аналитична проверка

На 4 август 2026 г. 37-годишен мъж е пребит в района на Младежкия хълм в Пловдив и по-късно умира в болница. На 6 август прокуратурата привлича като обвиняеми петима непълнолетни, а на 27 август – още трима. Според публикации, цитиращи данни от разследването, непълнолетно 17 годишно момиче от групата се представяло във Facebook за 15-годишно и уговорило срещата с мъжа, изпълнявайки ролята на примамка. На мястото го очаквали и други младежи. Разследващите посочват, че групата е подражавала на практиките на т.нар. „ловци на педофили“[11]; нападението е било заснето. Към момента на цитираните съобщения идеологическият мотив и организационната принадлежност не са установени, затова случаят не може да бъде определен като доказан пример за крайнодясно насилие.

Сравнителен контекст дава анализът на Сергей Катсуба на организираната саморазправа с LGBTQ+ лица в Русия, включително на Occupy Pedophilia, където онлайн подмамване, организирана среща и групово унижение се съчетават със заснемане и разпространение (Katsuba 2024). Литературата за т.нар. *paedophile hunters* описва сходни практики чрез понятието „гражданско правосъдие“ (виджилантизъм), т.е. присвояване на функции по разследване, разобличаване и наказание извън институционалните процедури (Tippett 2024; Campbell 2016).

Случаят е значим със съчетанието на дигитално организиране, групово действие и подкрепление, саморазправа и дигитална публичност на насилието. В термините на рамката той илюстрира мрежовата организация, проницаемостта между онлайн и офлайн средата и саморазправата като форма на насилие, но не позволява да се установи първото измерение – идеологическата идентичност и конструираната заплаха. При младежките онлайн субкултури символите, видимостта и дори насилието могат да служат за принадлежност и признание без последователна доктрина[12] (Miller-Idriss 2018), затова никой от тези елементи поотделно не доказва крайнодесен мотив.

Отделен пласт са мрежовите пресичания. Павел Малендович разглежда „Кръв и чест“ (Blood & Honour) като транснационална неонацистка мрежа (Malendowicz 2024). В Пловдив са установени двама младежи, обвинени за отделен, заснет на видео побой над непалски граждани, които са контактували с част от обвиняемите по случая на Младежкия хълм[13]. На 16

август полицията съобщава и за задържането на 18 лица, определени като свързани с „Кръв и чест“, като изрично посочва, че няма доказателства за връзка с убийството[14]. Тези данни са важни за анализа на средата, но тук важи ограничението от параграф II: близостта и контактите не доказват единна организация, общ мотив или причинна връзка.

Заради това ограничение Пловдивският случай е по-скоро проверка на границите на рамката, отколкото пример за нея. Резултатът е двоен: дигиталните механизми на организация и публичност са налице, а идеологическата компонента остава недоказана. Затова трябва да се различават установеното поведение, идеологическата близост, комуникационната свързаност, предполагаемата мотивация и доказаният насилствен екстремизъм.

Взети заедно, българските данни и Пловдивският случай очертават конфигурация от уязвимости, а не доказана единна траектория на крайнодясна радикализация. Дезинформацията остава в рамката като възможен усилващ фактор, но нито данните, нито случаят позволяват да се докаже ролята ѝ. Значението за сигурността не идва от изолираното присъствие на съдържание, символика или мрежов контакт; то нараства, когато възприетата заплаха, груповото подкрепление, институционалното недоверие и нормализирането на насилието се наслагват с конкретна цел, готовност и възможност за действие. От това следва задачата за институционален отговор без необосновано приписване на екстремистка мотивация.

VII. Значение за вътрешната и националната сигурност на България

Главното предизвикателство е ранното разпознаване на конфигурации, в които дигиталното съдържание, мрежовата динамика и конкретното поведение създават мобилизационен потенциал, без законното политическо несъгласие, субкултурната принадлежност или отделната символика да се превръщат сами по себе си в индикатори за екстремизъм. За България се очертават три практически направления.

Първото е аналитичен капацитет за публично достъпните българоезични дигитални екосистеми и движението на съдържание между платформите. Необходимо е разграничение между политическото несъгласие, дезинформационната манипулация, екстремисткото съдържание и поведенческите индикатори за насилие. Така анализът на крайнодесния екстремизъм и този на FIMI могат да се свързват, без да се отъждествяват. Второто е свързването на дигиталния анализ с местната превенция,

особено при непълнолетни и млади възрастни. Пловдивският случай, при който първите петима обвиняеми са непълнолетни, показва колко рано е нужно да се включат местните практики. Реакцията трябва да е ранна, но пропорционална и да не превръща всяка радикална публикация или досег с дезинформация в заплаха[15]. Третото е превеждането на националната стратегическа рамка в аналитична практика. Стратегията за противодействие на радикализацията и тероризма 2026 – 2030 г. поставя акцент върху превенцията, адаптацията към променящите се заплахи, уязвимите групи и междуинституционалното взаимодействие[16]. Това предполага ранно сигнализиране, споделени аналитични критерии и обратна връзка между национално и местно равнище. Разграничението между идеологическа среда, информационна манипулация и непосредствен поведенчески риск трябва да се запази, защото всяко равнище изисква различен институционален отговор – превенция и работа с общностите при идеологическата среда, стратегическа комуникация и сътрудничество с платформите при информационната манипулация, правоохранителна и оперативна реакция при непосредствения риск.

VIII. Заключение

Дигиталното измерение на крайнодесния екстремизъм не се свежда до технологичен ефект или до механично пренасяне на вече съществуващи организации в интернет. Дигиталната среда променя начина, по който хората срещат радикални идеи, свикват с тях и се включват в групови действия. Но връзката между онлайн съдържанието и насилието не е пряка: човек може да попадне на дадено послание, без да го приеме, а приемането му не означава непременно намерение или готовност за насилствено действие. Дезинформацията сама по себе си също не поражда екстремизъм или насилие.

Българските данни и Пловдивският случай не позволяват извод нито за мащаба, нито за единна национална траектория на крайнодясна радикализация. Те показват обаче как дигиталното посредничество, груповият статус, саморазправата и мрежовите пресичания могат да се комбинират, без отделен елемент да е доказателство за екстремизъм. Работната теза за наслагването на условия е подкрепена като аналитична рамка, но остава недоказана емпирично, защото изследването е качествено, разчита на публични данни и на един случай, а ролята на дезинформацията не може да бъде проверена самостоятелно. Основният

въпрос за вътрешната и националната сигурност е при какви условия тази конфигурация преминава от средова уязвимост към мобилизационен риск.

Благодарности. Авторът изказва благодарност на научния си ръководител полк. доц. д.н. Петър Маринов за методологическите насоки и професионалната подкрепа, както и на подполк. гл. ас. д-р Димо Иванов за съдействието при подготовката на ръкописа.

БЕЛЕЖКИ

1. EUROPEAN COMMISSION & HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY (HR/VP), 2018. *Action Plan against Disinformation,* 5 December 2018. JOIN(2018) 36 final. Brussels.

2. EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR MIGRATION AND HOME AFFAIRS, 2021. *Working Definition for Violent Right-Wing Extremism (VRWE).* Project Based Collaboration on Violent Right-Wing Extremism.

3. EU KNOWLEDGE HUB ON PREVENTION OF RADICALISATION, 2026. *The Nexus Between Online Radicalisation and Disinformation in the Western Balkans*. Conclusion Paper, 16 July 2026.

4. EUROPEAN EXTERNAL ACTION SERVICE (EEAS), 2024. *Safeguarding Democracy: Building Resilience Against Identity-Based Disinformation*, 8 November 2024.

5. EUROPOL, 2025. *European Union Terrorism Situation and Trend Report 2025.* Luxembourg: Publications Office of the European Union. DOI 10.2813/5425593.

6. COUNCIL OF THE EUROPEAN UNION (Council of the EU), 2025. *Nihilistic Extremist Violence: An Emerging Threat*. Note from the EU Counter-Terrorism Coordinator to Delegations, Council document 15477/25, 19 November 2025.

7. Пак там.

8. EUROPOL, 2025. *European Union Terrorism Situation and Trend Report 2025.* Luxembourg: Publications Office of the European Union. DOI 10.2813/5425593.

9. CENTRE FOR THE STUDY OF DEMOCRACY (CSD), 2020. *Overcoming Youth Vulnerabilities to Far-Right Narratives*. Sofia: CSD.

10. CENTRE FOR THE STUDY OF DEMOCRACY (CSD), 2026. *Youth Violence: Closing the Prevention Gap*. Policy Brief No. 167. Sofia: CSD, 20 August 2026.

11. Окръжна прокуратура – Пловдив, „Привлечени като обвиняеми петима непълнолетни за умишлено убийство на 37-годишен мъж, извършено с особена жестокост и по хулигански подбуди“, 6 август 2026 г.; Окръжна прокуратура – Пловдив, „Привлечени като обвиняеми и задържани още трима непълнолетни за умишленото убийство на 37-годишен мъж в района на Младежкия хълм“, 27 август 2026 г.

12. EU KNOWLEDGE HUB ON PREVENTION OF RADICALISATION, 2026. *Nihilistic Extremism in the Digital Age*. Conclusions Paper, Joint Meeting of Thematic Panels 1 and 3, 10 April 2026.

13. БТА, „Районна прокуратура – Пловдив привлече като обвиняеми двама младежи за нанесена телесна повреда на непалски граждани, като побоят е бил заснет на видеоклип“, 11 август 2026 г.; БТА, „Единият младеж, задържан за нападение над непалци в Пловдив, е присъствал на убийството на Младежкия хълм в града“, 12 август 2026 г.

14. БТА, „Общо 18 души, принадлежащи към международна неонацистка организация ‚Кръв и чест‘, са арестувани в Пловдив“, 16 август 2026 г.

15. COUNCIL OF THE EUROPEAN UNION (Council of the EU), 2025. *Nihilistic Extremist Violence: An Emerging Threat*. Note from the EU Counter-Terrorism Coordinator to Delegations, Council document 15477/25, 19 November 2025.

16. МИНИСТЕРСКИ СЪВЕТ, 2026. *Стратегия за противодействие на радикализацията и тероризма (2026 – 2030 г.),* [приета с Решение № 316 на Министерския съвет от 23 април 2026 г.]. София.

REFERENCES

CAMPBELL, E., 2016. Policing Paedophilia: Assembling Bodies, Spaces and Things. *Theoretical Criminology*, vol. 20, no. 3. DOI 10.1177/1741659015623598.

CASTELLI GATTINARA, P. & PIRRO, A. L. P., 2019. The Far Right as Social Movement. *European Societies*, vol. 21, no. 4, pp. 447 – 462. DOI 10.1080/14616696.2018.1494301.

CHRISTNER, C.; MAKHORTYKH, M. & GIL-LOPEZ, T., 2025. Populist Radical-Right Attitudes, Media Trust, and Social Media Reliance: Combining Survey and Tracking Data to Investigate Predictors of Online Exposure to Disinformation. *Telematics and Informatics*, vol. 98, 102250. DOI 10.1016/j.tele.2025.102250.

CRAWFORD, B.; KEEN, F. & SUAREZ-TANGIL, G., 2021. Memes, Radicalisation, and the Promotion of Violence on Chan Sites. *Proceedings of the International AAAI Conference on Web and Social Media*, vol. 15, pp. 982 – 991.

DE JONGE, L. & GAUFMAN, E., 2022. The Normalisation of the Far Right in the Dutch Media in the Run-up to the 2021 General Elections. *Discourse & Society*, vol. 33, no. 6, pp. 773 – 787. DOI 10.1177/09579265221095418.

DZHEKOVA, R.; TRIFONOVA, G. & GALEV, T., 2026. *Defending the Vote: Analysis of the Bulgarian Digital Information Environment*. Sofia: Center for the Study of Democracy.

FATTIBENE, G.; WINDLE, J.; LYNCH, O.; HELM, G.; PURVIS, J. & SEPPA, L., 2024. The Online Exchange of Conspiracy Theories within an Irish Extreme Right-Wing Telegram Group during the COVID-19 Pandemic. *Behavioral Sciences of Terrorism and Political Aggression,* vol. 18, no. 2, pp. 188 – 206. DOI:10.1080/19434472.2024.2409185.

KAKAVAND, A. E., 2024. Far-Right Social Media Communication in the Light of Technology Affordances: A Systematic Literature Review. *Annals of the International Communication Association*, vol. 48, no. 1, pp. 37 – 56. ISSN 2380-8985.

KATSUBA, S., 2024. Premeditated, Organized and Impactful: Dating Violence as a Method of Committing Hate Crimes Against LGBTQ People in Russia. *Journal of Family Violence*, vol. 39, pp. 1407 – 1420. DOI 10.1007/s10896-023-00638-z.

KENYON, J.; BINDER, J. F. & BAKER-BEALL, C., 2023. Online Radicalization: Profile and Risk Analysis of Individuals Convicted of Extremist Offences. *Legal and Criminological Psychology*, vol. 28, pp. 7490. ISSN 1355-3259.

KOEHLER, D., 2014/2015. The Radical Online: Individual Radicalization Processes and the Role of the Internet. *Journal for Deradicalization*, vol. 1, pp. 116 – 134. ISSN 2363-9849.

MALENDOWICZ, P., 2024. Neonazizm jako wyzwanie dla demokracji europejskich w czasach kryzysów (przykład sieci Blood and Honour). *Rocznik Integracji Europejskiej*, vol. 18, pp. 127 – 139. DOI 10.14746/rie.2024.18.9. [in Polish].

MATLACH, P.-C. Y. & HAMMER, D., 2024. *The German Far Right Online: A Longitudinal Study*. Institute for Strategic Dialogue Germany.

MILLER-IDRISS, C., 2018. *The Extreme Gone Mainstream: Commercialization and Far Right Youth Culture in Germany*. Princeton, NJ: Princeton University Press.

MUDDE, C., 2007. *Populist Radical Right Parties in Europe*. Cambridge: Cambridge University Press.

MUDDE, C., 2019. *The Far Right Today*. Cambridge: Polity Press.

NANGLE, B. M. & D'HAENENS, L., 2026. Affective-Discursive Ecologies of the Far Right: Multimodal Softening, Mobilisation and Algorithmic Proximity on Instagram. *New Media & Society*.

ODAĞ, Ö.; LEISER, A. & BOEHNKE, K., 2019. Reviewing the Role of the Internet in Radicalization Processes. *Journal for Deradicalization*, vol. 21, pp. 261 – 300. ISSN 2363-9849.

PIRRO, A. L. P., 2023. Far Right: The Significance of an Umbrella Concept. *Nations and Nationalism*, vol. 29, no. 1, pp. 101 – 112. DOI 10.1111/nana.12860.

TIPPETT, A., 2024. The Rise of Paedophile Hunters: To What Extent Are Cyber-Vigilante Groups a Productive Form of Policing, Retribution and Justice? *Criminology & Criminal Justice*, vol. 24, no. 4, pp. 711 – 732. DOI 10.1177/17488958221136845.

WHITTAKER, J., 2022. Rethinking Online Radicalization. *Perspectives on Terrorism*, vol. 16, no. 4, pp. 27 – 40. ISSN 2334-3745.

WODAK, R., 2021. *The Politics of Fear: The Shameless Normalization of Far-Right Discourse*. 2nd ed. London: SAGE.

ZHANG, X. & DAVIS, M., 2024. E-extremism: A Conceptual Framework for Studying the Online Far Right. *New Media & Society*, vol. 26, no. 5, pp. 2954 – 2970. ISSN 1461-4448.

THE DIGITAL DIMENSIONS OF FAR-RIGHT EXTREMISM: ONLINE RADICALIZATION, DISINFORMATION, AND RISKS TO BULGARIA'S INTERNAL SECURITY

Abstract. This article explores how the digital environment restructures socialization, normalization, and mobilization within far-right extremism, and examines the conditions under which its

interaction with disinformation becomes significant for Bulgaria's internal and national security. Based on a qualitative literature review, European institutional assessments, and publicly available Bulgarian data, an analytical framework with four dimensions is developed: group identity and threat construction; attitudes toward violence; network and subcultural organization; and the permeability between the digital and physical environments. Bulgarian data—specifically the Plovdiv case—serve to test the boundaries of this framework, revealing digital organization and the public display of violence, even while a clear ideological component remains unproven. The study concludes that the risk escalates when predisposing conditions converge with a specific objective, a readiness to act, and the capacity to do so; the article also outlines three implications for security practice.

Keywords: far-right extremism; online radicalization; disinformation; internal security; Bulgaria; Plovdiv case

Ivelina Dundakova, PhD student
Land Forces Department
Command and Staff Faculty
Rakovski National Defence College
82, Evlogi and Hristo Georgievi Blvd.
1504 Sofia, Bulgaria
E-mail: ivkaraba@gmail.com

https://doi.org/10. 66334/annu26_autoreshsyst

АВТОМАТИЗИРАНИ РЕШЕНИЯ И СИСТЕМИ С ИЗКУСТВЕН ИНТЕЛЕКТ В УПРАВЛЕНИЕТО НА КОРПОРАТИВНИЯ РИСК

доц. д-р Илина Козарова-Арменчева,
гл. ас. д-р Мирослава Младенова
Военна академия „Георги Стойков Раковски“

Абстракт. Използването на автоматизираните решения и системите с изкуствен интелект променя начина, по който организациите идентифицират, анализират и управляват рисковете. Технологиите позволяват обработването на големи обеми от данни, откриването на трудно забележими зависимости и наблюдението на ключови процеси в реално време, като така се създават условия за по-ранна реакция, по-добра информираност и по-ефективно използване на корпоративните ресурси. Наред с възможностите обаче, възникват рискове, свързани с качеството на данните, непрозрачността на алгоритмите, защитата на личната и служебната информация, киберсигурността и прекаленото предоверяване на автоматизирани оценки. Статията разглежда възможните приложения на автоматизирани решения в управлението на корпоративния риск, техните основни предимства и ограничения, както и развитието на регулаторната рамка. Основната идея е, че изкуственият интелект може да подобри корпоративната сигурност само ако бъде внедряван отговорно, при наличие на човешки надзор, ясна отчетност и постоянна оценка на риска.

Ключови думи: изкуствен интелект; автоматизирани решения; корпоративна сигурност; управление на риска; машинно обучение; човешки надзор; AI Act

I. Въведение

Управлението на риска е основна част от корпоративното управление и сигурност. Всяка организация осъществява дейността си в среда на несигурност, в която финансови, оперативни, технологични, правни и репутационни фактори могат да повлияят върху постигането на поставените цели. През последните години тази среда се усложнява допълнително от ускорената дигитализация, взаимната свързаност на информационните системи и постоянно увеличаващия се обем на наличните данни.

Традиционните методи за оценка на риска все още имат важно значение, но често не са достатъчни за обработването на големи потоци от информация и висока скорост на обновяване. Експертният анализ може да бъде затруднен и от необходимостта да се проследяват едновременно множество показатели, чиито взаимовръзки невинаги са непосредствено видими. Именно в тази област, автоматизираните решения и системите, основани на изкуствен интелект, намират все по-широко приложение. Технологиите дават възможности организациите да събират и анализират данни от различни източници, да откриват отклонения от нормалното състояние на дадена система и да оценяват вероятността от настъпване на неблагоприятни събития. Ползата им обаче не се изчерпва с ускоряването на вече съществуващи дейности. Те могат да променят самия подход към риска като насочат организациите от реактивен към проактивен подход, т.е. от реакция след настъпване на някакво негативно събитие към ранно предупреждение и превенция.

II. Автоматизирани решения при управлението на риска

В процеса по управлението на риска, автоматизираните решения могат да се определят като софтуерни и системни инструменти, които изпълняват предварително зададени операции без необходимост от постоянна човешка намеса. Те събират, обработват и съпоставят информация, проследяват показатели, откриват отклонения и генерират предупреждения или препоръки. Трябва да се отбележи, че не всяка автоматизирана система непременно използва изкуствен интелект. Част от инструментите функционират чрез зададени правила, като например системата да подава сигнал, когато определен показател премине предварително зададен праг. При по-сложните решения се използват машинно обучение, обработка на естествен език, прогнозни модели и др. Те могат да разпознават закономерности в статистически данни и да актуализират оценките си

при получаване на нова информация, но различните видове технологии пораждат различни рискове, свързани с проследимостта и прозрачността на системите. Система, работеща по ясни правила, обикновено позволява по-лесно да бъде проследена логиката на получения резултат, докато при някои модели, базирани на машинно обучение, връзката между входните данни и резултата може да бъде значително по-трудно проследима, което от своя страна има отношение към прозрачността, контрола и отговорността.

Ефективността на автоматизираните решения зависи и от тяхното интегриране в съществуващата информационна среда. Организациите разполагат с данни в най-различни системи – като например счетоводни, платформи за управление на клиенти, системи за контрол на достъпа, инструменти за киберсигурност и множество други източници. Ако данните са частични, разпокъсани, несъвместими или с ниско качество, дори технологично усъвършенстваният модел може да произведе ненадежден резултат. Следователно внедряването на системи с изкуствен интелект не трябва да се разглежда като изолиран технологичен проект, а като цялостен процес с предварителна подготовка на данните, адаптиране на работните процеси, обучение на служителите и ясно определяне на начина, по който автоматизираните оценки ще се използват при вземането на решения.

III. Приложение в управлението на корпоративния риск

Употребата на автоматизирани инструменти гарантира едно проактивно отношение на организациите спрямо рисковете, тъй като дават възможност за ранно идентифициране на потенциални негативни събития и предприемането на превантивни мерки, недопускащи тяхната реализация. За управлението на риска в дадена организация информацията е приоритетна и е свързана с определяне на ключови активи и ресурси. Следователно, друг положителен аспект на автоматизираните инструменти е способността им за персонализиране и мащабиране на данните, което ги прави приложими към всички сфери на дейност, отчитайки специфичните потребности на всяка организация. В този смисъл, ползите от имплементирането на такива инструменти са многобройни за компаниите както по отношение на процесите по управление на риска, така и спрямо всички останали корпоративни дейности.

Освен това, автоматизираните решения намират приложение на различни етапи от процеса по управление на риска. Те подпомагат

идентифицирането на заплахи чрез анализ на статистически и текущи данни. Това може да включва например необичайни финансови операции, промени в поведението на потребители, отклонения в производствен процес или признаци за компрометиране на информационна система. Технологиите могат да подпомогнат анализа и оценката на вече идентифицирани рискове като групират сходни случаи, да изведат факторите, които влияят върху вероятността за настъпване на дадено събитие, и да пресметнат възможното му отражение. Получените резултати биха били полезни за приоритизиране на рисковете и разпределяне на ресурси. На следващо място, автоматизацията може да е приложима при мониторинга и реакцията. Когато бъдат достигнати зададените прагови стойности, системата може да уведоми отговорните служители, за да се направи допълнителна проверка или да се задейства друга вътрешно-корпоративна процедура. Дори при някои технически процеси е възможно временно блокиране на дадена операция, но все пак крайните решенията следва да подлежат на човешки контрол.

Могат да се дадат много примери за приложение на технологиите в редица сфери на дейност: във финансовия сектор могат да подпомагат откриването на измами и съмнителни транзакции; в киберсигурността се използват за разпознаване на необичайна мрежова активност; в управлението на веригите за доставки могат да сигнализират за риск от забавяне, недостиг или зависимост от ограничен кръг доставчици; в производството могат да прогнозират технически неизправности, а в областта на човешките ресурси – да подпомагат административни и аналитични процеси, при спазване на изискванията за недискриминация и защита на личните данни.

IV. Възможни ползи от внедряването на автоматизирани решения

От гледна точка на потенциални негативни събития, най-големите предимства в прилагането на автоматизирани решения са свързани с по-висока ефективност и точност при идентификация и анализ на рисковете; мониторинг и възможност за сигнализиране/предупреждение в реално време; разнообразни възможности за вземане на решения; редуциране на грешките, породени от човешки фактор, както и елиминиране на присъщата за него субективност спрямо оценката на рисковете[1]. Автоматизацията на различни работни процеси може да доведе до множество ползи за организациите. Тя води до оптимизация и ефективност на различни работни процеси:

По-бърза обработка на информацията. Едно от основните предимства на автоматизираните системи е способността им да обработват значителни количества данни за сравнително кратко време. Това позволява на организациите да използват информация, която би била твърде обемна или сложна за изцяло ръчен анализ. Тази способност не означава, че резултатите са безпогрешни, тъй като точността зависи от качеството на данните, правилния избор на модел и начина, по който системата се използва. Предимството се състои преди всичко в бързината, мащаба и възможността за систематично проследяване на множество показатели.

Ранно идентифициране на заплахи. Анализът на текущи и вече обработени статистически данни може да разкрие ранни признаци за развитие на неблагоприятно събитие, което създава условия за проактивен подход при управлението на риска. Вместо организацията да реагира реактивно, т.е. едва след настъпването на вреда, тя може предварително да приложи контролни или превантивни мерки.

Наблюдение в реално време. Традиционните проверки често се извършват периодично и представят състоянието на риска към определен минал момент. Автоматизираните системи могат да следят процесите непрекъснато и да подават предупредителни сигнали непосредствено след откриване на дадено отклонение. Това е особено важно при кибератаки, финансови измами и технически неизправности, при които забавената реакция може значително да увеличи щетите.

Последователност на анализа. При човешката оценка е възможно сходни ситуации да бъдат интерпретирани по един и същи начин, но ако има предварително определени критерии и алгоритми, те могат да повишат качеството на анализа и също така да минимизират човешки грешки, породени било то от умората и неволни пропуски.

По-ефективно използване на ресурсите. Чрез автоматизирането на повтарящи се операции, служителите могат да насочат времето и усилията си към задачи, които изискват стратегическа преценка, комуникация и експертно решение. Това от своя страна може да намали дублирането на дейности и да подобри координацията между различните структурни звена.

Подпомагане на управленските решения. Решенията с изкуствен интелект имат възможности да правят сравнения между различни сценарии и да оценяват възможните последствия, като това е още една възможност, която повишава информационната осведоменост при взимането на ръководни решения.

Развитието на изкуствен интелект намира все по-широко приложение в корпоративните дейности и благодарение на базираните на ИИ системи, организациите могат да идентифицират и подлагат на анализ събития, които са трудно уловими за хората поради мащаба на данните, които следва да бъдат обработени. Резултатите от извършените анализи стоят в основата на планиране и предприемане на проактивни дейности срещу потенциални негативни събития, които могат да повлияят негативно на компаниите. Понастоящем, автоматизираните решения водят до редица промени чрез способностите си за обработка на огромни количества данни, за изключително кратки срокове и с безупречна точност[2]. Въпреки огромните ползи от внедряването на изкуствения интелект, не трябва да се забравя, че технологиите трябва да имат подпомагащи функции и крайното решение да е *manmade*. От икономическа гледна точка, ползите трябва да бъдат съпоставени с разходите, с рисковете от промяната, и чак тогава да се пристъпи към внедряване, тъй като това може да изисква значителни първоначални инвестиции, обучение на персонала и продължаваща техническа поддръжка, която не е по силите на компанията.

V. Рискове и ограничения

Освен редицата предимства от приложението на автоматизирани решения, те могат да породят също така множество рискове и предизвикателства, свързани с корпоративното управление:

Ненадеждни или непредставителни данни. Резултатите на една система зависят от данните, с които тя е разработена и функционира. Непълните, остарелите или неправилно категоризираните данни могат да доведат до подвеждащи оценки, а когато използваната информация съдържа системни отклонения, моделът може да ги възпроизведе и затова организациите следва да прилагат правила за качество, актуалност, проследимост и законен произход на данните.

Алгоритмични пристрастия и дискриминация. Алгоритмичните модели могат да третират неблагоприятно определени обществени групи, когато данните не ги представят достатъчно пълно и достоверно. Затова ограничаването на неблагоприятните последствия изисква предварително и периодично тестване, участие на различни експерти и ясна процедура за преглед или обжалване на решенията.

Недостатъчна прозрачност. При някои сложни модели, невинаги може лесно да бъде обяснено защо е получен определен резултат, което

затруднява контрола върху решенията и определянето на отговорността. Освен това, при решения с правни или други съществени последици, изискванията за прозрачност и контрол следва да бъдат доста по-високи, отколкото при помощни административни функции.

Киберрискове. Системите с изкуствен интелект могат да бъдат обект на разнообразни атаки – като манипулиране на входните данни, кражба на модели, неразрешен достъп или използване на уязвимости във външни компоненти. В същото време, изкуственият интелект може да подпомага злонамерени дейности, включително създаването на подвеждащо съдържание и автоматизирането на отделни етапи от кибератаки. Следователно, сигурността трябва да бъде заложена още на етап проект на системата и да се извършва периодичен контрол, защита на данните, регистриране на действията, управление на уязвимостите, както и да се приеме план за реакция при инциденти.

Защита на личните данни. Някои системи са предназначени да използват лични данни или чувствителна информация и това от своя страна създава риск от прекомерно събиране, неправомерно използване или разкриване на данни. В тези случаи организациите следва да прилагат принципите за целево и законосъобразно използване на данните (GDPR, оценка на въздействието, защитата на данните, киберсигурност).

Интелектуална собственост. Внедряването на ИИ поражда много въпроси за произхода на съдържанието и правата върху него. В този смисъл, особено внимание трябва да се отдели на генеративните системи, които могат да създават текст, изображения, програмни кодове или други резултати въз основа на големи масиви от данни. Преди внедряване, следва да се проверят условията на доставчика, допустимото използване на въведените данни, собствеността върху генерираните материали и риска от нарушаване на права на трети лица. Що се отнася за чувствителна корпоративна информация, тя не би трябвало да се въвежда във външни системи, без предварителна оценка и разрешение.

Прекомерна зависимост от технологията. Честото използване на автоматизирани решения може да доведе до това, те да бъдат приемани на 100%, без критично оценяване. Безусловното приемане и прилагане на тези решения също може да породи множество рискове, особено когато моделът работи в необичайна среда или с данни, различни от тези, за които е разработен. Служителите трябва да бъдат обучени не само как да използват определена система, но и да осъществяват контрол върху

резултатите ѝ, като по всяко време трябва да има възможност за човешка намеса, корекция и временно спиране.

VI. Регулаторна рамка

Съществуват редица обективни и субективни причини, поради които правните системи изпитват затруднения спрямо създаването на нормативната уредба в областта на изкуствения интелект. Едно от най-големите затруднения в областта на новите технологии е унифицирането на основните понятия, като например генеративен ИИ, Deep learning и други. Нужно е също така да се направи разграничение между изкуствен интелект, който е вграден в разнообразни SMART устройства и ИИ, който се създава под формата на софтуерни програми, ориентирани към изследване и разбиране на присъщия за човека интелект. Друго предизвикателство се явява въпросът с интелектуалната собственост и това, че изкуственият интелект също бива захранван от информация, която е обект на интелектуална собственост[3].

Правното регулиране на новите технологии, и в частност на изкуствения интелект, е затруднено също така от бързото развитие и разнообразието от приложения. Термини като машинно обучение, дълбоко обучение и генеративен изкуствен интелект описват свързани, но различни технологии. Ето защо, еднаквото им третиране би могло да доведе до прекомерни или недостатъчни ограничения.

В рамките на Европейския съюз основно значение има Регламент (ЕС) 2024/1689 за установяване на хармонизирани правила относно изкуствения интелект, известен като Акт за изкуствения интелект. Регламентът влиза в сила от 1 август 2024 г. и цели установяването на единна правна рамка спрямо системите с изкуствен интелект, която да съответства на ценностите на Европейския съюз[4]. Неговите разпоредби започват да се прилагат поетапно, а не едновременно за всички субекти и системи.

В основата на регламента е подходът според степента на риска. Част от практиките са забранени, когато се приемат за несъвместими с основните права и ценностите на Съюза. За системите с висок риск са предвидени по-строги задължения, включително управление на риска, документация, качество на данните, регистриране на събития, прозрачност, човешки надзор, точност, устойчивост и киберсигурност. Например, не е коректно да се твърди, че всяка употреба на биометрични системи или разпознаване на емоции е абсолютно забранена. Регламентът забранява определени

практики и предвижда конкретни изключения и условия. Правната оценка следва да отчита целта, контекста, използваната технология и засегнатите лица.

Актът за изкуствения интелект не действа изолирано. В зависимост от конкретния случай могат да бъдат приложими правилата за защита на личните данни, киберсигурността, безопасността на продуктите, потребителската защита, трудовото право и интелектуалната собственост. Това означава, че организациите трябва да извършват комплексна оценка, а не да проверяват съответствието само с един нормативен акт.

VII. Международно сътрудничество и обществено доверие

Рисковете, свързани с изкуствения интелект, често надхвърлят националните граници. Моделите могат да бъдат разработени в една държава, внедрени в друга и използвани от потребители в много различни юрисдикции. Това налага сътрудничество между правителства, международни организации, научни институции и частния сектор.

През ноември 2023 г. участниците в Срещата на върха за безопасността на изкуствения интелект приемат декларация, която подчертава необходимостта от съвместни действия по отношение на рисковете от най-усъвършенстваните модели[5]. Значими ориентири са също петте принципа на Организацията за икономическо сътрудничество и развитие (ОИСР) за изкуствения интелект, които се отнасят до устойчиво развитие и благосъстояние, зачитане на правата на човека и демократичните ценности, прозрачност и обяснимост, надеждност, сигурност и безопасност, и отговорност и отчетност[6]. Освен изброените принципи, ЮНЕСКО също издава препоръки за относно етичното използване на изкуствения интелект[7]. Обществото доверие не може да бъде изградено само върху уверения за ползите от технологията. То зависи от реалната възможност засегнатите лица да разберат кога взаимодействат със система с изкуствен интелект, как се използват техните данни и как могат да оспорят неблагоприятни решения, затова прозрачността, отчетността и ефективният надзор имат централно значение за приемането на технологиите.

VIII. Насоки за отговорно внедряване

Успешното въвеждане на автоматизирани решения изисква последователен процес, който обхваща целия жизнен цикъл на системата. За да е успешен този процес, организацията трябва ясно да определи

нуждите, който технологията следва да удовлетвори, тъй като внедряването не трябва да бъде самоцелно или пък мотивирано единствено от стремежа за следване на технологични моди и тенденции. Преди да се стартира този процес е необходимо е да се извърши качествен анализ на въздействието върху служителите, клиентите, информационната сигурност, защитата на данните и действащите бизнес процеси с предварителна оценка на ползите, разходите и рисковете. На следващо място, трябва да бъдат определени ясни роли и отговорности – кой одобрява използването на системата, кой наблюдава работата ѝ и кой носи отговорност при грешка или инцидент. Важно е да се извършва периодичен мониторинг на внедрените системи и данните, защото при промяната на външната среда може да се намали точността на система, която преди това е работила добре. Друг важен фактор за успешното внедряване е човешкият надзор, който следва да бъде съобразен с възможните последици, т.е. колкото по-съществено е въздействието на дадено решение, толкова по-силен трябва да бъде контролът върху него. По отношение на служителите, те трябва да получат подходящо обучение. То следва да включва не само технически инструкции, но и информация за ограниченията на модела, защитата на данните, киберрисковете и реда за докладване на инциденти.

IX. Заключение

Автоматизираните решения и изкуственият интелект предоставят значителни възможности за усъвършенстване на корпоративното управление на риска. Те позволяват обработване на големи информационни масиви, своевременно откриване на отклонения, наблюдение в реално време и по-добро информационно обезпечаване на управленските решения. При правилно внедряване могат да повишат устойчивостта на организацията и да насочат човешкия ресурс към дейности, които изискват стратегическа и експертна преценка.

Същевременно тези технологии не премахват несигурността и не гарантират безпогрешни решения. Те създават нови зависимости и уязвимости, свързани с качеството на данните, алгоритмичните пристрастия, непрозрачността, киберсигурността и защитата на основните права. Затова използването им трябва да бъде придружено от ясни правила, контрол, документация и реален човешки надзор.

Най-устойчивият подход е изкуственият интелект да се разглежда като средство, което допълва човешката експертиза. Технологичната

ефективност трябва да бъде съчетана със законосъобразност, прозрачност и отчетност. Само така организациите могат да използват потенциала на автоматизацията, без да допускат новите инструменти сами да се превърнат в неконтролиран източник на риск.

БЕЛЕЖКИ

1. *Automated Risk Assessment Tools – Data-Driven Risk Mitigation Strategies* [online]. Available from: https://www.wrk.com/blog/automated-risk-assessment-tools-data-driven-risk-mitigation-strategies/. [Last viewed: 29.08.2023].

2. *The Future of Risk Management: How AI is Transforming Decision-Making for Risk Managers* [online]. Available from: https://www.linkedin.com/pulse/future-risk-management-how-ai-transforming-managers-clayton-scott. [Last viewed: 10.06.2026].

3. *Изкуственият интелект като предизвикателство пред правото* [online]. Available from: https://news.lex.bg/%D0%98%D0%B7%D0%BA%D1%83%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%B8%D1%8F%D1%82%D0%B8%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D0%BA%D0%B0%D1%82%D0%BE%D0%BF%D1%80%D0%B5%D0%B4%D0%B8%D0%B7%D0%B2%D0%B8%D0%BA%D0%B0%D1%82%D0%B5%D0%BB%D1%81%D1%82%D0%B2%D0%BE%D0%BF%D1%80%D0%B5%D0%B4-%D0%BF%D1%80%D0%B0%D0-%B2%D0%BE%D1%82%D0%BE/.

[Last viewed: 20.11.2023].

4. ЕС, 2024. *Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 година за установяване на хармонизирани правила относно изкуствения интелект* [online]. Available from: https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=OJ:L_202401689. [Last viewed: 20.11.2025].

5. *The Bletchley Declaration by Countries Attending the AI Safety Summit*, 1 – 2 November 2023 [online]. Available from: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023. [Last viewed: 20.06.2026].

6. OECD, 2019. *Recommendation of the Council on Artificial Intelligence*. Paris: Organisation for Economic Co-operation and Development [online]. Available from: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. [Last viewed: 14.07.2026].

7. UNESCO, 2021. *Recommendation on the Ethics of Artificial Intelligence.* Paris: UNESCO. [online]. Available from: https://unesdoc.unesco.org/ark:/48223/pf0000381137. [Last viewed: 14.07.2026].

8. EC, 2021. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), COM/2021/206 final. [online]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206. [Last viewed: 16.07.2026]. Brussels: European Commission.

9. EP, 2023. EU AI Act: First regulation on artificial intelligence. [online]. Available from https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence. [Last viewed:16.07.2026].

10. EU, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Official Journal of the European Union, L 119, pp. 1 – 88.

11. EU, 2024. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, Official Journal of the European Union, L, 2024/1689.

12. ISO, 2018. ISO 31000:2018 Risk management – Guidelines. Geneva: International Organization for Standardization.

13. ISO/IEC, 2023. ISO/IEC 23894:2023 Information technology – Artificial intelligence – Guidance on risk management. Geneva: International Organization for Standardization.

14. NIST, 2023. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg, MD: National Institute of Standards and Technology.

15. ARMENCHEVA, I. & DIMITROV, T. 2020. Izkustveniyat intelekt – razvitie, postizhenia i napravlenia. In: *Sbornik nauchni trudove. Mezhdunarodna nauchna konferentsia „Shirokata sigurnost“,* vol. 2: Kibersigurnost. Ikonomicheska, sotsialna i kulturna sigurnost. Sofia: NBU. ISBN 978-619-7383-19-5. [in Bulgarian].

AUTOMATED SOLUTIONS AND ARTIFICIAL INTELLIGENCE SYSTEMS IN CORPORATE RISK MANAGEMENT

Abstract. The use of automated solutions and artificial intelligence systems is changing the way organizations identify, analyse, and manage risks. These technologies enable the processing of large volumes of data, the detection of patterns and correlations that are difficult to identify, and the real-time monitoring of key processes. This creates opportunities for earlier responses, improved situational awareness, and more efficient use of corporate resources. Alongside these opportunities, however, risks arise concerning data quality, algorithmic opacity, the protection of personal and confidential business information, cybersecurity, and excessive reliance on automated assessments. This research examines the potential applications of automated solutions in corporate risk management, their main advantages and limitations, and the development of the relevant regulatory framework. The central argument is that artificial intelligence can enhance corporate security only if it is implemented responsibly, with appropriate human oversight, clear accountability, and continuous risk assessment.

Keywords: artificial intelligence; automated solutions; corporate security; risk management; machine learning; human oversight; AI Act

Dr. Ilina Kozarova-Armencheva, Assoc. Prof.
ORCID iD: 0009-0007-3670-755X
National and International Security Department
National Security and Defense Faculty
Rakovski National Defence College
82, Evlogi i Hristo Georgievi Blvd.
1504 Sofia, Bulgaria
E-mail: i.armencheva@rndc.bg

Dr. Miroslava Mladenova, Assist. Prof.
ORCID iD: 0000-0003-1349-3142
National and International Security Department
National Security and Defense Faculty
Rakovski National Defence College
82, Evlogi i Hristo Georgievi Blvd.
1504 Sofia, Bulgaria
E-mail: m.mladenova@rndc.bg

https://doi.org/10. 66334/annu26_stratprizm

ТЕОРЕТИЧНИ АСПЕКТИ НА СТРАТЕГИЧЕСКАТА СТАБИЛНОСТ ПРЕЗ ПРИЗМАТА НА СЪВРЕМЕННАТА СРЕДА НА СИГУРНОСТ

Йорданка Савова
Военна академия „Георги Стойков Раковски“

Абстракт. Стратегическата стабилност е сред основните теоретични категории, чрез които се обясняват механизмите за предотвратяване на стратегически конфликти и ограничаване на риска от неконтролирана ескалация между държавите. Класическата концепция се формира в условията на Студената война и е тясно свързана с двуполюсната структура на международната система, ядреното възпиране, стратегическия паритет и взаимната уязвимост. Целта на изследването е да се направи преглед и критичен анализ на основните ѝ постановки и да се идентифицират факторите, които ограничават приложимостта ѝ в съвременния стратегически контекст. Разглеждат се промените в международната система, развитието на военните технологии и нарастващото значение на киберпространството, космоса, информационната среда и изкуствения интелект. Основната теза е, че трансформацията на стратегическата среда налага преосмисляне на традиционните представи за стратегическа стабилност. Очертават се основата и направленията за последващо разработване на актуализирана концептуална рамка, съобразена с характера на стратегическите отношения през XXI век.

Ключови думи: стратегическа стабилност; ядрено възпиране; ядрени оръжия; стратегическа конкуренция; нови технологии

I. Увод

На 5 февруари 2026 г. изтече срокът на Договора между САЩ и Руската федерация за мерки за по-нататъшно съкращаване и ограничаване на стратегическите настъпателни въоръжения (New START) – последното действащо двустранно споразумение за контрол над ядрените арсенали на двете държави.[1] За пръв път от повече от половин век двете страни, които притежават около 90% от ядрените бойни глави в света, нямат правно обвързващи взаимни ограничения върху стратегическите си сили (Liang 2026; SIPRI 2026). Това се случва в контекста на все по-влошаваща се среда на сигурност, причинена от активните военни действия на територията на Украйна и в Близкия изток, от развитието на технологиите, наличието на нови домейни на съревнование и все по-размиващите се граници между война и мир.

В периода от края на Студената война до 2022 г., тоест над три десетилетия, потенциалното използване на ядрено оръжие и военни действия между две или повече ядрени сили изглеждаха почти невъзможно. С избледняването на спомените от последната голяма война, естествено водещо със себе си и все по-разпространеното незачитане на международното право и норми, както и с развитието на технологиите и влиянието на корпорациите върху правителствата на най-развитите държави, това започва да се променя. Използването на тактическо ядрено оръжие от страна на Русия е едно от най-честите опасения, изразявани в Украйна и на Запад. Президентът на Руската федерация Владимир Путин представя пред населението си войната срещу Украйна като война срещу НАТО и Запада, а с хибридните си действия срещу страните от Европейския съюз тества границите на чл. 5 от Северноатлантическия договор – деяния, които се водят под прага на въоръжен конфликт и при поддържана стратегическа двусмисленост (Bowen et al. 2026). В този контекст потенциалният пряк конфликт между две или повече ядрени сили започва да изглежда не само като възможна, но и като съвсем реалистична стъпка в бъдещото развитие на света.

В изучаването на международните отношения ядреното възпиране се анализира концептуално в рамките на теорията за стратегическа стабилност, която е и основната тема на този доклад. Целта на изследването е да се направи преглед и критичен анализ на основните ѝ постановки и да се идентифицират факторите, които ограничават приложимостта ѝ в съвременната международна среда. Разглеждат се промените в международната система, развитието на военните технологии и нарастващото значение

на киберпространството, космоса, информационната среда и изкуствения интелект. Основната теза е, че трансформацията на стратегическата среда налага преосмисляне на традиционните представи за стратегическа стабилност.

Стратегическата стабилност няма една общоприета дефиниция (Acton 2013; Kühn 2023). В литературата се разграничават две основни разбирания за нея. Тясното, кодифицирано в съвместното съветско-американско изявление от 1 юни 1990 г., определя стратегическата стабилност като състояние на стратегическите отношения, при което е премахнат стимулът за нанасяне на първи ядрен удар.[2] Широкото разбиране, застъпено и в западната литература, обхваща цялостното състояние на отношенията между великите сили, включително техните политически, икономически и технологични измерения. За целта на това проучване ще се използва по-широкото общо разбиране, че стратегическата стабилност означава липса на пряк въоръжен конфликт между две или повече ядрени сили. В доклада са използвани историко-логически подход и контент-анализ при краткото разглеждане на историческото развитие на теорията за стратегическа стабилност, както и при анализирането на факторите в съвременната среда на сигурност, които налагат преосмисляне на основните ѝ постановки.

II. Класическата теория за стратегическа стабилност

Предисторията на концепцията за стратегическа стабилност започва едва година след като първите атомни удари при нападението на САЩ над японските градове Хирошима и Нагасаки поставя края на Втората световна война. Това развитие във военната технология променя фундаментално природата на войната и поставя началото на Студената война. Естествено, ядрото на този прелом в международните отношения става обект на разсъждения от учени, анализатори и съветници по военните въпроси. В книгата *The Absolute Weapon* на Бърнард Броуди (Brodie 1946) може да се проследи най-ясното начално формиране на основната идея, съдържаща се в теорията за стратегическа стабилност, а именно – способността за втори удар. Неговият аргумент започва с разсъждението, че атомната бомба е абсолютно оръжие, тоест оръжие, срещу което няма ефективна отбранителна стратегия. На практика нападнатата държава не може да противодейства на удара. В този смисъл единственият метод на защита срещу това абсолютно оръжие е нападащата държава да знае със сигурност, че ще получи ответен удар. Поради това Броуди определя гарантирането на способнос-

тта за ответен (втори) ядрен удар в случай на нападение като най-важна стъпка в развитието на всяка програма за сигурност. В тезата, изразена в *The Absolute Weapon*, се съдържа зародишът на идеята за стратегическа стабилност, а именно че в ядрената епоха сигурността не зависи от броя налични ядрени глави в арсенала на един от двата тогавашни световни полюса, а от способността им да оцелеят след ядрено нападение и да гарантират възможността за изстрелване на ответен удар.

Малко по-късно Албърт Уолстетър в статията си *The Delicate Balance of Terror* за Foreign Affairs очертава конкретните способности, нужни на една държава, за да гарантира способността си за втори удар (Wohlstetter 1959). Тези способности се коренят в преодоляването на редица препятствия – силите за ответен удар да се поддържат в готовност в мирно време, да бъдат разположени така, че да могат да оцелеят вражески ядрен удар, да бъдат гарантирани комуникационните линии, така че да могат да получат заповед за изпълнението на ответния удар, да преодолеят отбраната на нападателя и да поразят целите си въпреки нея.

Томас Шелинг превръща логиката на гарантирането на способността за втори удар в обща теория и доразвива идеята за ядрено възпиране в трудовете си *The Reciprocal Fear of Surprise Attack* и *The Strategy of Conflict* (Schelling 1958; Schelling 1960). Той показва, че по време на международна криза самият страх от ядрено нападение може да доведе до война. Той дава следния практически пример, който да обясни тезата му – стопанин се изправя с пистолет пред въоръжен крадец: и двамата не искат да стрелят, но се страхуват, че другият ще стреля пръв. Именно този страх може да доведе до стрелба, тоест ситуацията се балансира или чрез изчакване и липса на действие, или чрез взаимно нападение. В този смисъл сигурният ответен удар на противника е в интерес и на самата страна, тъй като уязвимостта на съперника повишава риска от ескалация.

Включително противниците имат общ интерес да избегнат война, предизвикана от грешка или страх, поради което сътрудничеството между тях става възможно. Върху този взаимен интерес Шелинг и Халпърин изграждат теорията за контрола над въоръженията (Schelling & Halperin 1961). Впоследствие Карибската криза от 1962 г. показва колко близо до ядрена война може да доведе един момент на неяснота спрямо намеренията на противника, което от своя страна ускорява първите стъпки към сътрудничество, например установяването на пряка линия за връзка между Вашингтон и Москва, както и подписването на Договора за частична забрана на ядрените опити (Freedman & Michaels 2019).

Ядреното въоръжаване на САЩ и СССР е определящо за двуполюсния модел на Студената война. В този период и двете суперсили придобиват способността за нанасяне на неприемливи за противника загуби след претърпяване на първи ядрен удар. Гарантирането на ефективен втори удар и от двете страни води до състоянието на т.нар. „взаимно гарантирано унищожение“ (Freedman & Michaels 2019).

Робърт Джървис определя това състояние като ядрена революция: когато и двете страни са взаимно уязвими, военното превъзходство престава да носи политическа изгода, а сигурността се основава не на защитата, а на заплахата от възмездие (Jervis 1989). Кенет Уолц в *The Stability of a Bipolar World* обяснява защо биполярният свят може да съществува в положение на стабилност (Waltz 1964). Аргументът му е от структурен характер и не се ограничава единствено до ядрените оръжия. В двуполюсната система липсва периферия: всяка промяна, където и да е по света, засяга пряко двете свръхсили, поради което те взаимно следят внимателно действията си и реагират своевременно. Тяхното съперничество е ожесточено, но е и предвидимо, а честите кризи служат като механизъм за постепенна адаптация, а не като риск за ескалация. Идентичността на основния противник е ясна, което намалява риска от грешки, идващи от нестабилни съюзи. Превъзходството на двете сили над всички останали прави равновесието независимо от поведението на техните съюзници. Ядрените оръжия единствено засилват всички тези ефекти на двуполюсния свят. Тезата на Уолц се превръща в основна предпоставка на цялата концепция за стратегическа стабилност, а именно че тя се разглежда като взаимовръзка между две суперсили.

Глен Снайдер представя като противовес на теорията за двуполюсна стабилност своя парадокс „стабилност – нестабилност“. Това означава, че когато на високо стратегическо ниво страхът от ефективен ответен удар прави прекия конфликт невъзможен, толкова по-чести и големи са конфликтите на по-ниско ниво или така наречените прокси конфликти (Snyder 1965). Според този парадокс стратегическата стабилност предотвратява най-лошия сценарий, но не гарантира мира.

От края на 60-те до края на 70-те години се провеждат Преговорите за ограничаване на стратегическите оръжия (SALT). Тези преговори преминават през два основни етапа и достигат до важни международни споразумения, сред които договорът за противоракетна отбрана, който ограничава защитата и по този начин защитава взаимната уязвимост[3], и договорът за ограничаване на стратегическите настъпателни оръжия, поставящ конкретни тавани за броя на ядрените носители и бомбардировачите.

Паралелно с това съветската страна възприема концепцията за паритет и за „еднаква сигурност“ като основа на преговорите, което позволява двете страни да работят с обща, макар и не напълно съвпадаща, представа за стабилност (Garthoff 1978). Именно този дългогодишен процес довежда до единственото съгласувано определение на стратегическата стабилност – съвместното изявление от 1 юни 1990 г.

Десетилетие по-късно настъпва разпадът на СССР и съответно премахването на основната предпоставка на теорията за стратегическа стабилност – двуполюсния модел. В първите десетилетия след края на Студената война теорията за стратегическата стабилност остава на заден план и отстъпва на изучаването на международното сътрудничество, международните организации и международното право. В този смисъл може да се стигне до заключението, че краят на Студената война създава у учените и анализаторите оптимистично усещане за развитието на света. Традиционен пример за това е теорията на Франсис Фукуяма за „край на историята“ (Fukuyama 1992). Той определя случващото се не просто като край на Студената война, а като крайната точка в идеологическата еволюция на човечеството и утвърждаването на западната либерална демокрация като окончателна форма на управление.

III. Еволюция на теорията за стратегическа стабилност

Тази оптимистична оценка за бъдещето започва да се променя поради редица събития, които влошават международната среда на сигурност. Без претенция за изчерпателност, като такива могат да се определят анексирането на Крим от Русия през 2014 г., активизирането на терористичните организации и международния тероризъм, задълбочаването на стратегическото съперничество между САЩ и Китай, както и пълномащабното нахлуване на Русия в Украйна през февруари 2022 г. Към тях могат да бъдат добавени и нарастващото напрежение в Близкия изток след войната в Газа, започнала през 2023 г., както и американските удари срещу Иран. Друг основен фактор е засилването на конкуренцията между големите държави в икономическата, технологичната, военната и информационната сфера. Всички тези процеси и явления поставят под въпрос оптимистичните очаквания за постепенно разпространение и консолидиране на либерално-демократичния модел и насочват вниманието към възможността за възстановяване на геополитическото съперничество и фрагментацията на международната система. Поради това е нужно и преразглеждане на кон-

цепцията за стратегическа стабилност, така че тя да отговаря на особеностите на XXI век.

В своята същност теорията за стратегическата стабилност такава, каквато е изградена по време на Студената война, стъпва върху няколко основни предпоставки. Те са следните: светът е двуполюсен и между двата полюса съществува паритет, стабилността е ядрено-центрична, а решението за удар е рационално и базирано на ясна и достоверна информация. Както обаче стана ясно след края на Студената война и особено след края на оптимистичния поглед на Запада за развитието на света, международната система излиза от своя еднополюсен модел, в който предимство има САЩ, и навлиза в период на все по-ясно противопоставяне на различни центрове на власт. Като пример за това може да бъде посочена оценката на Стокхолмския международен институт за изследване на мира (SIPRI), според която към януари 2026 г. ядреният арсенал на Китай наброява около 620 бойни глави (SIPRI 2026). При три ядрени сили паритетът на Уолц губи ясния си смисъл, защото всяка страна трябва да съпоставя силите си с тези на двама потенциални противници едновременно и то ако изключим всички останали ядрени сили и техните намерения. В този смисъл системата достига такава степен на сложност, че оценката и проверката на военните ѝ възможности стават практически неосъществими. Този проблем е описан в литературата като преход към „втора ядрена епоха“, в която многостранните и асиметричните отношения не се поддават на двустранната логика на паритета (Koblentz 2014).

Допълнително може да се разгледа нивото на комплексност на новата среда на сигурност, като се погледне критично върху ядрено-центричния характер на историческата теория за стратегическа стабилност. Разбира се, технологичното развитие във военната сфера все още не е довело до създаването на оръжие с по-голяма разрушителна мощ от ядреното. Ако обаче се върнем към примера с крадеца и собственика, насочили пистолетите си един срещу друг, съществуват редица допълнителни фактори, които могат да нарушат крехкото равновесие на взаимното изчакване и да предизвикат изстрел, продиктуван от страх. През XXI век високоточни и хиперзвукови оръжия, противоракетна отбрана, противоспътникови и кибернетични средства могат да застрашат силите за ответен удар и системите за командване и управление (Chyba 2020; Futter & Zala 2021). Киър Либер и Дарил Прес показват, че съчетанието от точност и подобрени способности за разузнаване и откриване прави силите за ответен удар значително по-уязвими, отколкото по време на Студената война (Lieber & Press 2017), докато

противоракетната отбрана и противоспътниковите средства поставят под въпрос самата взаимна уязвимост (Morgan 2010).

Удар по системи с двойно предназначение в хода на конвенционален конфликт може да бъде разчетен като подготовка за първи удар, тъй като преплитането между ядрените и неядрените системи за командване, управление и ранно предупреждение създава риск от непреднамерена ескалация (Acton 2018). Освен това може да се върнем към предупреждението на Снайдер относно неговия парадокс „стабилност – нестабилност". Ако го приложим към съвременната ситуация, виждаме, че убеждението на ядрените сили, че използването на атомно оръжие не им дава предимство, подплатени и с десетилетия субективна липса на директен конфликт помежду им, водят до реално влошаваща се среда на сигурност. Пример за това са хибридните атаки на Руската федерация срещу Европейския съюз, които според някои анализатори тестват границата на активирането на чл. 5 от Северноатлантическия договор (Bowen et al. 2026).

Допълнителен проблем, който следва от развитието на технологиите през XXI век, е липсата на способност за атрибуция на дадено деяние, както и новите домейни на противоборство. В класическата теория за стратегическа стабилност съществува предпоставката за рационално решение, взето от хора, които разполагат с достатъчно време и достоверна информация. Само че в контекста на съвременната международна обстановка автоматизацията и все по-бързите средства за удар съкращават времето за решение и увеличават риска от ескалация поради грешка (Horowitz 2019). Дезинформацията и по-комплексните и успешни информационни операции могат да изкривят представата на ръководителите за действията на противника (Trinkunas, Lin & Loehrke 2020), а наличието на инструменти за водене на хибридна война води до липсата на ясна атрибуция и размиването на границата между война и мир (Gartzke & Lindsay 2017).

Същността на концепцията остава напълно валидно – докато всяка ядрена сила разполага със сигурен ответен удар, никоя няма стимул да удари първа. Преосмислянето следователно не означава отхвърляне на класическата теория и дефиниция, а разширяване на рамката около нейната същност.

IV. Изводи

1. Класическата теория за стратегическа стабилност се изгражда в условията на двуполюсната система на Студената война и се основава на

ядреното възпиране, взаимната уязвимост и гарантираната способност за втори удар. Тази логика запазва значението си и днес.

2. Промяната в структурата на международната система и появата на повече ядрени сили обаче поставят под въпрос разглеждането на стратегическата стабилност единствено като баланс между две суперсили и значително затрудняват измерването и предвиждането на поведението на отделните държави.

3. Размиването на границата между война и мир, трудностите при атрибуцията и нарастващото значение на информационните операции увеличават риска действията на противника да бъдат неправилно интерпретирани и да доведат до непреднамерена ескалация.

4. Поради това класическата теория не следва да бъде отхвърляна, а преосмислена и разширена – същността ѝ се запазва, но към нея трябва да бъдат добавени новите технологии, новите домейни и променената структура на международната система.

V. Заключение

Класическата теория за стратегическа стабилност продължава да има значение за разбирането на стратегическите отношения, но вече не е достатъчна, за да обясни сложността на съвременната среда за сигурност. Създадена в условията на двуполюсна система и ядрено противопоставяне между две суперсили, днес тя трябва да отчита нови ядрени държави, нови технологии и нови домейни на противоборство. Затова преосмислянето ѝ не означава отказ от принципа на ядреното възпиране, а разширяване на рамката, в която той се разглежда – основа, върху която може да бъде изградена по-актуална концепция за стратегическа стабилност, съобразена с особеностите на международните отношения през XXI век.

БЕЛЕЖКИ

1. Договор между Съединените американски щати и Руската федерация за мерки за по-нататъшно съкращаване и ограничаване на стратегическите настъпателни въоръжения (New START). Подписан в Прага на 8 април 2010 г., влязъл в сила на 5 февруари 2011 г., удължен до 5 февруари 2026 г.

2. Съвместно съветско-американско изявление за бъдещите преговори по ядрените и космическите въоръжения и за по-нататъшното укрепване на стратегическата стабилност (Soviet–United States Joint Statement on Future Negotiations on Nuclear and Space Arms and Further Enhancing Strategic Stability). Вашингтон, 1 юни 1990 г. Достъпно на: https://www.presidency.ucsb.edu/documents/soviet-united-states-joint-statement-future-negotiations-nuclear-and-space-arms-and [видяно на: 28.09.2026 г.].

3. Договор между Съединените американски щати и Съюза на съветските социалистически републики за ограничаване на системите за противоракетна отбрана (Treaty on the Limitation of Anti-Ballistic Missile Systems). Москва, 26 май 1972 г. Съединените щати се оттеглят от него на 13 юни 2002 г.

REFERENCES

ACTON, J.M., 2013. Reclaiming Strategic Stability. In: *Strategic Stability: Contending Interpretations*, pp. 117 – 146. Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press.

ACTON, J.M., 2018. Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War. *International Security*, vol. 43, no 1, pp. 56 – 99.

BOWEN, A.S.; GARDING, S.E.; MIX, D.E.; THEOHARY, C.A., 2026. *Russian Hybrid Warfare Activities in Europe: Considerations for Congress*. Congressional research service. Report R49134, 11 August 2026. Washington, DC: Library of Congress. Available from: https://www.congress.gov/crs-product/R49134. [viewed: 28.09.2026].

BRODIE, B. (ed.), 1946. *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt, Brace and Company.

CHYBA, C.F., 2020. New Technologies and Strategic Stability. *Daedalus*, vol. 149, no 2, pp. 150 – 170.

FREEDMAN, L. & MICHAELS, J., 2019. *The Evolution of Nuclear Strategy*. 4th ed. London: Palgrave Macmillan.

FUKUYAMA, F., 1992. *The End of History and the Last Man*. New York: Free Press.

FUTTER, A. & ZALA, B., 2021. Strategic Non-Nuclear Weapons and the Onset of a Third Nuclear Age. *European Journal of International Security*, vol. 6, no 3, pp. 257 – 277.

GARTHOFF, R.L., 1978. Mutual Deterrence and Strategic Arms Limitation in Soviet Policy. *International Security*, vol. 3, no 1, pp. 112 – 147.

GARTZKE, E. & LINDSAY, J.R., 2017. Thermonuclear Cyberwar. *Journal of Cybersecurity*, vol. 3, no 1, pp. 37 – 48.

HOROWITZ, M.C., 2019. When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence and Stability. *Journal of Strategic Studies*, vol. 42, no 6, pp. 764 – 788.

JERVIS, R., 1989. *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon*. Ithaca, NY: Cornell University Press.

KOBLENTZ, G.D., 2014. *Strategic Stability in the Second Nuclear Age. Council Special Report No. 71*. New York: Council on Foreign Relations. Available from: https://www.cfr.org/report/strategic-stability-second-nuclear-age. [viewed: 28.09.2026].

KÜHN, U., 2023. Strategic Stability in the 21st Century: An Introduction. *Journal for Peace and Nuclear Disarmament*, vol. 6, no 1, pp. 1 – 8.

LIANG, X., 2026. New START Expires As U.S. Urges "Modernized" Treaty. *Arms control association*, March 2026. Available from: https://www.armscontrol.org/act/2026-03/news/new-start-expires-us-urges-modernized-treaty. [viewed: 28.09.2026].

LIEBER, K.A. & PRESS, D.G., 2017. The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence. *International Security*, vol. 41, no 4, pp. 9 – 49.

MORGAN, F.E., 2010. *Deterrence and First-Strike Stability in Space: A Preliminary Assessment. MG-916-AF*. Santa Monica, CA: RAND Corporation. Available from: https://www.rand.org/pubs/monographs/MG916.html. [viewed: 28.09.2026].

SCHELLING, T.C. & HALPERIN, M.H., 1961. *Strategy and Arms Control*. New York: Twentieth Century Fund.

SCHELLING, T.C., 1958. *The Reciprocal Fear of Surprise Attack. P-1342*. Santa Monica, CA: RAND Corporation.

SCHELLING, T.C., 1960. *The Strategy of Conflict. Cambridge*, MA: Harvard University Press.

SIPRI [STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE], 2026. *SIPRI Yearbook 2026: Armaments, Disarmament and International Security*. Oxford: Oxford University Press. Available from: https://www.sipri.org/media/press-release/2026/increasing-focus-nuclear-weapons-amid-heightened-escalation-risks-new-sipri-yearbook-out-now. [viewed: 28.09.2026].

SNYDER, G.H., 1965. The Balance of Power and the Balance of Terror. In: SEABURY, P. (ed.). *The Balance of Power*, pp. 184 – 201. San Francisco: Chandler.

TRINKUNAS, H.A.; LIN, H.S. & LOEHRKE, B. (eds.), 2020. *Three Tweets to Midnight: Effects of the Global Information Ecosystem on the Risk of Nuclear Conflict*. Stanford, CA: Hoover Institution Press.

WALTZ, K.N., 1964. The Stability of a Bipolar World. *Daedalus*, vol. 93, no 3, pp. 881 – 909.

WOHLSTETTER, A., 1959. The Delicate Balance of Terror. *Foreign Affairs*, vol. 37, no 2, pp. 211 – 234.

THEORETICAL ASPECTS OF STRATEGIC STABILITY THROUGH THE PRISM OF THE CONTEMPORARY SECURITY ENVIRONMENT

Abstract. Strategic stability is one of the fundamental theoretical categories used to explain the mechanisms for preventing strategic conflicts and limiting the risk of uncontrolled escalation between states. The classical concept emerged during the Cold War and is inextricably linked to the bipolar structure of the international system, nuclear deterrence, strategic parity and mutual vulnerability. The aim of this study is to review and critically analyse the concept's core tenets and to identify the factors that limit its applicability in the contemporary strategic context. The paper examines changes in the international system, the evolution of military technologies and the growing significance of

cyberspace, outer space, the information environment and artificial intelligence. The central thesis is that the transformation of the strategic environment necessitates a rethinking of the established notions of strategic stability. The study outlines the foundations and directions for developing an updated conceptual framework aligned with the nature of strategic relations in the 21st century.

Keywords: strategic stability; nuclear deterrence; nuclear weapons; strategic competition; emerging technologies

Yordanka Savova
ORCID iD: 0009-0008-7449-2024
National and International Security Department
Rakovski National Defence College
82, Evlogi i Hristo Georgievi Blvd.
1504 Sofia, Bulgaria
E-mail: yo.g.savova1@rndc.bg

https://doi.org/10. 66334/annu26_ustformarisk

УСТОЙЧИВОСТТА КАТО ФОРМА ЗА НАМАЛЯВАНЕ НА РИСКА И НЕСИГУРНОСТТА ВЪВ ВОЕННОТО ДЕЛО

Калин Градев
Военна академия „Георги Стойков Раковски“

Абстракт. Държавните и европейските институции налагат устойчивостта като задължителен модел, който гарантира сигурност за обществото и икономиката. Тя се разглежда като фундаментален стратегически приоритет, обезпечаващ способността на държавата да предотвратява, поема и преодолява кризи. Тя изисква синергия между военния капацитет, гражданската готовност и икономическата стабилност, за да се осигури непрекъснатост на държавното управление и обществените функции във всяка ситуация. Устойчивостта във военното дело е различна за стратегическо, оперативно и тактическо ниво на командване и управление и притежава различни ключови показатели.

Ключови думи: устойчивост; съпротива; въоръжени сили; намаляване на риска

Стратегическият компас е план за действие, с който се установяват обща стратегическа визия и конкретни цели за укрепване на политиката на Европейския съюз (ЕС) за сигурност и отбрана до 2030 г. Той обхваща всички аспекти на политиката за сигурност и отбрана и е структуриран около четири стълба – да действаме, да защитаваме, да инвестираме и да си партнираме.

В официалните документи на Европейската комисия ясно се откроява промяна в подхода към сигурността и устойчивостта на Европейския съюз. След 2022 г. и началото на пълномащабната война в Украйна ЕС все по-категорично разглежда отбранителния си капацитет като неразделна част от своята стратегическа устойчивост.

Устойчивостта вече се приема за фундаментален стълб в съвременното планиране, обединяващ военни, технологични и граждански ресурси. Тя гарантира способността на една държава да устои, да се адаптира и бързо да се възстанови при кризи, въоръжени конфликти или хибридни заплахи. Как се е разглеждала, какви нови подходи или решения на съществуващи проблеми, свързани с устойчивостта, могат да предложат на аналитици и лидери, за да придобият представа за нейната приложимост ще е основната цел на тази публикация.

Според Клаузевиц[1] математическото уравнение за спечелване на война е **Устойчивост = Средства х Воля.** Всяко желание за съпротива срещу определен противник може по същество да се измерва чрез разполагаемите средства, умножени по количеството воля, която командирите, офицерите от щаба, формированията и отделните военнослужещи притежават. За да осигури тази устойчивост, използвайки наличните средства, личния състав е необходимо да притежава и определена подготовка. Без воля и умения за боравене с наличните средства те ще останат непотребни. Без наличните средства, обаче волята остава само прекалено силно желание. Ако устойчивостта се разгледа като актът на шофиране, тогава средството ще бъде автомобила, а волята – горивото.

На съвременния етап на развитие на човечеството отбранителният капацитет се вписва в стратегическата устойчивост, разпределен по следните ключови направления:

1. Концепцията за „Всеобхватна отбрана“ (Total Defence) – интеграция между армия и общество. Модерната стратегическа устойчивост изисква съвместни действия между въоръжените сили, държавните институции, частния сектор и гражданите (по модела на скандинавските страни и Балтийските републики[2]). Гражданската готовност се разглежда в контекста на подготовката на населението за реакция при кризи, засилва устойчивостта и намалява паниката, което прави обществото трудна мишена за психологически операции.

2. Защита на критичната инфраструктура. Военно-гражданска синергия и обвързаността на отбранителните способности гарантират физическата и кибернетичната защита на ключови обекти – енергийни мрежи,

транспортни възли, водоснабдяване и комуникационни системи. Тук се разглежда и логистичната устойчивост, като се обръща внимание на способността на армията да оперира и да поддържа веригите за доставки дори при частично разрушена инфраструктура, тъй като се явява критична за оцеляването на държавния апарат.

3. Индустриален капацитет и технологичен суверенитет. При това направление се акцентира върху устойчиви вериги на доставки, защото, както военните конфликти от последните години показват, стратегическата устойчивост зависи от местното производство на боеприпаси, техника и резервни части. Иновациите и технологиите с двойна употреба също са елемент на това направление, тъй като развитието на отбранителните технологии (дронове, изкуствен интелект, квантови комуникации) подхранва както военния капацитет, така и гражданската икономика и намалява зависимостта от чужди държави.

4. Възпиращ ефект (Deterrence). Предотвратяването на конфликти е основният елемент в това направление, поради факта че силният и модернизиран отбранителен капацитет повишава цената на евентуална агресия за всеки потенциален противник. Възпирането е най-добрата форма на устойчивост, тъй като запазва стабилността, без да се стига до разрушения.

За устойчивостта могат да се открият множество определения в различните сфери на обществения живот – екологична устойчивост, икономическа устойчивост, социална устойчивост, корпоративна устойчивост. В научните среди концепцията за устойчивост не е просто абстрактна идея, а обект на сериозни изследвания. Тя се изучава чрез т.нар. „наука за устойчивостта“ (Sustainability Science) – млада, интердисциплинарна научна област, която интегрира природните, социалните и инженерните науки с цел решаване на глобалните кризи.[3]

Най-разпространеното определение на „устойчивост“, дадено през 1937 г. от Александр Андронов и Лев Понтрягин, е „Свойство на дадена система да запазва основните си характеристики при относително малка промяна на даден параметър“. Синонимното гнездо на думата е твърде широко и включва твърдост, крепкост, здравина, якост, солидност, стабилност; покой, неподвижност; съпротивление, съпротивляемост, упоритост, издръжливост, закаленост, непоколебимост, резистентност; постоянство, неизменност, трайност; непоклатимост и стабилитет.

В националните документи, свързани с военното дело, „устойчивостта“ като термин „се заключава в способността отбраняващите се войски да отразят ударите и настъплението противника и упорито да

удържат отбраняваната територия“.[4] Според Доктрината на въоръжените сили[5] тя представлява поддържането на готовност и капацитет на въоръжените сили за провеждане на операции (включително и тяхното всестранно осигуряване и поддръжка) в отговор на кризи от различен характер, които могат да се проявят и без предварителни индикации. Нейната същност се състои в наличието на достатъчна и решителна бойна мощ за постигане на националните и колективните цели по възпиране и отбрана при всякакви обстоятелства в средата на сигурност. Устойчивостта се отнася предимно към две основни направления – устойчивост на системата за командване и управление и жизнеспособност (живучест) на войските на бойното поле.

Във военната сфера се срещат и множество други термини, обвързани с устойчивостта и отнасящи се както към определени качествени параметри на командири, щабове, формирования, техника, личен състав, така и за прилаганите от тях действия, дейности, мерки и мероприятия. Основните предизвикателства по отношение на определянето на устойчивостта на сегашния етап от развитието на военното дело идва и от разнообразието от термини на английски език, които се прилагат в съюзнически формат (Resilience, Resistance, Robustness и др.). В превод те придобиват коренно различно значение, като най-близо смислово са устойчивост (resilience), съпротива (resistance) и издръжливост (robustness).

Всеки от представените термини има различни значения и приложения. Устойчивостта (resilience) се отнася до способността на сила, система или нация **да отразява, да се адаптира и да се възстановява** от атаки, смущения или трудности. В това значение се включват аспекти като: способността на инфраструктурата да продължи да функционира след атака; капацитетът на всеки отделен военнослужещ да поддържа ефективност въпреки трудностите; киберустойчивост за издържане и възстановяване от цифрови заплахи; психологическа устойчивост в самите формирования да издържат на продължително водене на бойни действия и стрес.

Съпротивата (resistance) обикновено се отнася до **активното противопоставяне** срещу вражески или противникови сили[6]. То може да приеме различни форми: организирани съпротивителни движения (партизанска война или криминални мрежи); неконвенционалните действия, включително саботаж, събиране на разузнавателна информация от цивилни и бунтове; пасивна съпротива, например гражданско неподчинение или отказ от сътрудничество, както и скрита поддръжка на противниковите сили. В об-

общение, устойчивостта се характеризира със способността за издържане на неблагоприятни въздействия и възстановяване след тях, докато съпротивата предполага активно противопоставяне и целенасочено противодействие на тези въздействия.

Основната разлика в двата термина се определя от доктриналната база на НАТО като се отчита, че устойчивостта е способността на една нация или армия да абсорбира шокове, да се адаптира и да се възстанови от криза, докато съпротивата е активното противодействие и отблъскване на непосредствена заплаха или чужда окупация. И двата термина са стълбове на съвременната концепция за тотална отбрана в рамките на НАТО[7], но функционират в различни фази на операциите и са възприети и от други държави.

Въз основа на формулираните на 15.09.2026 г. седем **основни изисквания за устойчивост**[8] и съответните цели, определени за всяко от тях, може да се направи изводът, че „устойчивостта“ се характеризира преди всичко със способността за възстановяване след неблагоприятни въздействия, докато „съпротивата“ се изразява в способността на дадено формирование да запазва в значителна степен своята структура, функционалност и оперативни способности под въздействието на неблагоприятни фактори.

Другият термин, който се обвързва с устойчивостта, е „адаптивност“ (издръжливост) (robustness), те са атрибути на две различни конструкции. Способността за поддържане, справяне с определени предизвикателства, както и за удържане на определени обекти е свързана с устойчивостта, докато възможността за възстановяване или оттегляне с цел запазване на боеспособност е свързана с адаптивността (издръжливостта).

Издръжливостта представлява способността за адаптиране към бъдещи събития, характеризиращи се с висока степен на неопределеност, както и към непредвидени изменения в условията на обстановката, при запазване на възможността за постигане на първоначално определеното желано крайно състояние. Гъвкавостта е основен елемент на адаптивността и се разглежда, като способността да се отложи, изостави, разшири или развие всяка обстановка към желаната цел. Устойчивостта е способността на системата да се върне в първоначалното си състояние или да премине към ново желано състояние, след като е била нарушена.

Таблица 1. Сравнителен анализ по критерии

Критерий	***Resilience (Устойчивост)***	***Resistance (Съпротива)***	***Robustness (жизнеспособност/ издръжливост)***
Основен фокус	Абсорбиране на удара, адаптация и бързо възстановяване на критичните функции	Активно отблъскване и противодействие на противникови сили	Устояване на удара
Времеви обхват	Дългосрочен и превантивен – изгражда се преди конфликта и продължава след него	Реактивен и оперативен – активира се по време на атака или окупация	Преди и по време на събитието
Обхват	Цялото общество (инфраструктура, институции, киберзащита, логистика, психология на населението)	Военни и нетрадиционни мрежи (партизански действия, специални сили, саботажи, криминални движения)	Остават твърди и непроменени
Цел	Да се поддържа жизнеспособността на формированието под силен натиск	Да се направи цената на окупацията непосилна за противника	Предотвратяване на срив от известни рискове

В процеса на планиране на операциите и тактическите действия (съгласно стандартите на НАТО и българските доктрини) за осигуряване на устойчивост и гъвкавост винаги се разработват частни планове (Branch Plans) и последващи планове (Sequel Plans), които са гръбнакът на управлението на риска и изненадата на бойното поле. Частните планове имат за цел справяне с неочаквани промени на условията на обстановката[9], които възникват по време на текущата фаза на операцията (например неочакван пробив на противника, загуба на връзка с формирования по фланга), така че да се продължи изпълнението на поставената мисия. Чрез него се търси управление на устойчивостта.

Последващите планове определят „какво следва след това“ и се прилагат въз основа на изхода от текущите действия (независимо дали са успешни или неуспешни). Те са насочени към запазване на жизнеспособността или издръжливостта.

Устойчивостта означава способността на дадена структура (органи-

зация, ведомство, щаб, формирование индивид) да поддържа определен курс на действие и да се приспособява към непредвидени условни събития (условия на обстановката). Гъвкавостта представлява способността за приспособяване към непредвидени външни събития чрез промяна на посоката и с готовност за отклонение от първоначалния курс. В действителност никоя стратегия не трябва да се гради изцяло върху устойчивостта или изцяло върху гъвкавостта, а е необходимо да има сливане между двете. В други интерпретации на термините се отстоява тезата, че устойчивостта е способността за бързо възстановяване от трудности, гъвкавостта е желанието за промяна, а адаптивността е способността за приспособяване към новите условия.[10]

Може да се каже, че гъвкавостта е реакция на адаптивността, която е решаващ компонент на устойчивостта. Военнослужещите ще бъдат много по-подготвени да реагират на трудности или предизвикателства, ако се научат да бъдат по-гъвкави. Осъзнаването на преходния характер на явленията и непрекъснатата изменчивост на условията на обстановката е предпоставка за развиването на гъвкавост у командирите, която им позволява да се адаптират към промените и да запазват способността си за ефективно вземане на решения и действие дори в условията на значителен натиск. В обобщение, командирите, щабовете и отделните военнослужещи с добре развити умения за устойчивост и гъвкавост са в състояние да повярват в себе си и в способността си да управляват ефективно и да отговарят на предизвикателствата, породени от промените в обстановката.

Възниква въпросът как могат да бъдат изградени и развити устойчивостта и гъвкавостта. Устойчивостта представлява динамичен процес, който може да бъде усъвършенстван и затвърждаван чрез прилагането на различни методи за подготовка. Нейното проявление има специфични особености при командирите, щабовете и формированията, което налага провеждането както на индивидуална, така и на колективна подготовка.

Участието на командирите в курсове за надграждане на подготовката е възможно най-добрият подход. За щабовете е уместно включването в международни щабни тренировки. Командно-щабни учения и военни игри на различна тематика и промяна в условията на оперативната и тактическата обстановка предоставят възможност за развитие на по-силна устойчивост. Превръщането на всяка ситуация във възможност за учене, описване на поуките от практиката и коригиране на допуснатите грешки следва да бъде приоритет на всеки командир, желаещ да развива устойчивостта у подчинените си. При срещата с различни гледни точки и предизвикване на

собствените способности за вземане на решения ще се тренират адаптивността, критичното мислене и възможността за търсене на нови подходи за действие. Това води до развитие на гъвкавостта у командирите, щабовете и отделните военнослужещи.. Колкото са по-устойчиви военнослужещите, толкова по-адекватно ще използват трудните събития като възможност да се отворят към нови подходи за постигане на победа.

На въпроса какви са ползите от укрепването на устойчивостта и гъвкавостта, могат да се изтъкнат като отговори постигането на по-добри резултати; придобиването на по-добра адаптивност в различни условия на обстановката; по-добро самочувствие и емоционален контрол и самоконтрол; по-добро управление на стреса и напрежението, породено от участието в бойните действия; по-добри взаимоотношения с другите и -подобрени способности за решаване на проблеми дори в ситуации на високо напрежение.

От всичко казано дотук следва, че е удачно да се възприемат определени показатели за ефективност, които ще доведат до повишаването на устойчивостта на формированията. **Ключовите показатели за ефективност** (KPI) за формированията от Сухопътните войски (СВ) са насочени предимно към измерване на огневата мощ, тактическата мобилност, оперативната съвместимост със съюзниците от НАТО и логистичната издръжливост.

Показателите могат да се подразделят на четири основни направления със съответните критерии:

1. Оперативна готовност и време за развръщане:

– времето за реакция (Notice to Move) се определя от максималният брой часове/дни, необходими за привеждане на дадено тактическо формирование (например батальонна бойна група) в пълна бойна готовност за развръщане;

– процентът на окомплектоване (Personnel Fill Rate) е съотношението между реално наличния личен състав в бойните части и щатния състав по военновременен разчет;

– показател за развръщане (Deployability) е процентът от общия състав на формированието, който е обучен, оборудван и сертифициран за реално участие в предстояща операция.

2. Бойна изправност и техническо осигуряване:

– коефициентът на техническа изправност (Mission Capable Rate) се определя от дела на бойните бронирани машини (ББМ), танковете и артилерийските системи, които са в пълна готовност за незабавно изпълнение на бойни задачи;

– логистичният капацитет за автономност (Sustainability) се определя от броя дни, в които дадено формирование може да води бойни действия без външно снабдяване (с отчитане минимум на запаси от боеприпаси, гориво-смазочни материали и медицински консумативи);

– време за техническо възстановяване (Mean Time to Repair) – средното време за ремонт и връщане в строя на повредена техника от полевите ремонтни органи.

3. Подготовка и съвместимост:

– интензивност на тактическата подготовка, която да отчита броя на часове полеви учения за една година за всеки военнослужещ, както и брой проведени батальонни и ротни тактически учения (като например „БАЛКАН“ или „STRIKE BACK“);

– стандартизацията по STANAG е критерий, който следва да се оценява чрез процентния дял на комуникационните и информационните системи, напълно интегрирани със системите за командване и контрол на НАТО (напр. цифрова интеграция на тактическо ниво);

– огневата ефективност се определя от резултатите от подготвителните, контролните и бойните стрелби – процент на поразените цели в нормативно време при симулирани бойни условия.

4. Управление на личния състав:

– физическата и медицинската годност се определят като процент от състава, успешно покрил годишните изпити за физическа подготовка и медицинските стандарти;

– коефициентът на текучество е процентът на напускащите военнослужещи спрямо новоназначените, което е критично за нивата на дефицит във всяко формирование от Сухопътните войски.

Устойчивостта, адаптивността и гъвкавостта са възприемани като ключови качества на концептуалния компонент, определен за основата на постигането на превъзходство при използването на съществуващите и нововъзникващите технологии и следва да се търсят възможности за подпомагането на развитието им във всички направления на военното дело. Поддържането на висок боен дух е една от най-важните предпоставки за успех във военни действия. Той е резултат от реалистична подготовка, когнитивна устойчивост, увереност в ефективността на въоръжението и оборудването, доверие в командирите, себеуважение, дисциплина и ясно разбиране на ситуацията и задачите.

БЕЛЕЖКИ

1. „Ако искаме да победим врага, трябва да съразмерим нашите усилия с неговата сила на съпротива. Тя се изразява като произведение от два фактора, които не могат да бъдат разделени: сумата от наличните средства и силата на волята“.

2. Моделът за устойчивост на скандинавските страни и Балтийските републики (често разглеждани заедно в рамките на регионалния формат NB8 – Nordic-Baltic Eight) представлява уникална комбинация от икономическа конкурентоспособност, социално благополучие и дългосрочна екологична и дигитална трансформация.

3. How science can help to create a sustainable world. *Unesco*. Available from: https://www.unesco.org/en/articles/how-science-can-help-create-sustainable-world.

4. Боен устав на механизиран (танков) батальон, 1996. София: Издателство на Министерство на отбраната.

5. Министерство на отбраната на Република България, 2025. Доктрина на въоръжените сили на Република България (НП-01). Одобрена със Заповед на министъра на отбраната № ОХ-1126 от 3 декември 2025 г.

6. НП-3.2 Доктрина за сухопътни операции, 2025.

7. Доктрина на НАТО (ROC – Resistance Operating Concept).

8. NATO, 2026. Resilience Baseline Requirements 15 September 2026. Available from: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/09/15/2026-resilience-baseline-requirements.

9. „Условия на обстановката“ е термин прилаган на тактическо ниво и се определя от факторите: противник, собствени сили, терен, време, климат и цивилно население.

10. Rosaury V., 2023. Is Resiliency equal to Flexibility? Do they make you more adaptable? *Linkedin*. Available from: https://www.linkedin.com/pulse/resiliency-equal-flexibility-do-make-you-more-adaptable-rosaury-viaje/.

11. Европейски съвет. Съвет на Европейския съюз. *Стратегически компас за сигурността и отбраната*. Достъпно на: https://www.consilium.europa.eu/bg/policies/strategic-compass/.

12. HUSDAL, J., 2004. Flexibility and robustness as options to reduce risk and uncertainty. *Husdal.com*. Available from: https://husdal.com/2004/12/15/flexibility-and-robustness-as-options-to-reduce-risk-and-uncertainty.

13. MUNOZ, A.; BILLSBERRY, J. & AMBROSINI, V., 2022. Resilience, robustness, and antifragility: Towards an appreciation of distinct organizational responses to adversity. *International Journal of Management Reviews*, vol. 24, pp. 181 – 187. Available from: https://doi.org/10.1111/ijmr.12289.

14. BURNARD, K. & BHAMRA, R., 2011. Organisational resilience: Development of a conceptual framework for organisational responses. *International Journal of Production Research*, vol. 49, pp. 5581-5599. Available from: DOI: 10.1080/00207543.2011.563827.

15. ROUVROIJE, M., 2025. The Resistance Operating Concept's Deterrent to Impress: Distinct Causal Theories of Success. In: *European Security Studies Conference*

(EISS). Available from: https://eiss-europa.com/papers/2025-the-resistance-operating-concept-s-deterrent-to-impress-distinct-causal-theories.html.

16. CLAUSEWITZ, C., 1999. *On War*. Translated by J. J. Graham. Abridged and edited with an introduction by L. Willmot. Ware: Wordsworth Editions.

RESILIENCE AS A FORM OF REDUCING RISK AND UNCERTAINTY IN THE MILITARY SPHERE

Abstract. State and European institutions impose resilience as a mandatory model that guarantees security for society and the economy. It is seen as a fundamental strategic priority that guarantees the state‘s ability to prevent, absorb and overcome crises. It requires synergy between military capacity, civil preparedness and economic stability to ensure the continuity of state governance and public functions in any situation. Resilience in military affairs is different for strategic, operational and tactical levels of command and control and has different key indicators.

Keywords: resilience; resistance; armed forces; risk reduction

Colonel Dr. Kalin Gradev, Assoc. Prof.
ORCID iD: 0000-0002-5436-1173
Command and Staff Faculty
Rakovski National Defence College
82, Evlogi & Hristo Georgievi Blvd.
E-mail: k.gradev@rndc.bg

https://doi.org/10. 66334/annu26_adaptsystdef

АДАПТАЦИЯТА НА СИСТЕМИТЕ ЗА ОТБРАНА В БЪЛГАРСКАТА АРМИЯ И ПРЕДИЗВИКАТЕЛСТВАТА ПРЕД СУХОПЪТНИТЕ ВОЙСКИ

Калин Градев
Военна академия „Георги Стойков Раковски“

Абстракт. Адаптацията на системите за отбрана и сигурност е процес на непрекъсната трансформация, продиктуван от динамичната геополитическа обстановка. Тя включва модернизация на въоръжените сили, технологични иновации, съвместимост с колективната отбрана на НАТО и ЕС, и засилване на киберсигурността и устойчивостта на критичната инфраструктура. Разкриването на направленията за осъществяването на този нелек процес ще подпомогне обществото в познавателния контекст за основните елементи по планирането и прилагането му.

Ключови думи: системи за отбрана; приоритети, модернизация; Сухопътни войски

Представянето на конкретни приоритети и направления за развитие на военния инструмент на мощта (въоръжените сили) и отбранителните способности на държавата е обвързано с доктриналните документи на оперативно ниво. Те са своеобразният мост между стратегия и практика и заемат централно място в йерархията на документите, именно защото трансформират политико-стратегическите цели в разбираеми принципи

за използване на наличните способности и за планиране и провеждане на операции. По този начин се осигурява връзката между общата политика за сигурност и практическото развитие на системата за отбрана.

Ключовите направления в адаптацията на отбранителните способности включват: „Модернизация“, „Европейска интеграция“, „Наука и иновации“ и „Адаптация на отбранителните планове“.

Модернизация на отбранителните способности: Придобиване на ново поколение бойна техника и системи за противовъздушна отбрана, които са обвързани с актуалните проекти и програми на правителството и на Министерството на отбраната на Република България.

Европейска интеграция: Хармонизиране на националните стратегии с Общата политика за сигурност и отбрана на Европейския съюз, която цели подобряване на средствата за защита и надеждно възпиране.

Наука и иновации: Интегриране на изследванията и космическите технологии за управление на риска чрез Центъра за изследвания по национална сигурност и отбрана към БАН, научни изследвания във висшите военни и други образователни институции, дейности по подобряване на доктриналната база и приобщаване на бизнеса към развитие в това направление.

Адаптация на отбранителните планове: Съгласуване на способностите и мащабни инициативи с глобалните геостратегически приоритети и партньори, свързани с дейността на Министерството на отбраната и отговорности на Щаба на отбраната, Съвместното командване на силите и видовете въоръжени сили.

В сферата на отбраната на Република България се реализира мащабна модернизация, подкрепена от бюджет за отбрана в размер на 2,25% от БВП, с дългосрочен план за достигане на 5% до 2035 г. Стратегическата цел е ускореното превъоръжаване на трите основни вида въоръжени сили и постигане на пълна оперативна съвместимост в рамките на НАТО.

Стратегическата рамка, в която се реализира отбранителната политика на страната включва:

Конституцията и законите на страната;

Националните и съюзни стратегически документи на сигурността и отбраната[1];

Глобална стратегия за външната политика и политиката на сигурност на ЕС[2];

Стратегически компас на ЕС[3];

Регламент (ЕС) 2025/1106 на Съвета от 27 май 2025 г. за създаване на

инструмента „Мерки за сигурността на Европа (SAFE) чрез укрепване на европейската отбранителна промишленост“;

Програмите и плановете за развитие на въоръжените сили[4] и техните способности;

Декларираните и одобрени от Народното събрание „Численост на въоръжените сили“ и „Ниво на политическа амбиция в отбраната“;

Ресурсната макрорамка и прогнозите за развитие на икономиката;

Програмата за управление на правителството.

В края на август 2026 г. се представи и Управленска програма на правителството 2030 г. Раздел 9: Отбрана, в която са засегнати следните приоритети[5]:

Приоритет 9.1. Кадрова и социална политика. Мерки в изпълнителната власт;

Приоритет 9.2. Активно участие и изпълнение на поетите от Република България съюзни ангажименти;

Приоритет 9.3. Модернизация на въоръжението и техниката на Българската армия;

Приоритет 9.4. Инфраструктура в отбраната;

Приоритет 9.5.Трансформация на отбраната чрез внедряване на съвременни технологии с висок асиметричен ефект.

Отбранителна индустрия в България – Активно се интегрира в новата Програма за европейска отбранителна индустрия (EDIP) на ЕС, която стимулира съвместни иновации и поръчки между държавите членки с цел намаляване на външните зависимости. Основният въпрос е включването до инициативата на Европейския съюз „Действия за сигурност за Европа“ (SAFE) с бюджет от 150 милиарда евро, която има ключово значение за укрепването на европейските отбранителни способности.

Военновъздушни сили (ВВС) – Усвояване на изтребители F-16 Block 70: ключов фокус е подготовката на инфраструктурата и състава за оперативно въвеждане в експлоатация на новата ескадрила. Развитие на ПВО способности: осигуряване на съвременни средства за защита на въздушното пространство. Важен елемент е и противодействие на безпилотни летателни системи (БЛС), като в тази насока е модернизирането на нормативната уредба за използване на кинетични и некинетични средства за борба с БЛС около стратегически обекти.

Военноморски сили (ВМС) – Придобиване на многофункционални модулни патрулни кораби, с цел изграждане на способности за надводна и подводна защита в акваторията на Черно море. За бреговите ракетни

комплекси е договорено придобиване на нови противокорабни системи от САЩ с цел модернизация на бреговата отбрана.

Сухопътни войски – Бойна техника за батальонни групи: изграждане на съвсем нови механизирани формирования чрез придобиване на съвременни бойни машини от последно поколение (вкл. машините Stryker). Преодоляване на кадровия дефицит: прилагат се програми насочени за намаляване на некомплекта от военнослужещи, като най-осезаем напредък се отчита при окомплектоването на войнишкия състав.

„Страйкър“ (Stryker) е семейство от осемколесни (8x8) високомобилни бойни бронирани машини, които съставляват гръбнака на текущата модернизация на Сухопътните войски на България. През есента на 2023 г. държавата сключи мащабен договор със САЩ за придобиването на общо 198 машини, от които 183 броя са от фамилията Stryker.

Проектът навлиза в решителна фаза с ключови събития по доставката и усвояването на техниката, като разработеният график на доставките се спазва и първата партида от пет машини „Страйкър“ официално пристигнаха на пристанище Бургас през февруари 2026 г. Публичния дебют се състоя през юни 2026 г., когато първият български Stryker беше официално демонстриран пред обществеността по време на международното изложение „Хемус 2026“ в Пловдив. В плана за 2026 г., Българската армия очаква да приеме общо 33 бойни машини в рамките на настоящата календарна година. Всичките 183 бр. машини – пълният комплект – трябва да бъдат доставени до началото на 2028 г., като се очаква те да са основата за формиране на батальонни бойни групи.

Индустриално сътрудничество и логистика – Обвързано е с финалното асемблиране на собствена територия. Въпреки, че машините пристигат от САЩ и Канада, те се сглобяват финално в държавния завод „ТЕРЕМ – Хан Крум“ във Велико Търново. За целта в предприятието бяха инвестирани 17 млн. лв. за подготовка на линиите.

Как ще се осъществи разпределението им също е известно, като първите готови и окомплектовани машини са предназначени за нуждите на 61-ва механизирана бригада в Карлово. Обучението се осъществява от мобилни тренировъчни екипи от Националната гвардия на САЩ (с участието на Вашингтон и Тенеси), които провеждат интензивна подготовка на българския личен състав за експлоатация и поддръжка на платформите. През юли[6] се проведоха и множество визити, на които бяха разгледани актуални въпроси, свързани с двустранното военно сътрудничество, съвместната подготовка и модернизацията на формированията на Сухопътните войски

Модификациите и въоръжението на бойните машини включва различни конфигурации на платформата с цел пълноценно оборудване на механизираните ни формирования:

Бойни машини на пехотата (XM1296 Dragoon) – оборудвани с 30-мм автоматично оръдие Bushmaster за висока огнева мощ;

Командно-щабни машини (M1130), осигуряващи оперативното управление и координация на бойното поле;

Медицински евакуационни машини (M1133) – предназначени за бърза и защитена евакуация на ранени;

Инженерни и спомагателни модификации – включва и широк спектър от машини, включително и машини за ядрена, химическа и биологична защита (ЯХБЗ).

По искане на страната ни, машините са заявени с допълнителна подсилена балистична защита (V-образно дъно срещу мини и импровизирани взривни устройства) и съвременна система за управление на боя (BMS).

Българските машини „Страйкър“ се придобиват със съвременно въоръжение, боеприпаси и цифрово оборудване, които се интегрират поетапно в завод „ТЕРЕМ – Хан Крум“ във Велико Търново. Интеграцията обхваща три основни направления:

Оръжейни системи и огнева мощ. Основното въоръжение на бойните модификации (XM1296 Dragoon) са 30-мм автоматични оръдия Bushmaster, които осигуряват поразяване на лекобронирана техника и жива сила на големи разстояния. Противотанкови ракетни комплекси Javelin („Джавелин“) също са включени, като част от машините ще бъдат оборудвани с пускови установки за тези ракети, което позволява унищожаването на тежки танкове по метода „стреляй и забрави“. Дистанционно управляеми оръжейни станции (RCWS), от своя страна, позволяват на екипажа да произвежда огън с картечници (напр. 12.7-мм) от вътрешността на корпуса, без да се излага на вражески обстрел.

Комуникации и управление (C4ISR). Система за управление на боя (BMS) осигурява и софтуер и хардуер за цифрово картографиране, които обменят данни за тактическата обстановка в реално време между отделните машини, пехотата и щаба и командирите. Радиостанции Harris са съвременни криптирани тактически радиосистеми за обмяна на глас и данни, като екипи за обучение още в началото на септември тази година пристъпиха към обучение на българските военнослужещи от 61-ва механизирана бригада. Те гарантират пълна съвместимост и сигурна връзка с останалите съюзници в НАТО. Прилагането на навигационни системи (DAGR) се

осъществява посредством защитени военни GPS приемници, устойчиви на електронно заглушаване.

Системи за защита и сигурност. Предвижда се да се придобият и допълнителни бронирани модули, които да предоставят възможност за интегриране на пакетирана балистична защита срещу осколки и снаряди, както и противоминни седалки за екипажа. Очаква се системите за откриване и предупреждение за лазерно облъчване да алармират екипажите, ако машината попадне под прицел на вражески ракети, и автоматично задействат димни гранати за маскировка.

Филтро-вентилационни уредби за предотвратяване на ЯХБ заплахи представляват специализирано оборудване на машини за защита на личния състав при ядрено, химическо или биологично заразяване.

Българските фирми и поддръжката на новопридобитите машини се очаква „да стъпят“ на основния стълб на индустриалното сътрудничество – държавният холдинг „ТЕРЕМ“. Дейностите по поддръжката и доставките са структурирани по следния начин:

Локално във Велико Търново: машините се приемат като сглобени шасита (с двигател, трансмисия и шаси), а в завода се извършва финалното доокомплектоване, монтажът на въоръжението, радиостанциите Harris и оптичните прибори;

За производство на боеприпаси у нас е постигнато споразумение с американския производител General Dynamics, като в заводите на „ТЕРЕМ“ се изграждат мощности за лицензирано производство на четири типа 30-милиметрови боеприпаси за оръдията Bushmaster;

Договорът предвижда българското предприятие да се превърне в сертифициран регионален център за дългосрочен ремонт и поддръжка на машини „Страйкър“, обслужващ Източния фланг на НАТО.

Процесът по сертифициране на първите боеспособни формирования (батальоните) следва стриктен график, обвързан с доставките на техниката:

Първоначална подготовка (2026 г.) започна още с пристигането на първите машини през февруари 2026 г., като започна и интензивно тактическо обучение на екипажите от 61-ва механизирана бригада в Карлово.

Сформиране на батальонни групи (2027 г.) се очаква да приключи до края на следващата година, когато по-голямата част от планираните 183 машини ще бъдат сглобени и Сухопътните войски ще разполагат с напълно окомплектована първа батальонна група.

Пълна оперативна готовност (2028 г.). Пълната сертификация на трите батальонни групи по стандартите на НАТО (CREVAL) е планирана за

началото на 2028 г., като тогава приключват и финалните доставки на машините по договора. Сертифицирането ще бъде запечатано по време на мащабни многонационални учения (като традиционните "Strike Back" на полигон Ново село).

В крайна сметка, при достатъчно добра организация и спазване на установените срокове, очакваните ефекти от страна на правителството се изразяват в:

Подобрен социален статус на българските военнослужещи.

Увеличени разходи за отбрана.

Промени в законовата уредба, свързана с отбраната, резерва на въоръжените сили и реализиране на проектите в структурите на Министерство на отбраната.

Изпълнени количествени и качествени изисквания на Пакет Цели по способностите на НАТО 2025 за Република България.

Напълно реализирани проекти за придобиване на въоръжение и техника.

Напълно изградена инфраструктура за приемане и експлоатиране на новопридобитите платформи.

Ефективно и дигитално управление на собствеността на Министерството на отбраната и структурите към него и въвеждане на строг контрол и надзор върху изпълняваните проекти.

Обновени стратегически документи за развитие на отбранителните способности.

Придобити пълни способности за борба с последствията от бедствия, аварии и катастрофи.

Внедрени съвременни технологии с висок асиметричен ефект.

Увеличен броя на проекти с българско участие по EDF, EDPCI, EDIP и други европейски инструменти в подкрепа на сектора.

БЕЛЕЖКИ

1. НС, 2018. Актуализирана стратегия за национална сигурност на Република България, [приета с Решение на НС от 14.03.2018 г.]. *Държавен вестник*, бр. 26 от 23.03.2018 г. София; МО, 2025. *Национална отбранителна стратегия*, [приета с РМС № 131 от 06.03.2025 г.]. София; *Стратегическа концепция на НАТО*, [приета на 29 юни 2022 г. по време на Срещата на върха на Алианса в Мадрид]. [online]. Available from: https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf target="_blank".

2. [online]. Available from: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf target="_blank".

3. [online]. Available from: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT /en/pdf target="_blank";

[online]. Available from: https://www.consilium.europa.eu/bg/policies/strategic-compass/.

4. МО, 2021. *Програма за развитие на отбранителните способности на въоръжените сили на Република България 2032 и План за развитие на Въоръжените сили на Република България до 2026 г.* [онлайн]. Достъпно на: https://www.strategy.bg/bg/strategy-documents/1566. София.

5. МС, 2026.*Управленска програма на правителството 2030 г.*, Раздел 9: Отбрана, [21 август 2026]. [онлайн]. Достъпно на: https://armymedia.bg/2026/08/21/%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D1%81%D0%BA%D0%B0-%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0-%D0%BD%D0%B0-%D0%BF%D1%80%D0%B0%D0%B2%D0%B8%D1%82%D0%B5%D0%BB%D1%81%D1%82%D0%B2/. София.

6. Върховният главнокомандващ на Обединените въоръжени сили на НАТО в Европа генерал Алексъс Гринкевич бе на посещение в България на 1 юли по покана на началника на отбраната адмирал Емил Ефтимов. На 7 юли 2026 г. официална делегация от Националната гвардия на щата Тенеси, водена от генерал-майор Трент Скейтс (заместник-генерал-адютант), посети Съвместното командване на силите (СКС) в България.

На 9 юли в щаба на Сухопътните войски се прие официална делегация от 278-и кавалерийски полк на Националната гвардия на щата Тенеси, Съединени американски щати водена от командира на полка полковник Дони Хебел. По време на визитата са разгледани актуални въпроси, свързани с двустранното военно сътрудничество, съвместната подготовка и модернизацията на формированията на Сухопътните войски.

7. МО, 2017. *Доктрина на въоръжените сили на Република България (НП-01(А)*, с. 10. [онлайн]. Достъпно на: https://www.mod.bg/bg/doc/zapovedi/2012/20120130_OX057_DoktrinaVSRB.pdf. София.

8. МО, 2020. *Доктрина за сухопътни операции (НП-3.2(А)*. София.

9. МО, 2016. *Национална отбранителна стратегия*, [приета с РМС № 283 от 18 април 2016 г. и е официално отменена през 2025 г.]. София.

10. МС, 2026. *Програма за управление на Република България 2026 г. – 2030 г.*, [приета с РМС № 612 от 12 август 2026 г.]. [онлайн]. Достъпно на: https://www.gov.bg/special/bg/pravitelstvo/programa-za-upravlenie-na-republika-balgariya-2026-g-2030-g/programa-za-upravlenie-na-republika-balgariya-2026-g-2030-g.

11. МО, 2019. *Ръководство за планиране на отбраната, базирано на способности*. София.

12. НС, 2026. Доклад за изпълнение на Програмата за инвестиции в отбраната до 2032 г. през 2025 г. [онлайн]. Достъпно на: https://www.parliament.bg/pub/plenary_documents/52-602-00-29_.pdf. София.

13. ANGELOV, G., 2022, Nyakoi aspekti na natsionalnata mosht na savremennata darzhava. In. *Natsionalna sigurnost*, 2-ro izd., vol. 11, pp. 15 – 20. Sofia : Viktori izdat. ISSN 2682-941X ISSN 2682-9983. [in Bulgarian].

14. DIMITROVA, M. & SPASOVA, A., 1980. *Sinonimen rechnik na savremennia balgarski knizhoven ezik*, pp. 111, 564. Sofia: BAN. ISBN 954-02-0256-6. [in Bulgarian].

15. TAGAREV, T. & KOLEKTIV, 2012. *Metodologia za planirane na voennovremenni otbranitelni sposobnosti.* Sofia: Tsentar po menidzhmant na sigurnostta i otbranata. ISBN 978-954-91700-4-7. [in Bulgarian].

THE ADAPTATION OF DEFENSE SYSTEMS IN THE BULGARIAN ARMY AND THE CHALLENGES FACING THE LAND FORCES

Abstract. The adaptation of defense and security systems is a process of continuous transformation, dictated by the dynamic geopolitical environment. It includes modernization of the armed forces, technological innovations, compatibility with the collective defense of NATO and the EU, and strengthening cybersecurity and the resilience of critical infrastructure. The disclosure of the directions for the implementation of this difficult process will help society in the cognitive context of the main elements of its planning and implementation.

Keywords: defense systems, priorities, modernization, Land Forces

Colonel Dr. Kalin Gradev, Assoc. Prof.
ORCID iD: 0000-0002-5436-1173
Command and Staff Faculty
Rakovski National Defence College
82, Evlogi i Hristo Georgievi Blvd.
1504 Sofia, Bulgaria
E-mail: k.gradev@rndc.bg

https://doi.org/10. 66334/annu26_macrosec

ВЛИЯНИЕ НА МАКРОИКОНОМИЧЕСКАТА СРЕДА ВЪРХУ СИГУРНОСТТА И ОТБРАНАТА

доц. Катя Пейчева
Военна академия „Георги Стойков Раковски“

Абстракт. Устойчивата икономическа база е фундаментална предпоставка за ефективното функциониране и дългосрочното развитие на всяко стопанство. Тя осигурява условията за стабилно производство, рационално разпределение на ресурсите и поддържане на икономическата активност в условията на променяща се външна среда. Докладът има за цел да анализира влиянието на макроикономическата среда върху сигурността и отбраната, като се направи сравнителен анализ между България, Европейския съюз и глобалната икономика. С оглед на това е необходимо да се изясни същността на макроикономическата среда и нейната връзка с националната сигурност, да се анализира влиянието на икономическия растеж, инфлацията, публичните финанси и пазара на труда върху отбраната, да се изследва динамиката на военните разходи, да се анализира влиянието на икономическата нестабилност върху модернизацията и отбранителните способности.

Ключови думи: отбрана; сигурност; макроикономическа среда; икономически растеж; публични финанси

Въведение

Устойчивата икономическа база е фундаментална предпоставка за ефективното функциониране и дългосрочното развитие на всяко стопанство. Тя осигурява условията за стабилно производство, рационално разпределение на ресурсите и поддържане на икономическата активност в условията на променяща се външна среда. Наличието на стабилна икономическа основа допринася за повишаване на конкурентоспособността, финансовата стабилност и създаване на предпоставки за дългосрочен икономически растеж. В този смисъл тя е ключов фактор за осигуряване на балансирано развитие, което съчетава икономическа ефективност, социална отговорност и рационално използване на наличните ресурси.

Сигурността и отбраната са сред основните функции на съвременната държава, като тяхното ефективно осъществяване е невъзможно без наличието на икономически фундамент, който да осигурява изграждането и функционирането им. Способността на една държава да поддържа въоръжени сили, да инвестира в отбранителни технологии, да обезпечава необходимия човешки ресурс и да реагира при кризи зависи в значителна степен от състоянието на националната икономика.

Връзката между икономиката и отбраната е двустранна. От една страна, икономическият растеж създава финансовите възможности за поддържане и развитие на отбранителни способности. От друга страна, високите разходи за отбрана могат да окажат влияние върху публичните финанси, инвестициите и разпределението на ограничените обществени ресурси. Този проблем придобива особена актуалност в условията на нарастваща геополитическа нестабилност, войната в Украйна, повишените цени на енергията, инфлацията и технологичната конкуренция между водещите световни икономики.

През 2024 г. световните военни разходи достигат рекордните 2,718 трилиона щатски долара, което представлява реално увеличение от 9,4% спрямо 2023 г. и 37% спрямо 2015 г. Така те вече представляват 2,5% от световния брутен вътрешен продукт (БВП). Военните разходи в Европа са нараснали със 17% през 2024 г.[1] Тези процеси показват, че макроикономическата среда и сигурността са все по-тясно свързани. Държавите са изправени пред необходимостта едновременно да поддържат фискална устойчивост, икономически растеж и социална стабилност и да увеличават инвестициите си в отбраната.

Настоящият доклад има за цел да анализира влиянието на макроикономическата среда върху сигурността и отбраната, като направи сравнителен анализ между България, Европейския съюз и глобалната икономика.

В тази връзка е необходимо да се изясни същността на макроикономическата среда и нейната връзка с националната сигурност, да се анализира влиянието на икономическия растеж, инфлацията, публичните финанси и пазара на труда върху отбраната, да се изследва динамиката на военните разходи в България, Европа и света, да се анализира влиянието на икономическата нестабилност върху модернизацията и отбранителните способности, да се формулират изводи и препоръки за повишаване на икономическата и отбранителната устойчивост. Важно за настоящето изследване е да се подчертае, че устойчивата макроикономическа среда създава необходимите финансови, технологични и човешки предпоставки за изграждане на адекватни отбранителни способности, докато макроикономическата нестабилност ограничава възможностите за дългосрочно отбранително планиране и повишава уязвимостта на националната сигурност.

Макроикономическа среда, сигурност и отбрана

Макроикономическата среда представлява съвкупността от икономически условия и процеси, които определят функционирането на националната икономика. Основните ѝ характеристики се измерват посредством показатели като брутен вътрешен продукт, икономически растеж, инфлация, безработица, държавен бюджет, държавен дълг, лихвени проценти, инвестиции и външна търговия. Икономическият капацитет на държавата, състоянието на публичните финанси, наличието на човешки и технологичен капитал, както и устойчивостта на икономиката към външни и вътрешни сътресения са от изключителна важност за адекватното изграждане на сигурността и отбраната на всяка една страна. Ако една силна и стабилна икономика може да е фундамент при изграждането на националната сигурност, то в сила е и обратното твърдение – слабото стопанство е предпоставка за възникване на множество рискове. При невъзможност на икономиката да генерира растеж и стабилност следва ограничаване на средствата за отбрана, зависимост от външно финансиране, което е свързано с прокарване на чужди идеи и интереси, намаляване на инвестициите, загуба на квалифициран човешки капитал и др. Именно затова можем да твърдим, че икономическата устойчивост е в основата на изграждане на националната сигурност.

Макроикономическата среда в България, Европа и света

Глобалната икономическа среда през последните години се характеризира с висока динамика, мащабни промени и сериозни шокове. Тук може

да бъдат посочени пандемията от COVID-19, прекъсвания във веригите за доставки, енергийна криза, висока инфлация, повишаването на лихвените проценти и геополитическите конфликти. Според данни на Световната банка темпът на икономически растеж е слаб, като се очаква глобалният растеж да бъде около 2,7% през 2025 и 2026 г., което е значително под средния темп от 3,1% през десетилетието преди пандемията.[2] Данните на Международния валутен фонд (МВФ) са за малко по-високи нива като за 2024 г. те са 3,3%, 2025 г. са 3,2% и според прогнозата от октомври 2025, предвижданият растеж за 2026 г. е 3,1 %, което в никакъв случай не променя общата картина на нещата, като се има предвид, че и тази международна финансова институция подчертава повишената несигурност и рисковете, свързани с геополитическите конфликти и инфлацията.[3]

Макар данните на повечето финансови институции да са сходни, през 2026 г. динамиката се променя. Според данни на Организацията за икономическо сътрудничество и развитие (ОИСР – OECD) глобалният растеж през първата половина на 2026 г. се е забавил до приблизително 2,6% на годишна база, спрямо 3,6% през втората половина на 2025 г., като основните причини за това забавяне са енергийният шок, повишаването на цените на петрола и природния газ, по-високата инфлация, отслабването на реалните доходи, повишаването на дългосрочните лихвени проценти и геополитическата несигурност. Важен компенсиращ фактор се явява технологичният сектор и инвестициите, свързани с изкуствения интелект. Прави впечатление фактът, че OECD изрично посочва, че продължаващите инвестиции в изкуствен интелект (ИИ – AI) са подкрепили производството, търговията и икономическия растеж през 2026 г.[4] и макар с развитието и използването на AI да се подобряват някои стопански показатели, то това твърдение не се приема еднозначно. Различни са гледните точки относно това дали AI има толкова силен положителен ефект върху стопанството в световен мащаб или дори има редица отрицателни тенденции върху хората и стопанските показатели.[5]

Традиционно американската икономика се приема като един от основните двигатели на глобалната. Според данни на OECD растежът на САЩ се очаква да достигне 2,2% през 2026 г., след което да се забави до 2,1% през 2027 г. Основно значение за ръста на икономиката имат технологичният сектор и инвестициите в изкуствен интелект. От друга страна обаче, американската икономика е изправена пред няколко ограничения, сред които висока цена на финансирането, повишени тарифни бариери, натиск върху реалните доходи, по-слабо потребление и високи фискални дефи-

цити, като тези показатели са индикатори за развитие на кризисни фактори в икономиката на САЩ.[6] Съвременната щатска икономика се опитва да демонстрира иновативен устрем, но едновременно с това е притисната от сериозни структурни дисбаланси. Настоящата икономическа реалност показва, че САЩ се намират в период на забавяне, където технологичният напредък се бори с натрупаните макроикономически тежести. Двигател на растежа е развитието на изкуствения интелект и технологиите. Чрез тях се правят опити за преструктуриране на цели индустрии (от финанси до здравеопазване) и временно се компенсира по-слабото представяне на традиционните производствени сектори.

Ситуацията в Европа е сложна и специфична. От една страна, в ЕС има редица държави с големи икономики, развити финансови пазари и значителен технологичен потенциал. От друга страна, Европа е изправена пред проблеми като нисък потенциален растеж, застаряване на населението, енергийна зависимост и повишени разходи за сигурност. През 2024 г. дефицитът на сектор „Държавно управление“ за ЕС е 3,1% от БВП, а държавният дълг достига 80,7% от БВП. Тези стойности показват, че увеличаването на разходите за отбрана се извършва в условията на ограничено фискално пространство.[7] Показателни за всичко това са данните за държавния дълг на някои европейски държави, които могат да се видят в таблица 1.

Таблица 1. Държавен дълг по страни 2024 г. (% от БВП)

Държава	***Държавен дълг (% от БВП), 2024***
България	23,8%
Германия	62,5%
Франция	113,2%
Италия	134,9%
Испания	101,6%
Гърция	154,2%
ЕС	80,7%

Източник: Eurostat. European Commission

Таблицата показва съществената разлика във фискалната позиция на отделните държави. България е сред страните с най-ниско съотношение държавен дълг/БВП в ЕС, което създава сравнително по-голямо пространство за финансиране на стратегически разходи. Това не е достатъчно условие за увеличаване на публичните разходи, част от които са и разходите за сигурност и отбрана на страните. Макар да се наблюдават слабости в

европейската икономика, тя все пак генерира икономически растеж, макар и относително слаб. ОИСР прогнозира растеж на Еврозоната от 1,0% през 2026 г. и 1,0% през 2027 г. Сред факторите, които имат силно влияние и ограничават икономическата динамика в Европа, са висока зависимост от външни енергийни доставки, високи цени на природния газ, слаба промишлена активност, високи лихвени проценти, демографски ограничения, геополитическа близост до военни конфликти и необходимост от увеличаване на разходите за отбрана. Разходите за отбрана са специфична категория и тяхното увеличаване може да има двояко икономическо въздействие. В краткосрочен план то покачва съвкупното търсене и производството, но в дългосрочен възниква въпросът за алтернативната цена на публичните средства и натискът върху бюджетите, което много често събужда общественото недоволство. Гражданите невинаги приемат нарастването на разходите за отбрана, още повече когато необходимите средства са за сметка на някое от другите основни разходни направления на държавата.

Важно значение за състоянието на националната, а и на световната икономика имат инвестициите и преките чуждестранни инвестиции. През 2025 г. глобалните преки чуждестранни инвестиции (ПЧИ) се възстановяват количествено, но качеството и разпределението на това възстановяване са неравномерни.8 Според UNCTAD (Конференция на ООН за търговия и развитие) глобалните ПЧИ достигат около 1,6 трилиона щатски долара през 2025 г., което представлява увеличение с 6% според окончателния доклад за 2026 г. Необходимо е да се отбележи обаче, че инвестициите в развитите икономики нарастват с 11%, а в развиващите се икономики – само с 2%. Над 80% от глобалните ПЧИ са концентрирани в 20 водещи приемащи икономики и значителна част от новите инвестиции са насочени към AI и цифрова инфраструктура. Това означава, че световната инвестиционна система се характеризира с нарастваща концентрация на капитал, а не с равномерно разпределение на инвестиционните потоци. Факт е, че световната инвестиционна система не функционира на принципа на балансираното разпределяне на ресурсите. Вместо това тя се движи от концентрация на капитал, насочен предимно към развитите икономики и бързо развиващите се пазари с висок потенциал за възвръщаемост, стабилна инфраструктура и нисък риск. Последиците от това явление са т. нар. инвестиционни „магнити“, при които няколко държави и региони (като САЩ, Китай и Западна Европа) привличат огромната част от преките чуждестранни инвестиции (ПЧИ). Също така се разширява икономическата пропаст, по-бедните или нестабилни региони остават в периферията, тъй като

се възприемат като твърде рискови от големите институционални инвеститори. Глобалните потоци се контролират от ограничен брой финансови центрове и мултинационални компании, което засилва тяхното влияние върху световната сцена.

Други важни фактори, които са взаимосвързани и оказват цялостно влияние върху стопанството на национално, регионално и световно ниво са инфлацията и енергийната сигурност. През 2025 г. основната тенденция е към постепенно намаляване на инфлацията. През 2026 г. обаче геополитическият конфликт в Близкия изток предизвика значителни сътресения на енергийните пазари. Инфлацията и енергийната сигурност са сред най-влиятелните фактори, въздействащи върху световната икономика. Те са силно обвързани и функционират едновременно като икономически показатели, стратегически рискове и катализатори на кризи. Инфлацията е ключов макроикономически показател измерващ темпа, с който цените на стоките и услугите се повишават, което води до намаляване на покупателната способност на парите. Енергийната сигурност е стратегически и геополитически фактор. Тя представлява постоянната наличност на енергийни ресурси (нефт, газ, електроенергия, възобновяеми източници) на достъпна цена, без прекъсвания в доставките.

И двата фактора имат фундаментално значение, тъй като задвижват т.нар. „верижна реакция“ в глобален мащаб – енергията като двигател на всичко, всяко производство, транспорт и услуга в света зависят от енергия. Когато има заплаха за енергийната сигурност (например поради войни, санкции или политическо напрежение), цените на енергоносителите скачат рязко. Поскъпването на енергията директно увеличава разходите за производство и транспорт на всички останали стоки. Високата инфлация „изяжда“ доходите на хората и свива потреблението. Бизнесът от своя страна ограничава инвестициите си поради несигурност и високи разходи, централните банки повишават лихвените проценти. Това оскъпява кредитите, забавя икономическия растеж и понякога може да доведе до рецесия. Според прогнозите на ОИСР инфлацията в G20 през 2026 г. ще се повиши до 4,1%.[9] Това показва промяна от инфлационно успокояване към нов инфлационен натиск. Тези изменения имат мултиплициращ ефект, който се изразява в това, че по-високите енергийни цени водят до по-високи транспортни разходи, които повишават производствените разходи и така нарастват цените на храните и промишлените стоки. В резултат на това намалява реалния разполагаем доход, ограничава се потреблението и се забавя икономическия растеж.

Фискалната политика и разпределението на публичните средства са едно от най-сложните предизвикателства, поради факта че правителствата едновременно трябва да финансират социални системи, инфраструктура, отбрана, технологична трансформация, здравеопазване и др. Това създава конкуренция между публичните разходни приоритети. Икономическата политика все повече се превръща в инструмент на националната сигурност.

Влияние на основните макроикономически фактори върху отбраната

Промените в икономическия растеж и БВП оказват пряко въздействие върху финансовите възможности на държавата за поддържане и развитие на отбранителния сектор, тъй като именно БВП формира основата на фискалния потенциал и ресурсната обезпеченост на публичните разходи. Когато е налице устойчив икономически растеж, съществуват по-големи възможности за финансиране на отбраната, без да се поражда необходимост от прекомерно ограничаване на други жизненоважни обществени функции. Обратно, свиването на БВП и забавянето на растежа обикновено води до повишен натиск върху публичните финанси и необходимост от преразпределение на ограничени ресурси между конкуриращи се публични сфери. Важен момент при разглеждане на отбранителните разходи е, че те не трябва да се разглеждат единствено като бюджетно потребление, защото инвестициите в отбранителни способности стимулират развитието на технологичен потенциал, научноизследователска дейност, индустриални производства, човешки капитал и критична инфраструктура. Поради тази причина говорим за двустранна връзка между икономическата устойчивост и отбранителната способност – икономиката осигурява ресурсната основа на отбраната, а адекватно финансираната отбранителна система допринася за защитата на условията, при които икономическата дейност може да се развива устойчиво. Високите нива на икономическа активност увеличават способността на държавата да поддържа дългосрочна модернизация на въоръжените сили, включително чрез придобиване на съвременни технологии и изграждане на устойчиви отбранителни вериги за доставки. Добре изградената и функционираща система за национална сигурност от своя страна създава предпоставки за предвидимост, защита на собствеността, функциониране на инфраструктурата и устойчивост на стратегически сектори, които са фундаментални за стопанството. Това несъмнено се оценява положително и от чуждестранните инвеститори при търсене на нови възможности за инвестиране в дадена страна.

От казаното дотук можем да направим обобщение, че икономическият растеж и БВП представляват не само количествени показатели за състоянието на националното стопанство, а са също така ключови фактори за определяне на реалния капацитет на държавата да гарантира своята национална сигурност. Поради това е важно да се търси правилното съотношение между икономическия потенциал, бюджетните приоритети и отбранителните разходи, тъй като то е жизненоважно за устойчивото функциониране на стопанството и за поддържането на необходимите отбранителни способности.

Друг важен показател от държавните финанси, имащ пряка връзка и влияние върху отбраната, са държавният дълг и бюджетният дефицит. При високи нива на държавен дълг е налице сериозен натиск върху публичните финанси, а това от своя страна пряко застрашава и ограничава устойчивото финансиране на отбраната. Данните в таблица 1 показват именно заплахата, която съществува над Европа не само от развитие и ескалиране на дългова криза, но и заплаха за отбранителния сектор и изграждането на системата на сигурността на национално и на европейско ниво.

В контекста на отбранителните разходи инфлацията показва не само обезценяването на парите и намаляване на покупателната способност на населението, но и намаляването на реалната покупателна способност на отбранителните бюджети, което оскъпява поддръжката на въоръжението, доставките и заплатите в сектора на отбраната. При високи нива на инфлация държавите са притиснати и е необходимо да пренасочват средства от дългосрочни инвестиции за отбрана към текущи оперативни разходи.

Отбранителната политика е важно да бъде съобразена с необходимостта от поддържане на финансова стабилност, ограничаване на държавната задлъжнялост, приоритизиране на инвестиционните разходи и дългосрочно бюджетно планиране. На глобално равнище проблемът е още по-сериозен. По данни на МВФ глобалният публичен дълг през 2025 г. е достигнал почти 94% от световния БВП и се очаква да достигне 100% през 2029 г.[10] Това означава, че увеличаването на разходите за отбрана в световен мащаб ще се осъществява при все по-сериозни ограничения от страна на публичните финанси.

В контекста на изследване на макроикономическите показатели внимание заслужава и пазарът на труда. Според International Labour Organization (ILO) глобалната безработица през 2026 г. се очаква да остане около 4,9%. Това обаче прикрива значителни структурни проблеми. ILO изчислява глобалния jobs gap – броя хора, които желаят платена работа, но

не могат да я намерят, на около 408 млн. души през 2026 г. Следователно ниската официална безработица не трябва автоматично да се интерпретира като пълна устойчивост на пазара на труда.

Сред основните структурни проблеми може да посочим младежката безработица, нискокачествената заетост, технологичната автоматизация, демографското застаряване, недостиг на квалифицирана работна сила, както и несъответствие между уменията и потребностите на бизнеса. Ако разгледаме пазара на труда и безработицата от гледна точка на армията, става видно, че секторът на отбраната и сигурността е все по-зависим от висококвалифицирани специалисти от всички области на знанието. Колкото по-ниска е безработицата в една държава, толкова по-силно се конкурира армията с частния сектор за квалифицирани кадри. Според данните на Националния статистически институт (НСИ) за 2025 г. средното ниво на безработица в България е 3,5%. От гледна точка на държавната макроикономическа политика това е един много добър и стабилен показател, но в същото време се увеличава конкуренцията между въоръжените сили и частния сектор. Икономическият просперитет може да има двоен ефект върху отбраната, тъй като той увеличава бюджетните възможности, но едновременно с това повишава цената на човешкия ресурс.

Военните разходи в България, Европа и света

Военните разходи представляват значим показател за ресурсите, които държавите отделят за поддържане и развитие на отбранителните си способности. Данните на Stockholm International Peace Research Institute (SIPRI) показват трайна тенденция към увеличаване на световните военни разходи. За 2025 г. глобалните военни разходи достигат 2,887 трилиона щатски долара, което представлява реално увеличение от 2,9% спрямо 2024 г. и 41% ръст за периода 2016 – 2025 г. Разходите за отбрана възлизат на 2,5% от световния БВП.[11]

Данните за отбранителните разходи в Европа показват, че през 2025 г. общите военни разходи са достигнали приблизително 864 млрд. щатски долара, което е 14% увеличение спрямо предходната година. Делът им от регионалния БВП нараства от 2,8% през 2024 г. до 3,2% през 2025 г. Европейските държави от НАТО изразходват общо около 559 млрд. долара за отбрана през 2025 г.[12]

Тенденциите в България следват общата европейска картина към увеличаване на ресурсите за отбрана. Според данните на НАТО оценените

разходи на страната за 2025 г. са 1,933 млрд. щ.д. по постоянни цени и валутни курсове от 2021 г., което съответства на 2,06% от БВП. Спрямо 2014 г. реалното увеличение е около 112%. Тези данни се различават от националните бюджетни данни, тъй като НАТО използва собствена методология за определяне на разходите за отбрана.[13]

Като анализираме представените данни, можем да твърдим, че има значително нарастване на военните разходи в световен и в европейски мащаб. България също следва тенденциите и увеличава ресурса, отделян за отбрана, съобразно своите възможности. Тази динамика е свързана с променящата се европейска и международна среда за сигурност и с усилията на държавите от НАТО да увеличат отбранителните си способности.

Макар Европа да не води класацията по размер на разходи за отбрана, трябва да се подчертае фактът, че регионът е с едно от най-бързите увеличения на военните разходи. Този ръст е свързан основно с войната в Украйна, промяната в оценката на рисковете за европейската сигурност, необходимостта от попълване на запасите от боеприпаси, модернизацията на въоръжените сили, увеличаването на инвестициите в противовъздушна и противоракетна отбрана, както и развитието на безпилотни и кибернетични способности.

Съпоставянето на България, ЕС и света показва няколко важни тенденции. България има сравнително нисък държавен дълг, умерен икономически растеж, ниска безработица, постепенно увеличаване на разходите за отбрана, значителна зависимост от международни доставчици на модерно военно оборудване. Фискалната позиция е силна в сравнение с много европейски държави. Държавният дълг от 23,8% от БВП през 2024 г. е сред най-ниските в ЕС. Европейският съюз пък разполага със значително по-голям икономически и технологичен потенциал, но е изправен пред по-висока задлъжнялост, демографски проблеми, зависимост от определени стратегически технологии и суровини, необходимост от координация между националните отбранителни системи. В световен мащаб тенденцията показва ясно увеличаване на разходите за сигурност и отбрана. Това е показателно за факта, че сигурността постепенно заема по-голямо място в икономическите политики на държавите.

Заключение

Макроикономическата среда оказва съществено влияние върху сигурността и отбраната, тъй като определя финансовите възможности на държавата за поддържане и развитие на необходимия отбранителен капацитет. Икономическият растеж, инфлацията, бюджетните ограничения и

равнището на публичния дълг пряко се отразяват върху способността за финансиране на отбранителни политики и инвестиции. В условията на икономическа нестабилност необходимостта от ефективно разпределение на ресурсите и дългосрочно стратегическо планиране придобива особено значение. Поради това устойчивостта на националната икономика следва да се разглежда като важен фактор за гарантиране на националната сигурност и за изграждане на адекватни отбранителни способности.

Благодарности. Публикацията е разработена в рамките на Националната научна програма „Сигурност и отбрана“, финансирана от Министерството на образованието и науката на Република България в изпълнение на Националната стратегия за развитие на научните изследвания 2017 – 2030 г., приета с Решение на Съвета с Министерско постановление № 731 от 21 октомври 2021 г.

БЕЛЕЖКИ

1. SIPRI, 2025. *Unprecedented rise in global military expenditure as European and Middle East spending surges*. 28 April 2025. Available from: https://www.sipri.org/media/press-release/2025/unprecedented-rise-global-military-expenditure-european-and-middle-east-spending-surges.

2. World Bank, Global Economic Prospects, January 2025: Executive Summary (English). Available from: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099321003242538637.

3. IMF, Global Economy in Flux, Prospects Remain Dim, October 2025. Available from: https://www.imf.org/en/publications/weo/issues/2025/10/14/world-economic-outlook-october-2025.

4. Global growth holds up despite successive shocks, but risks persist. 23 September 2026. Available from: https://www.oecd.org/en/about/news/press-releases/2026/09/global-growth-holds-up-despite-successive-shocks-but-risks-persist.html.

5. Diteramb Consult , 2026. *Феноменът „ИИ Бумеранг“: Защо корпоративните гиганти тихичко връщат съкратените си служители“.* Available from: https://www.diterambconsult.com/blog/article/ii-bumerang-sakrashtenia-korporacii-analiz.

6. IMF, IMF Executive Board Concludes 2026 Article IV Consultation with the United States. 2 April 2026. Available from: https://www.imf.org/en/news/articles/2026/04/01/pr-26102-usa-imf-executive-board-concludes-2026-article-iv-consult.

7. United Nations Publications, 2026. *World Investment Report*. Available from: https://unctad.org/system/files/official-document/wir2026_en.pdf.

8. ВУЛОВ, Г., 2026. *ОИСР повиши прогнозата си за растеж на глобалния БВП за 2026 г. на 2,9% и я понижи за 2027 г. на 3*. Available from: https://3e-news.net/bg/a/view/72701/oisr-povishi-prognozata-si-za-rastej-na-globalnija-bvp-za-2026-g-na-2-9-i-ja-poniji-za-2027-g-na-3.

9. IMF, FISCAL MONITOR, 2026. Fiscal Policy under Pressure: High Debt, Rising Risksq. ISBN: 979-8-22904-253-6 (PDF). Available from: https://www.imf.org/-/media/files/publications/fiscal-monitor/2026/april/english/text.pdf.

10. SIPRI, 2025. *Trends in World Military Expenditure*. Available from: https://www.sipri.org/publications/2026/sipri-fact-sheets/trends-world-military-expenditure-2025.

11. EDA. *EDA Defence Data 2024 – 2025*. Available from: https://eda.europa.eu/publications-and-data/thematic-policy-reports/eda-defence-data-2024-2025.

12. NATO, 2025. Defence Expenditure of NATO Countries (2014 – 2025). Available from: https://www.nato.int/en/news-and-events/articles/news/2025/08/28/defence-expenditure-of-nato-countries-2014-2025

13. ELVEREN, A. Y., 2025. *Heterodox economics of military spending*. New York, ISBN: 978-1-032-87136-3. Available from: https://books.google.bg/books?id=sHiNEQAAQBAJ&pg=PT7&hl=ru&source=gbs_selected_pages&cad=1#v=onepage&q&f=false

IMPACT OF THE MACROECONOMIC ENVIRONMENT ON SECURITY AND DEFENCE

Abstract. A sustainable economic base is a fundamental prerequisite for the effective functioning and long-term development of any economic system. It provides the conditions for stable production, the rational allocation of resources, and the maintenance of economic activity at a changing external environment. The report aims to analyze the impact of the macroeconomic environment on security and defence by conducting a comparative analysis involving Bulgaria, the European Union, and the global economy. In this context, it is necessary to clarify the nature of the macroeconomic environment and its relationship with national security; to analyze the impact of economic growth, inflation, public finances, and the labor market on defence; to examine the dynamics of military expenditure; and to analyze the impact of economic instability on modernization and defence capabilities.

Keywords: defence; security; macroeconomic environment; economic growth; public finances.

Dr. Katya Peycheva, Assoc. Prof.
ORCID iD: 0000-0001-7149-0375
Security and Defense Management Department
National Security and Defense Faculty
Rakovski National Defense College
Sofia, Bulgaria
E-mail: k.peicheva@rndc.bg

https://doi.org/10. 66334/annu26_opminebsea

ОПЕРАТИВНА СРЕДА И ПРОТИВОМИНЕН КАПАЦИТЕТ В ЧЕРНО МОРЕ: РЕГИОНАЛНИ КАЗУСИ, ДЕФИЦИТИ И ДОКТРИНАЛНИ РЕАЛНОСТИ

капитан II ранг д-р Красимир Ангелов
ВВМУ „Н. Й. Вапцаров“

Абстракт. В доклада се изследва оперативната среда и противоминният капацитет на черноморските държави в условията на продължаващата война между Руската федерация и Украйна. Анализират се конкретни регионални казуси, които разкриват критични дефицити и уязвимости на противоминните кораби спрямо съвременните асиметрични заплахи. Резултатите от изследването показват значителен дисбаланс в способностите на разглежданите държави. Докато Украйна и Грузия изпитват остра липса на ефективни платформи в Черно море, а Русия търпи ограничения и загуби, държавите от НАТО (Турция, Румъния и България) компенсират вакуума в сигурността чрез съвместната инициатива MCM Black Sea. Основният извод е, че на регионално ниво липсва единна концептуална визия за преход към иновативни противоминни системи от ново поколение, като повечето флотове продължават да разчитат на остаряваща доктринална рамка.

Ключови думи: минна заплаха; противоминни способности; противоминни кораби; морска сигурност1

I. Въведение

Ситуацията в Черноморския регион през последните години показва динамика на процесите на политическо и военно равнище. Водещ фактор за нестабилността в региона е продължаващата вече повече от пет години пълномащабна война между Руската федерация и Украйна. В значителна степен морската транспортна система в Черно море е повлияна и от минната заплаха, която има своите реални измерения. За изясняване на сложността в региона на Черно море се използват емпирични изследвания, включващи детайлен анализ на информационни източници и историческа ретроспекция. Методите за теоретични изследвания се базират на научен анализ, сравнение и логическо обобщение.

II. Изложение

Румънските противоминни способности в момента на провеждане на изследването са съизмерими с тези на българските Военноморски сили. Според официалните източници те са съвкупност от три морски миночистача проект „Муска“ и два минни ловеца клас „Сандаун“.[1] Наблюдава процес на преход от стара към съвременна противоминна доктрина, т.е. тенденция към извеждане на остарелите противоминни способности за сметка на технологично обновление.[2]

Показателен е инцидентът с румънския миночистач Lt. Dimitrie Nicolescu от септември 2022 г., който катализира процеса по модернизация на противоминните сили на Румъния. Той илюстрира неактуалността на стария противоминен модел, използващ Stand-In концепцията. Миночистачът е назначен за неутрализиране на дрейфуваща мина североизточно от пристанище Констанца. Вследствие на неблагоприятните хидрометеорологични условия в района на операцията екипажът няма възможност за спускане на корабната подривна команда с лодка. Операцията се осъществява през тъмната част на денонощието при силен вятър. Корабът се натъква на мината с кърмовата си част[3].Този случай доказва критичната уязвимост на противоминните кораби от по-старо поколение, неразполагащи с дистанционно управляеми апарати. Ако румънските Военноморски сили (ВМС) имаха безпилотен катер или подводен апарат за неутрализиране на мини, корабът и личният състав биха могли да останат на безопасно разстояние, а неблагоприятните външни условия нямаше да възпрепятстват изпълнението на задачата. Независимо че до момента липсва информация от извършената проверка, може да се направи обосновано предположение,

че вследствие на този процес ВМС на Румъния придобиват от Великобритания два по-приспособени на неблагоприятната среда минни ловци клас Sandown.

Въоръженият конфликт с Украйна значително промени оперативната среда за ***Черноморския флот на Руската федерация***, в това число и за неговите противоминни кораби. Първоначалните стратегически планове на руското ръководство имаха за цел да установят морски контрол в северозападната част на Черно море, за да се улесни последващата десантна операция (Popa & Learschi 2025, p. 10). Съгласно тази оперативна концепция руските противоминни сили бяха натоварени със задачата да осигурят противоминна защита на бойните и десантните кораби. Украинските безпилотни катери се доказаха като евтин, но мощен актив за атака срещу руски кораби. Освен това използването на противокорабни крилати ракети допълнително увеличи риска за руските сили на море.

Въпреки активните дезинформационни кампании от руска и украинска страна, може да се направи извод, че силите на Черноморския флот са понесли сериозни загуби. Редица западни анализатори допускат, че тези загуби достигат 20% до 2023 г.[4] Освен безпилотни надводни апарати и противокорабни крилати ракети, украинските въоръжени сили използват безпилотни летателни апарати и противотанкови ракети. За поразяване на големи надводни цели, разположени във военноморски бази или корабостроителници, се използват балистични ракети с малък обсег на действие.[5,6]

Съобщенията за успешни атаки на украинските въоръжени сили срещу противоминни кораби на Черноморския флот остават противоречиви и непотвърдени. Досега въз основа на информация от открити източници може да се предположи, че украинската страна е организирала успешна атака с надводни и въздушни дронове срещу морския миночистач „Иван Голубец“ във военноморската база Севастопол на 22 октомври 2022 г., довела до шестмесечен ремонт за възстановяване на боеспособността му.[7,8] Съществува и доклад, непотвърден от руски или независими източници, относно унищожаването на друг морски миночистач проект 266М „Ковровец“ на 19 май 2024 г. Твърди се, че корабът е бил ударен от тактическа балистична ракета ATACMS.[9,10] Многобройните успешни атаки срещу кораби на Черноморския флот принудиха руското ръководство да предприеме нетрадиционни за голяма морска сила мерки – а именно да пребазира значителна част от корабния състав от Севастопол в Новоросийск, за да намали риска от допълнителни загуби.

Оценката на настоящите способности на противоминните сили на Руската федерация в Черно море е сложна и противоречива. От една страна, Русия използва четири модерни кораба – три от клас „Александрит“ и един от проект 02668, които осигуряват значителни възможности както срещу контактни, така и срещу неконтактни мини. Тези платформи значително намаляват риска за кораба и екипажа, но в сравнение с принципите на съвременната противоминна Stand-Off концепция[11], те са морално остарели още с въвеждането си в експлоатация. Останалите противоминни кораби функционират на значително по-ниско технологично ниво. Те разчитат на традиционните контактни и неконтактни тралове срещу морските мини.

Поради заплахата от украински атаки руските военни кораби действат в по-ограничени райони, което затруднява осигуряването на защитата на противоминните кораби срещу различните видове заплахи при плаване. Освен това асиметричните предизвикателства, по-специално използването на безпилотни надводни и летателни апарати, създават сериозни нови заплахи, на които традиционните противоминни кораби не са проектирани да противодействат (Bozov 2022, p. 116).

Текущото състояние на способностите на противоминните кораби от руския Черноморски флот е противоречиво. Въпреки че модернизацията е в ход, замяната на остарелите платформи с модерни кораби, оборудвани с усъвършенствани системи за противоминна борба, е несигурна. Наблюдават се значителни изменения в планираната трансформация поради различни фактори. Войната в Украйна разкри сериозни уязвимости в руския флот пред асиметричните заплахи, което ограничи значително оперативните им възможности. Ефективността на противоминните действия от руска страна в Черно море остава под въпрос, тъй като противоминните сили са принудени да се адаптират към нова и все по-неблагоприятна среда.

Противоминните способности на Украйна след разпадането на Съветския съюз са незадоволителни, до голяма степен те не се различават от общото състояние на корабния състав, който украинските военноморски сили придобиват при серията от споразумения между Украйна и Русия в периода 1992 – 1997 г. за разпределяне на военните кораби между двете държави в Черно море. Получените плавателни средства са стари и в незадоволително техническо състояние и то на фона на общото тежко макроикономическо състояние на страната. Това възпрепятства възможността за поддържането и придобиването на нова техника. След анексирането на Крим от Москва Украйна губи своите миночистачи, както е посочено в Таблица 1[12]. Съдбата на единствения рейдови миночистач е противоречива,

като от руска страна се твърди, че е унищожен, докато според Украйна той е част от новосформирания противоминен дивизион, към който формално принадлежат и дарените от западните партньори минни ловци. Корабите от Великобритания, Белгия и Нидерландия не са във военноморските бази на страната поради прилаганата от Турция Конвенция от Монтрьо. Текущият противоминен състав на Украйна включва два кораба клас „Сандаун“, дарени от Великобритания, и три кораба клас „Трипарти/Алкмаар“, два от които дарени от Нидерландия и един от Белгия.

Таблица 1. Противоминни кораби във ВМС на Украйна (1997 – 2014 г.)

Проект, вид	***Бордови номер***	***Име***	***Въведен в експлоатация***	***Забележка***
ммч пр. 266М	U310	„Чернигив“	10.09.1974 г.	Под контрола на РФ от 24.03.2014 г.
	U311	„Черкаси“	10.06.1977 г.	Под контрола на РФ от 25.03.2014 г.
бмч пр. 1265	U330	„Мелитополь“	30.09.1979 г.	Снет от въоръжение на 30.05.2013 г.
	U331	„Мариуполь“	29.12.1978 г.	Снет от въоръжение на 07.11.2012 г.
рмч пр. 1258	U360	„Геническьк“	10.07.1985 г.	В строя

В началото на Руско-Украинската война през 2022 г. с цел защита на десантно достъпните места от своята брегова линия Украйна изгражда минно-артилерийски позиции около пристанище Одеса. Допуска се, че поради скъсани минрепи вследствие на неблагоприятни хидрометеорологични условия в района на минните постановки стотици мини от типа „ЯМ“ и „КРМ“ стават дрейфуващи мини и съответно заплаха за свободното корабоплаване в западната част на Черно море. Към момента Украйна не притежава противоминни способности, тъй като Турция се позовава на Конвенцията от Монтрьо и не допуска през проливната зона (Дарданели и Босфор) придобитите от Великобритания, Нидерландия и Белгия минни ловци. Получава се парадокс – от една страна, благодарение на асиметричните бойни действия на украинските въоръжени сили срещу Черноморския флот на Руската федерация, руският корабен състав е изтеглен на изток във военноморска база Новоросийск, от друга страна, Украйна не

притежава способности за прочистване на своята акватория, което възпрепятства нормалното функциониране на морската транспортна система в западната и централната част на Черно море.

Бойният потенциал на корабния състав на грузинските въоръжени сили след Руско-Грузинската петдневна война от 2008 г. де факто е сведен до нула. След войната запазените активи преминават като елемент от Бреговата охрана (към Министерството на вътрешните работи).[13] В настоящия момент Грузия не разполага с плавателни средства, които да осигуряват противоминната отбрана на страната. Малките патрулни катери, придобити чрез дарение от САЩ и Турция, не разполагат с въоръжение, способно да противодейства на минната заплаха.[14] Евентуалните минозаградни действия от страна на противника в основните пристанища на страната (Поти и Батуми) ще парализират морската транспортна система и за извеждането от това неблагоприятно състояние ще е необходима помощ от партньорски държави.

Развитието на ***противоминния корабен състав на Турция*** е в пряка зависимост от общото състояние на Военноморските сили на страната и положителната тенденция за придобиване и поддържане на актуални системи за отбрана. В количествено и качествено отношение Турция притежава балансиран конвенционален противоминен флот в разглеждания регион. Основните противоминни кораби на турските военноморски сили са от клас Aydin[15], общо шест на брой, приети на въоръжение в периода 2005 – 2009 г. Те са сравнително модерни платформи срещу съвременните минни заплахи, но не трябва да се пренебрегва фактът, че са минни ловци, принадлежащи към по-старата концепция Stand-In, при която рискът за кораба и личния състав съществува. Към противоминния състав на Турция все още принадлежат и три значително по-стари платформи (първо поколение минни ловци) от клас Engin[16]. Те са френски кораби, произведени в началото на седемдесетте години на миналия век и приети в турските ВМС през 1998 – 1999 г. Стратегическото разположение на Турция и контролирането на Проливната зона (Босфора, Мраморно море, Дарданелите) осигуряват възможност за лесно пребазиране на корабите от военноморска база „Ердек“ в акваторията на Черно море за осъществяване на национални противоминни операции или операции в съюзен формат.

След нахлуването на Руската федерация в Украйна през 2022 г. Турция затвори проливната зона за военни кораби на воюващите и нелиторалните държави. Решението бе взето въз основа на Конвенцията от Монтрьо от 1936 г. и с цел избягване на ескалация на напрежението в Черно море. Невъзможността за присъствие на нечерноморски държави доведе до фак-

тически вакуум в областта на морската сигурност в региона. В отговор на това по инициатива на Турция през 2024 г. беше подписан Меморандум за разбирателство между България, Румъния и Турция, с който се създава Противоминната военноморска група в Черно море (MCM Black Sea)[17]. Групата действа чрез планирани активации, определени от съвместен комитет. Основната ѝ тактическа задача е да гарантира безопасността на морските пътища в отговор на заплахата от дрейфуващи мини, възникнала непосредствено след руската агресия срещу Украйна. Този оперативен фокус директно стабилизира морските коридори в западната част на Черно море.

III. Заключение

Проведеният анализ, свързан с противоминния капацитет на държавите от Черноморския регион, потвърждава тезата, че на регионално ниво съществува значителен дисбаланс в тяхното развитие в противоминно отношение. Поради политически и финансови причини липсва единно разбиране за необходимостта от изследване на възможността за придобиване на съвременно въоръжение, отговарящо на най-актуалните концептуални решения, свързани с модулно противоминно оборудване и противоминни кораби-майки, осигуряващи много високо ниво на безопасност за екипажите и въоръжението. Дори Република Турция, която успешно изпълнява ролята на регионален лидер в сферата на отбраната, акцентира в по-висока степен върху превъоръжаването и подновяването основно на бойния си корабен състав.

БЕЛЕЖКИ

1. FORȚELE NAVALE ROMÂNE, 2026. *Navele Divizionului 146 Nave Minare-Deminare* [online]. Constanța: Statul Major al Forțelor Navale. Available from: https://www.navy.ro/despre/organizare/divizion_146/nave_div146.php. [viewed: 07.07.2026].

2. FORȚELE NAVALE ROMÂNE, 2026. *Istoricul Divizionului 146 Nave Minare-Deminare* [online]. Constanța: Statul Major al Forțelor Navale. Available from: https://www.navy.ro/despre/organizare/divizion_146/istoric.php. [viewed: 07.07.2026].

3. FORȚELE NAVALE ROMÂNE, 2022. *Dragorul maritim 29 a suferit avarii ușoare în urma exploziei unei mine marine* [online]. Constanța: Statul Major al Forțelor Navale, 8 September 2022. Available from: https://www.navy.ro/comunicat.php?id=641. [viewed: 07.07.2026].

4. COOK, E., 2023. Fifth of Russia's Black Sea Fleet ‚Destroyed' in 4 Months: UK. *Newsweek* [online]. 26 December 2023. Available from: https://www.newsweek.com/russia-black-sea-fleet-crimea-ukraine-landing-ship-1855450. [viewed: 07.07.2026].

5. COLEMAN, J., 2022. Video Shows 2 Russian Warships Escaping as Ukrainian Missiles Blast a Docked Ship. *Business Insider* [online]. 24 March 2022. Available

from: https://www.businessinsider.com/video-2-russian-warships-escape-as-ukrainian-missiles-blast-a-docked-ship-2022-3. [viewed: 07.07.2026].

6. NEWDICK, T., 2022. Ukraine Claims TB2 Drones Sunk Russian Patrol Boats Off Snake Island. *The War Zone* [online]. 2 May 2022. Available from: https://www.twz.com/ukraine-claims-tb2-drones-sunk-russian-patrol-boats-off-snake-island. [viewed: 07.07.2026].

7. BICKERTON, J., 2022. Russia Says Minesweeper Hit in 'Massive' Attack on Black Sea Fleet. *Newsweek* [online]. 29 October 2022. Available from: https://www.newsweek.com/explosions-reported-near-crimean-city-russia-drones-shot-down-sevastopol-1755579. [viewed: 07.07.2026].

8. BARKHUSH, A., 2024. Black Sea Fleet Vessels Russia Has Lost since the Beginning of the Full-Scale Invasion. *United24 Media* [online]. 29 July 2024. Available from: https://united24media.com/latest-news/all-the-black-sea-fleet-vessels-russia-has-lost-since-the-beginning-of-the-full-scale-invasion-1445. [viewed: 07.07.2026].

9. HIGHAM, A., 2024. Ukraine Destroys Russian Black Sea 'Kovrovets' Minesweeper. *Newsweek* [online]. 19 May 2024. Available from: https://www.newsweek.com/ukraine-destroys-black-sea-kovrovets-minesweeper-1902259. [viewed: 07.07.2026].

10. POVILAS, M., 2024. Another Win for ATACMS: Ukraine Destroyed a Large Russian Marine Minesweeper. *Technology.org* [online]. 28 May 2024. Available from: https://www.technology.org/2024/05/28/another-win-for-atacms-ukraine-destroyed-a-large-russian-marine-minesweeper/. [viewed: 07.07.2026].

11. EXAIL, 2025. *First Mooring of the Oostende in Zeebrugge, the First Mine Countermeasures Vessel in the Belgian-Dutch rMCM Programme* [online]. 4 November 2025. Available from: https://www.exail.com/news/first-mooring-of-the-oostende-in-zeebrugge-the-first-mine-countermeasures-vessel-in-the-belgian-dutch-rmcm-programme. [viewed: 07.07.2026].

12. IISS, 2013. *The Military Balance 2013: The Annual Assessment of Global Military Capabilities and Defence Economics*. London: Routledge. ISBN 978-1-85743-680-8.

13. MINISTRY OF INTERNAL AFFAIRS OF GEORGIA, 2026. *Coast Guard* [online]. Tbilisi: MIA Border Police of Georgia. Available from: https://bpg.gov.ge/en/page/border-police/coast-guards. [viewed: 12.09.2026].

14. IISS, 2024. The Military Balance 2024: The Annual Assessment of Global Military Capabilities and Defence Economics. London: Routledge. ISBN 978-1-03278-004-7.

15. TURKISH NAVAL FORCES, 2026. *Aydın-Class Mine Countermeasures Vessels* [online]. Ankara: Deniz Kuvvetleri Komutanlığı. Availablefrom: https://www.dzkk.tsk.tr/en-US/Destek/Content/aydin-class. [viewed: 12.07.2026].

16. TURKISH NAVAL FORCES, 2026. *Engin-Class Mine Countermeasures Vessels* [online]. Ankara: Deniz Kuvvetleri Komutanlığı. Available from: https://www.dzkk.tsk.tr/en-US/Destek/Content/engin-class. [viewed: 12.07.2026].

17. МИНИСТЕРСТВО НА ОТБРАНАТА НА РЕПУБЛИКА БЪЛГАРИЯ, 2024. *България, Турция и Румъния подписаха Меморандум за създаване на Про-*

тивоминна военноморска група в Черно море (MCM Black Sea) [онлайн]. София: Министерство на отбраната, 11 януари 2024 [прегледан на 12.07.2026]. Достъпно на: https://mod.bg/news8303.

REFERENCES

BOZOV, Z., 2022. Comparative Analysis of the Remotely Piloted Aircraft Systems Used in the Russia-Ukraine War. In: *International Scientific Conference - Defense Technologies DefTech 2022*, pp. 114-119. Shumen: Faculty of Artillery, Air Defense and Communication and Information Systems. ISSN 2367-7902

POPA, A. & LEARSCHI, S., 2025. *The Strategic Collapse of the Russian Navy in the Context of the War in Ukraine (2022–2025)*. Constanța: Maritime Security Forum.

OPERATIONAL ENVIRONMENT AND MINE COUNTERMEASURES CAPACITY IN THE BLACK SEA: REGIONAL CASE STUDIES, DEFICITS AND DOCTRINAL REALITIES

Abstract. The report examines the operational environment and the mine countermeasures (MCM) capacity of the Black Sea states amidst the ongoing war between the Russian Federation and Ukraine. Specific regional case studies are analyzed, revealing critical deficits and vulnerabilities of MCMVs against modern asymmetric threats. The research findings indicate a significant imbalance in the capabilities of the observed nations. While Ukraine and Georgia experience an acute shortage of effective platforms in the Black Sea, and Russia faces operational limitations and losses, the NATO members (Turkey, Romania, and Bulgaria) are compensating for the security vacuum through the joint MCM Black Sea initiative. The primary conclusion is that, at the regional level, there is a lack of a unified conceptual vision for transitioning to innovative, next-generation MCM systems, as most fleets continue to rely on an aging doctrinal framework.

Keywords: mine threat; mine countermeasures capabilities; mine countermeasures vessels (MCMVs); maritime security.

Commander Dr. Krasimir Angelov
WoS Researcher ID: ABK-9726-2022
ORCID iD: 0000-0003-0773-6611
Naval Tactics Department
Faculty of Navigation
Nikola Vaptsarov Naval Academy
73, Vasil Drumev St.
9002 Varna, Bulgaria
E-mail: angelov@nvna.eu

https://doi.org/10. 66334/annu26_systsystem

МРЕЖОВО-ЦЕНТРИЧЕН МОДЕЛ НА СИСТЕМА ОТ СИСТЕМИ В ПРОТИВОМИННАТА БОРБА

капитан II ранг д-р Красимир Ангелов
ВВМУ „Н. Й. Вапцаров“

Абстракт. В доклада се изследва трансформацията на противоминната борба чрез прилагането на системно-инженерната концепция за мрежово-центрична „система от системи“. Обосновава се необходимостта от преход от традиционни платформи, действащи в рискови зони, към иновативна архитектура, която обединява оперативно кораб носител и хетерогенни безпилотни платформи. Чрез адаптиране на системните критерии на Бордман, Сосър и Город се извежда профил на равновесие на противоминния комплекс и се определят критичните коефициенти на оперативна ефективност. Вградена е трислойна мрежово-центрична структура (сензорен, информационен и команден слой), осигуряваща мултидомейно сливане на данни. Резултатите доказват, че в тази мрежово-центрична рамка корабът носител се трансформира в тактически интеграционен възел, действащ на безопасно разстояние, а синергията между безпилотните модули съкращава цикъла за вземане на решение.

Ключови думи: мрежово-центрична система; противоминна „система от системи“; противоминна борба; безпилотни комплекси

I. Въведение

Концептуалната рамка на мрежово-центричните действия, инициирана от Артър Цебровски и Джон Гарстка (Cebrowski & Garstka 1998), предопределя развитието на съвременните военноморски операции. В теорията на Албъртс и др. (Alberts et al. 1999, pp. 10 – 14) бойното пространство се декомпозира на три взаимосвързани области: физическа (платформи, сензори и оръжия), информационна (преносни среди, C4ISR мрежи и потоци от данни) и когнитивна (ситуационна осведоменост, приемане на решения и команден замисъл).

Приложението на тази хипотеза в противоминната борба изисква преформатиране на традиционния доктринален подход. Минната заплаха в съвременните морски конфликти се характеризира с висока асиметричност, наличие на класически контактни и интелигентни неконтактни мини. Традиционната концепция *Stand-In MCM*, разчитаща на физическо навлизане на единичен кораб (миночистач или минен ловец) в миноопасния район, генерира високо ниво на риск за личния състав и кораба.

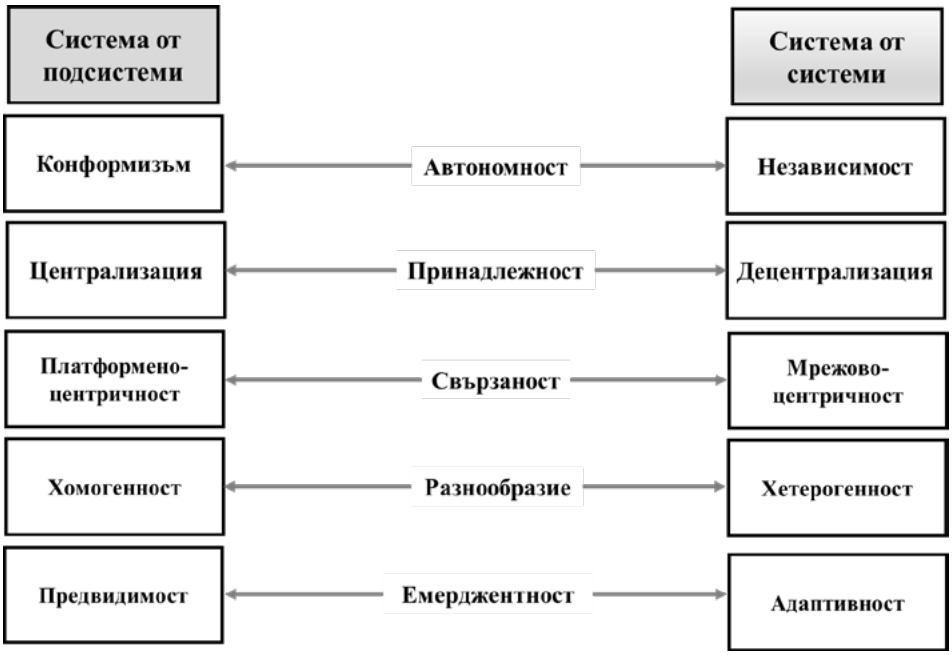
Трансформацията към мрежово-центрична противоминна борба надхвърля обикновената свързаност между плавателните съдове. Тя се базира на системно-инженерната концепция за „система от системи“ (CoC), при която корабът носител и хетерогенни безпилотни платформи – безпилотни надводни катери, безпилотни летателни апарати, автономни подводни апарати и дистанционно управляеми подводни апарати – се обединяват в единен оперативно-технически контур. В тази архитектура всяка отделна безпилотна система запазва своята оперативна и управленска автономност, но в комбинация с останалите генерира качествено ново, синергично преимущество, което нито един от компонентите не притежава самостоятелно (Stoyanov 2017, p. 25).

II. Изложение

2.1. Приложение и адаптиране на системните критерии на Бордман, Сосър и Город за противоминни роботизирани комплекси

Според класификацията на Бордман, Сосър и Город (Sauser et al. 2009, pp. 200 – 204) една структура се квалифицира като „система от системи“, когато притежава пет фундаментални характеристики: автономност, принадлежност, свързаност, разнообразие и емерджентност. За разграничаване на CoC от класическата сложна система авторите дефинират противо-

поставящи се силови двойки (парадокси), флуктуиращи между системните полюси.



Фигура 1. Системни характеристики и техните парадокси (адаптирано по Sauser et al. 2009)

Определянето и аналитичното извеждане на точките на равновесие (T_{eq}) между тези системни парадокси се базира на математически модел за оценка на оперативната ефективност (K_{eff}) на противоминния комплекс.

2.1.1. Аналитична рамка за оперативна ефективност

Формулирането на интегралния оперативен капацитет на противоминната „система от системи“ (E_{SoS}) се базира върху принципите на Теорията на търсенето във военноморските изследвания на операциите (Koopman 1980, pp. 53 – 78). В настоящия модел (E_{SoS}) се дефинира като функция от интегралната вероятност за пълно прочистване (P_{MCM}), производителността на обследване (V_{clear}) и защитеността на силите (S_{force}):

$$E_{SoS} = P_{MCM} \cdot \mathrm{V}_{\mathrm{clear}} \cdot \mathrm{S}_{\mathrm{force}} \qquad (1)$$

където:

$P_{MCM} = P_{det} . P_{id} . P_{neutr}$ (съответни вероятности за откриване, идентификация и неутрализиране на мината);

$S_{force} = 1 - R_{crew}$, където $R_{crew} \in [0, 1]$ е индексът на риск за личния състав. При преход от *Stand-In* към *Stand-off MCM* $R_{crew} \rightarrow 0$, следователно $S_{force} \rightarrow 1$.

За целите на модела, трите фактора за оценка на минния риск, заложени в Доктрината за противоминни операции на САЩ[1], са математически формализирани в следния индекс на минната заплаха (E_{Threat}):

$$E_{Threat} = \rho_{mine} . S_{target} . \eta_{env} \quad (2)$$

където ρ_{mine} е плътността на минното поле, S_{target} е чувствителността на минните взриватели, а η_{env} е коефициентът на хидроакустична неопределеност на средата.

Условието за достигане на точка на оперативно равновесие (T_{eq}) се дефинира като състоянието, при което коефициентът на ефективност $K_{eff} = 1$:

$$K_{eff} = \frac{E_{SoS}(t, D_{stand-off}) E_{SoS}(t, D_{stand-off})}{E_{Threat} \quad E_{Threat}} = 1 \Leftrightarrow \Leftrightarrow E_{SoS}(t, D_{stand-off}) - E_{Threat} = 0 \quad (3)$$

където t е оперативното време за обследване и неутрализиране, а $D_{stand-off}$ е безопасната дистанция на кораба носител до миноопасната зона.

2.1.2. Количествено определяне на точките на равновесие (T_{eq})

Постигането и поддържането на дефинираното аналитично условие за оперативно равновесие (K_{eff}) изисква локализиране на точките на равновесие (T_{eq}) по всяка от петте характеристики на CoC. Тези точки определят оптималния баланс между системните парадокси, позволяващ нарастване на E_{SoS} при минимален риск.

2.1.2.1. Автономност (A): Конформизъм – Независимост

Автономността флуктуира между спазването на стандартните оперативни процедури и независимите алгоритми на апаратите. Точката на равновесие A се определя от функцията на контрол $C_{human} \in [0, 1]$:

$$T_{eq}(A) = w_1 \cdot (1 - C_{human}) + w_2 \cdot A_{software} \quad (4)$$

Тъй като неутрализацията на бойни експлозиви изисква задължителен човешки контрол, $C_{human} \approx\approx 0{,}8$, което премества точката *A* умерено вляво към Конформизма ($T_{eq}(A) = 0{,}35$).

2.1.2.2 Принадлежност (P): Централизация – Децентрализация

Централизацията се изразява в ролята на кораба носител като възел за командване и управление, а децентрализацията – във възможността безпилотни надводни и подводни апарати да предават управлението си на друг възел. Тъй като $D_{stand\text{-}off} > D_{direct_link}$, безпилотните системи трябва да притежават автономност при възможна загуба на връзка. Точката *P* се позиционира умерено вдясно към Децентрализацията ($T_{eq}(P) = 0{,}65$).

2.1.2.3. Свързаност (C): Платформено-центричност – Мрежово-центричност

Свързаността се определя от пропусквателната способност на комуникационната мрежа (*Bnet*) спрямо обема на сензорния поток (D_{sensor}). При $Bnet \geq\geq D_{sensor}$ клони към пълна мрежово-центричност. Тъй като обработката на хидроакустични данни изисква висок капацитет, се прилага хибридна архитектура – бордова първична филтрация на безпилотните подводни апарати и пълна мрежова интеграция на данните. Точката *C* се позиционира силно вдясно към Мрежово-центричността ($T_{eq}(C) = 0{,}80$).

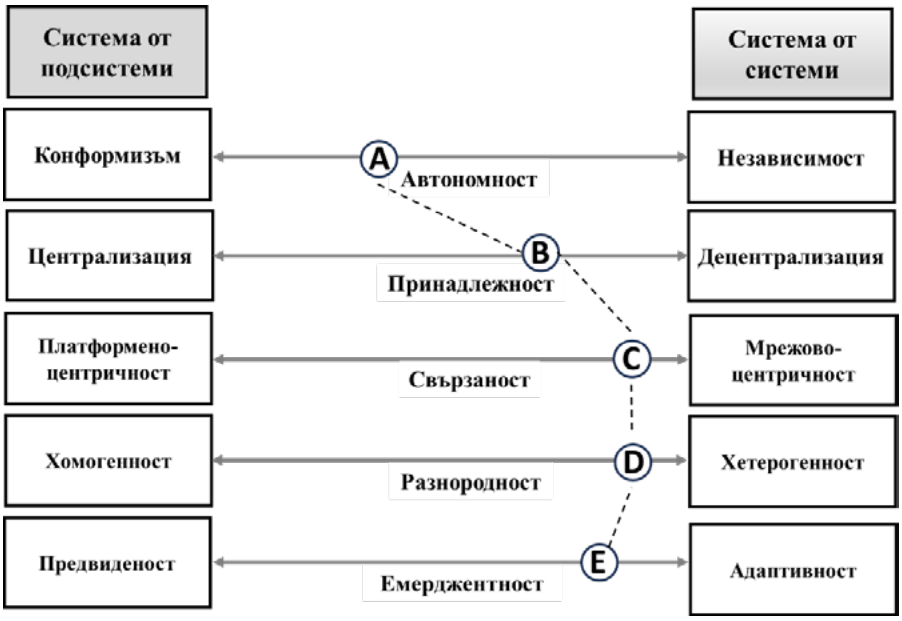
2.1.2.4. Разнообразие (D): Хомогенност– Хетерогенност

Разнообразието (качествено и количествено) се детерминира от физическата и функционалната неоднородност на сензорните канали (сонар, лазер, магнитометър, оптични камери) съгласно Закона за необходимото разнообразие (Ashby 1956, pp. 202 – 218). Поради необходимостта от детекция и неутрализация на широк спектър от мини (дънни, котвени, плаващи), системата изисква висок спектър от хетерогенни платформи. Точката *D* клони силно вдясно към Хетерогенността ($T_{eq}(D) = 0.85$).

2.1.2.5. Емерджентност (E): Предвидимост – Адаптивност

Емерджентността флуктуира между предварително планираните поискови галсове и динамичното самоорганизиране на автономните апарати при промяна на хидрологията в района на противоминната операция. Поради неопределеността на подводната среда адаптивността е критична за

преизчисляване на маршрутите при откриване на препятствия. Точката *E* се позиционира силно вдясно към Адаптивността ($T_{eq}(E) = 0{,}75$).



Фигура 2. Профил на равновесие и детерминирани точки на противоминната CoC (адаптирано по Sauser et al. 2009)

За разлика от невоенните CoC, при противоминната CoC точката на автономност (*A*) е изместена към полюса на конформизма. Това не нарушава характера на системата, а отразява фундаменталната военна специфика: строгата подчиненост на морските роботизирани комплекси на командната верига, правилата за употреба на сила и оперативните протоколи на кораба носител. Тази специфична конфигурация потвърждава, че противоминната система функционира като управляем тип CoC.

2.2. Мрежово-центрична архитектура и информационни слоеве

Мрежово-центричният характер на противоминната CoC се материализира чрез структурирането на трислойна комуникационно-информационна архитектура, която интегрира физическата, информационната и когнитивната област.

2.2.1. Сензорен слой

Обхваща безпилотни апарати намиращи се във въздушното пространство, на повърхността и под повърхността на водата. Автономните

подводни апарати и безпилотните надводни катери събират първични хидроакустични данни чрез специализирани хидроакустични станции, магнитометри и оптични камери. Слоят генерира суров информационен поток, който се подлага на първична филтрация.

2.2.2. Информационен слой

Осигурява устойчива преносна среда чрез комбинация от радио-, оптични и акустични канали:

Подводна комуникация. Използва се хидроакустичен модем за връзка между безпилотните подводни апарати/дистанционно управляеми апарати с безпилотните надводни катери.

Надводна/Въздушна комуникация. Безпилотните надводни катери предават данни към ретранслатор на борда на БЛА или директно към кораба носител чрез защитен радиоканал.

Оперативна връзка. Корабът носител споделя обобщената картина към флагманския кораб на тактическата група/бреговия център за управление.

2.2.3. Команден/Когнитивен слой

Разположен е в Бойния информационен пост на кораба носител. Постъпващите данни се подлагат на мултидомейно сливане посредством алгоритми с изкуствен интелект и автоматично разпознаване на цели. Това намалява времето за обработка и свива цикъла за вземане на решение – от часове на броени минути – генерирайки Единна оперативна картина.

2.3. Функционален и технически анализ на съставните системи в противоминната СоС

За разкриване на пълния оперативен профил на СоС е извършен функционален анализ на четирите основни съставни компонента.

2.3.1. Кораб носител

Корабът-носител се трансформира от класическа противоминна платформа в мобилен команден и логистичен интеграционен възел. Той оперира на безопасно разстояние ($D_{stand\text{-}off} \geq\geq 15$ nm) от границата на минното поле.

Функционални модули на кораба носител:

Система за спускане и обиране. Специализирани кран-балки и кърмови рампи с компенсация на клатенето за безопасно опериране с безпилотен надводен катер и автономни подводни апарати при вълнение на морето до 4 – 5 бала.

Център за управление и сливане на данни. Модулен боен информационен пост, оборудван със сървърни масиви за анализ на основата на изкуствен интелект на хидроакустични изображения.

Логистично-технически контейнерен модул. Стандартизирани 20-футови контейнери за техническо обслужване, зареждане на акумулаторни батерии и съхранение на подривни заряди.

2.3.2. Безпилотен надводен катер

Надводният катер изпълнява ролята на предноизнесен повърхностен сензорен и ретранслационен възел, навлизащ непосредствено в миноопасната зона.

Оперативни функции. Носи на борда си специализирана буксируема ХАС (хидроакустична станция) за бързо обследване на големи морски акватории; служи като платформа за спускане на малки автономни подводни апарати/дистанционно управляеми подводни апарати; изпълнява функциите на комуникационен хъб между подводната акустична среда и радиомрежата на повърхността.

Технически показатели: Дължина 11 – 13 m, висока автономност (24 h), ниско магнитно и акустично поле.

2.3.3. Безпилотен летателен апарат

Безпилотният летателен апарат осигурява въздушния компонент на системата, свързвайки физическата и информационната област.

Оперативни функции. Изпълнява ролята на въздушен комуникационен ретранслатор, разширявайки хоризонта на пряка видимост за трансфер на данни между безпилотния надводен катер и кораба носител на разстояния над 20 nm; провежда оптическо, инфрачервено и лазерно разузнаване за откриване на плаващи и плитководни дрейфащи мини.

2.3.4. Автономни и дистанционно управляеми подводни апарати

Подводните роботизирани комплекси са прецизни поразяващи и идентифициращи инструменти на СоС.

Автономен подводен апарат. Провежда високоскоростно автономно батиметрично картографиране и откриване на дънни мини по предварително зададени галсове. Разполага с високочестотна ХАС и инерциална навигационна система.

Дистанционно управляем подводен апарат. Използва се в цикъла за идентификация и неутрализиране на мините. Насочва се до открития миноподобен обект чрез видеокамери и ХАС, след което извършва неутра-

лизиране чрез полагане на подривен заряд или чрез апарат за еднократно неутрализиране (напр. Saab MuMNS / Seafox C).

III. Заключение

Проведеният анализ потвърждава, че преходът от конвенционални противоминни кораби към мрежово-центрична CoC представлява фундаментална промяна в концепцията за провеждане на противоминни операции.

Направеният анализ позволява да бъдат формулирани следните изводи:

1. Чрез позициониране на кораба носител на безопасно разстояние и изнасяне на рисковите функции върху безпилотните платформи, индексът на риск за личния състав се свежда до минимум.

2. Резултатите от математическия модел показват, че оптималното равновесие на системата изисква преход към децентрализирана, хетерогенна и адаптивна мрежова архитектура при запазване на пълния оперативен контрол от човека оператор при неутрализацията на откритите мини.

3. Вграждането на трислойната информационна архитектура осигурява реално мултидомейнно сливане на данни, съкращавайки цикъла за вземане на решение и постигайки нарастване на поисковата производителност, благодарение на паралелното изпълнение на задачите от безпилотните модули, спрямо последователния поискови цикъл на традиционните минни ловци.

БЕЛЕЖКИ

1. DEPARTMENT OF THE NAVY, 1996. *NWP 3-15: Naval Mine Warfare,* ch. 3 – 4. Washington, D.C.: Office of the Chief of Naval Operations, Department of the Navy.

REFERENCES

ALBERTS, D.; GARSTKA, J. & STEIN, F., 1999. *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd ed. Washington, D.C.: CCRP Publication Series. ISBN 1-57906-019-6.

ALBERTS, D.; GARSTKA, J.; HAYES, R. & SIGNORI, D., 2001. *Understanding Information Age Warfare*. Washington, D.C.: CCRP Publication Series. ISBN 1-893723-04-6.

ASHBY, W., 1956. *An Introduction to Cybernetics.* London: Chapman & Hall. ISBN 978-0416683003.

CEBROWSKI, A. & GARSTKA, J., 1998. Network-Centric Warfare: Its Origin and Future. *U.S. Naval Institute Proceedings*, vol. 124, no. 1, ch. 1, p.139 [January 1998].

[online]. Available from: https://www.usni.org/magazines/proceedings/1998/january/network-centric-warfare-its-origin-and-future. [Last viewed: 04 August 2026].

KOOPMAN, B., 1980. *Search and Screening: General Principles with Military Applications.* Annapolis, MD: Naval Institute Press. ISBN 978-0870216275.

SAUSER, B.; BOARDMAN, J. & GOROD, A., 2009. System of Systems Management. In: JAMSHIDI, M. (Ed.). *System of Systems Engineering: Innovations for the 21st Century*, ch. 8, pp. 191 – 217. Hoboken, NJ: John Wiley & Sons. ISBN 978-0-470-19792-9.

STOYANOV, N., 2017. *Riskove i zaplahi za sigurnostta na vodnata transportno-prenosna sistema*. Varna: Tera Balkanika. ISBN 978-619-90844-0-3. [in Bulgarian].

NETWORK-CENTRIC SYSTEM OF SYSTEMS MODEL IN MINE COUNTERMEASURES

Abstract. The paper investigates the transformation of mine countermeasures (MCM) operations through the application of the systems engineering concept of a network-centric "System of Systems" (SoS). It substantiates the necessity of transitioning from traditional vessels operating in risk zones to an innovative architecture that operationally integrates a mothership and heterogeneous unmanned platforms (USVs, UAVs, AUVs, and ROVs). Utilizing an adapting Boardman, Sauser, and Gorod's systemic criteria, the analytical equilibrium profile of the MCM complex is derived, establishing critical operational effectiveness coefficients. A three-tiered network-centric framework (sensor, information, and decision grids) is integrated, providing multi-domain data fusion. The results demonstrate that within this framework, the mothership is transformed into a tactical integration hub operating at a safe standoff distance, while synergy among unmanned modules significantly compresses the decision loop.

Keywords: network-centric system; mine countermeasures "System of Systems"; mine countermeasures; unmanned systems

Commander Dr. Krasimir Angelov
WoS Researcher ID: ABK-9726-2022
ORCID iD: 0000-0003-0773-6611
Naval Tactics Department
Faculty of Navigation
Nikola Vaptsarov Naval Academy
73, Vasil Drumev St.
9002 Varna, Bulgaria
E-mail: angelov@nvna.eu

https://doi.org/10. 66334/annu26_commodinfo

КОМУНИКАЦИОННИ МОДЕЛИ НА ВЛИЯНИЕТО НА МЕДИЙНАТА ИНФОРМАЦИЯ ВЪРХУ СПОРТА КАТО ЕЛЕМЕНТ НА НАЦИОНАЛНАТА УСТОЙЧИВОСТ

Кубрат Пулев
Военна академия „Георги Стойков Раковски“

Абстракт. Настоящият доклад изследва ролята на медийната информация и спортния дискурс като стратегически компоненти на националната устойчивост. Анализирани са класическите комуникационни модели – теорията за поставяне на дневен ред, рамкирането и култивацията, като е проследено тяхното проявление в съвременната дигитална система (Web 2.0). Специално внимание е отделено на децентрализирания мрежов модел и влиянието на социалните мрежи върху изграждането на дигитална устойчивост на общностите и мотивацията за масов спорт. Докладът идентифицира както позитивните ефекти от спортния наратив (социална кохезия, демографско здраве, мека сила), така и системните рискове, свързани с алгоритмичната поляризация, ехо-камерите и кибертормоза над националните спортни елити. Обосновава се тезата, че етичното и стратегическото конструиране на медийното спортно съдържание е критичен стълб за стабилността на нацията при кризи.

Ключови думи: комуникационни модели; медийна информация; национална устойчивост; дигитални медии; спортен дискурс; социална кохезия

Въведение

В съвременното глобализирано и силно дигитализирано общество медиите и спортът се намират в дълбока интерактивна симбиоза (Wenner 1998). Спортът отдавна е надхвърлил рамките на чистата физическа култура и развлечението, превръщайки се в мощна индустрия, инструмент за социално сближаване и проекция на мека сила (*soft power*) на международната сцена (Nye 2004). От своя страна медийната информация е основният катализатор, който оформя общественото възприятие за спортните процеси.

Концепцията за **национална устойчивост** (*national resilience*) обхваща способността на едно общество и неговите институции да устояват на външни и вътрешни кризи, да поддържат социална стабилност, системна цялост и да запазват своите фундаментални ценности. **Медийната информация в областта на спорта функционира като критичен фактор за укрепване или дестабилизиране на националната устойчивост.** Настоящият доклад анализира механизмите на това влияние чрез прилагането на класически и съвременни комуникационни модели.

Класически теоретични комуникационни модели

Връзката между традиционните масови медии, спортния наратив и обществото се обяснява чрез три фундаментални комуникационни теории:

● **Модел за поставяне на дневен ред (Agenda-Setting Theory).** Разработен от Маккомбс и Шоу (McCombs & Shaw 1972), този модел утвърждава, че медиите не казват на хората *какво да мислят*, а *за какво да мислят*. Когато медийната среда приоритизира масовия спорт, здравословния начин на живот или успехите на националните отбори, тя насочва обществения интерес към теми, които укрепват социалното здраве.

● **Модел на рамкирането (Framing Theory).** Според Ентман (Entman 1993) рамкирането включва подбора на определени аспекти от реалността и акцентирането върху тях в медийния текст с цел дефиниране на проблем или морална оценка. Начинът, по който се отразява дадено спортно събитие, може да бъде рамкиран като „национален триумф и обединение“ или като „символ на системен държавен разпад“, променяйки обществените нагласи.

● **Модел на култивацията (Cultivation Theory).** Джордж Гербнер (Gerbner et al. 2002) аргументира, че дългосрочното излагане на медийни съобщения оформя и „култивира“ възгледите на хората за света. Систе-

матичното присъствие на спортни ценности като честна игра (*fair play*), дисциплина и екипна работа изгражда по-устойчива ценностна система в гражданското общество.

Дигитални медии и социални мрежи в спортната екосистема

В ерата на Web 2.0 традиционната линейна комуникация е заменена от децентрализиран хоризонтален модел (Suarez-Lledo & Alvarez-Galvez 2023). Съгласно концепцията на Мануел Кастелс за **„мрежовото общество“** (*network society*) дигиталните мрежи трансформират социалните структури и се утвърждават като стратегическа инфраструктура за формиране на общественото мнение (Castells 2010). В спорта потребителите вече са активни съавтори (*prosumers*), които пряко участват в изграждането на спортния дискурс (Rowe, 2011).

Дигиталната трансформация променя динамиката на националната устойчивост в две основни направления:

А. Дигитална устойчивост и виртуални общности. В периоди на социални конфликти или глобални кризи дигиталните медии в спорта започват да изпълняват функции по поддържане на т.нар. **дигитална устойчивост** (*digital resilience*) на общностите (Shyyan & Halai 2024). Интерактивният модел за кризисна комуникация (*Interactive Crisis Communication Model – ICCM*) демонстрира как заинтересованите страни в мрежата си взаимодействат, за да изградят обществена психическа устойчивост (Cheng 2021). Чрез платформи като Facebook, Instagram и TikTok спортните организации бързо мобилизират подкрепа, разпространяват здравна информация и поддържат духа на населението.

Б. Стимулиране на физическата култура. Съгласно Модела за онлайн спортна комуникация (*Model for Online Sport Communication – MOSC*) интерактивността и достъпността на дигиталното спортно съдържание определят неговото реално социално въздействие (Pedersen et al. 2021). Изследванията показват, че позитивните ролеви модели на спортисти, инфлуенсъри в социалните мрежи, стимулират здравословно поведение и мотивират младежите да се занимават с физическа активност (Popa et al. 2024). Това директно рефлектира върху здравната и демографската устойчивост на нацията.

Измерения на националната устойчивост чрез спортната информация

Медийното отразяване на спорта влияе върху три основни стълба на националната устойчивост, които са обобщени в таблица 1. В контекста на

хибридни заплахи спортната журналистика, базирана на етични стандарти, служи като информационен буфер. Тя генерира градивни разказвателни модели (*narratives*), които неутрализират опитите за външно дестабилизиране на общественото съзнание.

Таблица 1. Влияние на медийното отразяване на спорта върху националната устойчивост

Измерение на устойчивостта	***Роля на медийната информация в спорта***	***Ефект върху нацията***
Социално-психологическо	Изграждане на национална гордост и колективна идентичност при международни победи	Намаляване на вътрешните социални деления; засилване на социалната кохезия
Здравно и демографско	Популяризиране на масовия и ученическия спорт чрез дигитални кампании.	По-здраво население, по-ниски разходи за здравеопазване, физическа готовност при кризи
Геополитическо	Проектиране на позитивен образ на държавата чрез спортна дипломация и успехи	Укрепване на международния авторитет и легитимността на държавата

Рискове, дезинформация и негативни влияния

Комерсиализацията и алгоритмичната структура на съвременните медийни платформи крият и специфични рискове за националната сигурност:

● **Информационни балони и радикализация на феновете.** Социалните мрежи често свиват публичния дебат в „ехо-камери“. Алгоритмите, целящи сензации, често фаворизират конфликтното съдържание (скандали, съдийски грешки, хулиганство). Това може лесно да бъде експлоатирано за разпалване на вътрешна агресия и разделение в обществото (Rowe 2011).

● **Дигитален натиск върху националните елити,** Спортистите, представляващи страната, са подложени на интензивен кибертормоз и медиен натиск. Този дигитален стрес причинява висока предсъстезателна тревожност и влошава спортното представяне (Popa et al. 2024). Провалът на национално ниво, мултиплициран от негативно медийно рамкиране,

води до спад в колективния дух и националното самочувствие.

Нагледен пример за използване на спорта като спойка за нацията е политиката на американския президент Доналд Тръмп. Спортът заема изненадващо централно и стратегическо място в дневния ред на администрацията му, като се явява основен инструмент в неговата Национална стратегия за устойчивост[3] така и в по-широката му вътрешна и геополитическа политика.

През втория си мандат Тръмп предприема безпрецедентни стъпки за интегриране на спорта в държавното управление, разглеждайки го като въпрос на национална сигурност и обществена стабилност. Мястото на спорта в неговата стратегия се проявява в три ключови направления:

● **Законодателно и финансово стабилизиране на колежанския спорт**. Тръмп официално дефинира хаоса в американския колежански спорт (произтичащ от съдебни дела и новите правила за заплащане на атлетите чрез NIL договори) като криза, застрашаваща националната система. Президентът подписва поредица от изпълнителни заповеди за спасяване на колежанския спорт. Те налагат строги федерални регулации върху трансферите и финансирането. Администрацията му застава зад двупартийния закон ***Protect College Sports Act***. Целта е да се защитят над 500 000 студенти атлети и да се гарантират близо 4 милиарда долара годишни стипендии, което се разглежда като инвестиция в младежката устойчивост на нацията.

● **Защита на женския спорт и социална политика**. Спортът се превръща в основно бойно поле за прокарването на социалните приоритети на Белия дом, свързани с традиционните ценности и вътрешната кохезия. Тръмп издава ключова изпълнителна заповед, с която **забранява на транссексуални спортистки да се състезават в женските спортове** в училища с федерално финансиране. Мотивът е „защита на безопасна и честна спортна среда за жените и момичетата“.

● **Спортът като „мека сила“ и инструмент за сигурност**. В контекста на съвместното домакинство на САЩ, Мексико и Канада на **Световното първенство по футбол** през 2026 и подготовката за **Олимпийските игри в Лос Анджелис** през 2028 година, администрацията на Тръмп използва големите спортни форуми за икономическа мобилизация и проекция на американската мощ.

Тези факти водят до извода, че докато класическата устойчивост на Тръмп се фокусира върху сигурността, веригите за доставки и икономическия суверенитет, **спортът служи като психосоциалното лепило в неговата доктрина „Америка на първо място“**. Чрез силна федерална

намеса в регулацията на спорта неговата стратегия се опитва да запази финансовата стабилност на младежките програми, да защити традиционните ценности и да проектира глобално влияние. За да се постигне тази цел се прилага структурна схема на комуникационните потоци (фигура 1). Анализът очертава определена схема на използване на медиите като проводник на конкретни послания и нагласи в обществото. Тази схема илюстрира как медийната информация преминава през филтрите на различните комуникационни модели и се трансформира в ресурси за национална устойчивост или в дестабилизиращи рискове за конкурентните системи.

ГЕНЕРАТОРИ НА ИНФОРМАЦИЯ
(Спортни събития, атлети-инфлуенсъри, държавни институции, кризи)

КАНАЛИ ЗА РАЗПРОСТРАНЕНИЕ
Традиционни медии (ТВ, преса) – линейни информационни потоци
Дигитални платформи & Web 2.0 – интерактивни потоци

КОМУНИКАЦИОННИ ФИЛТРИ И МОДЕЛИ
ПОСТАВЯНЕ НА ДНЕВЕН РЕД
(Фокус върху масов спорт срещу скандали)
РАМКИРАНЕ (Национален триумф срещу системен колапс)
КУЛТИВАЦИЯ (Дългосрочно вграждане на етични ценности и Fair Play)

ПОЗИТИВЕН ИЗХОД: УСТОЙЧИВОСТ	**НЕГАТИВЕН ИЗХОД: РИСКОВЕ**
Психосоциална кохезия	Радикализация на феновете (Ехо-камери)
Дигитална устойчивост при кризи	Кибертормоз над спортния елит
Подобрено демографско здраве	Ерозия на националното самочувствие

Фигура 1. Структурна схема на комуникационните потоци

Методологически насоки за емпиричното изследване

Изследователският проект с работно заглавие „Медийно отражение на спорта и неговото влияние върху националната устойчивост: Модели-

ране, ефекти и измерване“ представлява пълноценна научноизследователска рамка за емпирична верификация на теоретичните комуникационни модели в реална среда. Основната цел е да се установи по какъв начин разгледаните комуникационни модели при отразяването на спорта в националните медии трансформират спортната информация в реален фактор за укрепване на физическото здраве, социалната кохезия и информационния имунитет на българското общество.

Обектът на изследването може да се дефинира най-общо като медийното спортно съдържание в българските масмедии и съответните социално-поведенчески реакции на аудиторията, чрез които медийно отразеният спорт влияе върху трите измерения на националната устойчивост – здравна, психологическа и информационна.

Основните изследователски въпроси са:

– до каква степен медийният дневен ред приоритизира масовия спорт спрямо комерсиалния елитен спорт;

– как различните рамки на отразяване (позитивна интеграция срещу скандали и корупция) променят общественото доверие и социалната ангажираност;

– по какъв начин спортните герои и медийните кампании функционират като катализатори на националната кохезия по време на кризи.

За да се верифицират теоретичните допускания в изследването относно ролята на спорта в националната устойчивост на Република България, се предлага провеждането на смесено изследване, което комбинира количествени и качествени подходи:

А. Обект, предмет и цели на изследването:

– обект – българското медийно пространство (дигитални спортни медии и официални страници на спортни федерации във Facebook/Instagram);

– предмет – влиянието на спортните публикации и потребителските коментари върху усещането за национална гордост, социално единство и мотивация за физическа активност;

– основна цел – да се измери съотношението между мобилизиращия (позитивен) и поляризиращия (негативен) ефект на спортните новини в дигиталната среда.

Б. Методи за събиране на данни:

а. Количествен контент-анализ:

– извадка – анализ на текстовете на най-четените спортни материали и постове в социалните мрежи по време на голямо международно събитие (напр. олимпийски игри или европейско първенство);

– кодировъчни единици – търсят се ключови маркери за рамкиране (напр. „национален дълг“, „провал“, „герои“, „корупция“). Публикациите се класифицират по скала на тоналност – позитивна, неутрална, деструктивна.

б. Онлайн анкета:

– таргет група – национално представителна извадка на активни потребители на дигитално спортно съдържание (възраст 18 – 65 г.);

– ключови индикатори – честота на потребление на спортни новини, нива на субективно усещане за национална принадлежност и самооценка на личната спортна активност, вдъхновена от социалните мрежи.

в. Дълбочинни интервюта. Провеждане на полуструктурирани интервюта със спортни журналисти и психолози на национални отбори с цел установяване на реалния размер на психологическия натиск и дигиталния стрес (cyberbullying) върху състезателите.

В. Основни изследователски хипотези за тестване:

– H1 – публикациите, рамкиращи спортните постижения като колективен успех на нацията, повишават равнището на социална кохезия сред потребителите независимо от техните политически пристрастия;

– H2 – дигиталните алгоритми в социалните мрежи извеждат приоритетно конфликтни и сензационни спортни новини на преден план (поставяне на дневен ред), което засилва обществената тревожност и усещането за институционална нестабилност;

– H3 – Наличието на координирани кампании за масов спорт в социалните мрежи има по-висока степен на култивация на здравословни навици сред младежите в сравнение с традиционните телевизионни формати.

Заключение

Медийната информация за спорта не е просто пасивен хроникьор на събития, а **активен инструмент за управление на социалните процеси и укрепване на националната устойчивост**. Класическите модели на поставяне на дневен ред и рамкиране, съчетани със съвременните дигитални мрежови модели, доказват, че начинът на конструиране на спортния наратив има директни държавнотворчески последици. За да функционира спортът като истински елемент на националната устойчивост, е необходима целенасочена държавна политика за подкрепа на спортната журналистика, дигитална медийна грамотност и стратегическо използване на дигиталните мрежи за промотиране на здраве, единство и споделени ценности.

БЕЛЕЖКИ

1. THE WHITE HOUSE, 2026. *National Resilience Strategy*, Jun 2026. Available from: https://www.whitehouse.gov/wp-content/uploads/2026/06/2026-National-Resilience-Strategy-1.pdf.

REFERENCES

CASTELLS, M., 2010. *The Rise of the Network Society* (2nd ed.). Hoboken: Wiley-Blackwell.

CHENG, Y., 2021. Social Media Crisis Communication Model for Building Public Resilience. *Journal of Contingencies and Crisis Management*, vol. 29, no. 4, pp. 370 – 380.

ENTMAN, R.M., 1993. Framing: Toward Clarification of a Fractured Paradigm. *Journal of Communication*, vol. 43, no. 4, pp. 51 – 58.

GERBNER, G.; GROSS, L.; MORGAN, M. & SIGNORIELLI, N., 2002. Growing up with television: The cultivation perspective. In: J. BRYANT & D. ZILLMANN (Eds.), *Media effects: Advances in theory and research* (pp. 43 – 67). Lawrence Erlbaum Associates.

MCCOMBS, M.E. & SHAW, D.L., 1972. The Agenda-Setting Function of Mass Media. Public Opinion Quarterly, vol. 36, no. 2, pp. 176 – 187.

NYE, J. S., 2004. *Soft Power: The Means to Success in World Politics*. PublicAffairs.

PEDERSEN, P.M.; LAUCELLA, P.C.; KIAN, E.M. & GEURIN, A.N., 2021. *Strategic Sport Communication* (4th ed.). Human Kinetics.

POPA, D. et al., 2024. Digital social media factors impacting on athletes‘ motivation and performance. *Journal of Sport and Kinetic Movement*, vol. 43. no. 2, pp. 12 – 19. Available from: https://doi.org/10.52846/jskm/44.2024.1.8.

ROWE, D., 2011. *Global Media Sport: Flows, Forms and Futures.* Bloomsbury Academic.

SHYYAN, O. & HALAI, M., 2024. Digital resilience of sports communities in a Facebook group during periods of crisis. *Health, Sport, Rehabilitation*, vol. 10, no. 2, pp. 45 – 56.

SUAREZ-LLEDO, V. & ALVAREZ-GALVEZ, J., 2023. *The Digital Communication model: A New Paradigm of Interactivity.* ResearchGate.

WENNER, L.A. (Ed.), 1998. *MediaSport*. London: Routledge.

COMMUNICATION MODELS OF THE INFLUENCE OF MEDIA INFORMATION ON SPORT AS AN ELEMENT OF NATIONAL RESILIENCE

Abstract. This report examines the role of media information and sports discourse as strategic components of national resilience. It analyzes classical communication models – Agenda-Setting, Framing, and Cultivation theories – tracing their manifestation within the contemporary digital ecosystem (Web 2.0). Particular

attention is given to the decentralized network model and the impact of social media (Facebook, TikTok, Instagram) on building digital resilience within communities and motivating mass sports participation. The report identifies both the positive outcomes of sports narratives (social cohesion, demographic health, soft power) and systemic risks linked to algorithmic polarization, echo chambers, and cyberbullying directed at national sports elites. It concludes that the ethical and strategic construction of media sports content represents a critical pillar for maintaining national stability during crises.

Keywords: communication models; media information; national resilience, digital media; sports discourse; social cohesion.

Kubrat Pulev
Land Forces Department
Command and Staff Faculty
Rakovski National Defence College
82, Evlogi and Hristo Georgievi Blvd
1504 Sofia, Bulgaria
E-mail: k.pulev@rndc.bg

https://doi.org/10. 66334/annu26_systprotuav

СИСТЕМЕН ПОДХОД ЗА ПРОТИВОДЕЙСТВИЕ НА БЕЗПИЛОТНИ ЛЕТАТЕЛНИ АПАРАТИ

доц. д-р Любосвет Стоев, полковник доц. д-р Живо Петров
Военна академия „Георги Стойков Раковски“

Абстракт. Разпространението на ниско бюджетни безпилотни летателни системи (БЛС) промени коренно характера на съвременния конфликт и създава безпрецедентна „асиметрия на разходите и обмяната на енергия“ в противовъздушната отбрана. Тази статия разглежда глобалния пейзаж на борбата с БЛС (C-UAS) през системна призма, анализирайки оперативния опит от Украйна, Близкия изток и други конфликтни зони, за да идентифицира модели, неуспехи и нововъзникващи решения. Въз основа на количествен анализ на разходите и ефективността и скорошни оперативни данни ние твърдим, че ефективната стратегия за C-UAS изисква многопластов, базиран на знания подход, интегриращ усъвършенствани системи за насочена енергия с доказани практически мерки. Статията оценява както екзотични технически решения, включително лазерни системи, електромагнитно и вихрово оръжие, така и прагматични подходи като мобилни огневи екипи за прехват на дронове. В заключение, нито една технология не предлага панацея. Успехът изисква системна архитектура, която балансира разходите, мащабируемостта и оперативната адаптивност.

Ключови думи: анализ на ефективността; електронна война; защита от дронове; оръжия с насочена енергия; противодействие на безпилотни летателни апарати; системно инженерство

I. Увод

Ерата на кибервойната, в която дроновете играят централна роля, настъпи с изумителна скорост. Това, което започна като ограничена и целева способност за разузнаване, се превърна в повсеместен тактически инструмент, използван както от официални въоръжени сили и служби за сигурност, така и от недържавни играчи и дори отделни лица. Конфликтът в Украйна ясно подчерта тактическата стойност на дроновете във войната (Lin-Greenberg 2025). И двете страни разгърнаха безпилотни системи за разузнаване, електронна война и целенасочени удари. Както анализаторите отбелязват, мнозина са „осъзнали факта, че сега сме здраво в ерата на войната на дронове".

Тази трансформация създава значимо стратегическо предизвикателство. Асиметрията между разходите и размяната на средства е поразителна: защитата срещу руски безпилотни летателни апарати на стойност 400 долара често изисква разходване на ракетен прехващач, който струва стотици хиляди долари. Количественият анализ показва, че цената на атака варира с повече от „пет порядъка" в различните категории системи, варирайки от приблизително 20 долара за електронно противодействие до 4,75 милиона долара за зенитни управляеми ракети. Този съществен икономически дисбаланс прави традиционните архитектури на противовъздушната отбрана икономически неустойчиви при сценарии за противодействие на рояк от дронове – едно предизвикателство, което се среща все по-често (Boyle 2020).

Отвъд бойните полета и зони на конвенционални и неконвенционални военни конфликти нарастването на неправомерната активност на граждански дронове създава значителен интерес към използването на системи за противодействие на дронове (C-UAS) в световен мащаб. Многобройните инцидентите с дронове на летища, в близост до критична инфраструктура и по време на публични събития предизвикват реакция както във военната, така и в гражданската сфера. Безпилотните системи са не само тактическо, но и системно предизвикателство.

Настоящата статия използва смесен методологичен подход, който комбинира следните елементи:

• Анализ на приложението на безпилотните летателни системи (БЛС) и тяхното противодействие в конфликтни региони (Украйна, Близкия изток, Афганистан – Пакистан, Югоизточна Азия, Африка и Латинска Америка) въз основата на информация от открити източници, които включват както посочен фактологичен материал, така и аналитични публикации.

• Количествен анализ на разходите и ефективността на използваните подходи за C-UAS. Въз основа на Многослойния модел на отбранителната икономика (MILDEM), разработен от публично достъпни набори от данни (Oryx, SIPRI, ACLED) и спецификации на отбранителната индустрия, се оценяват редица различни C-UAS системи спрямо стандартизирани профили на заплахи чрез използване на описателна статистика и Монте Карло симулация (Pokorny 2026).

• Рамков подход за системно инженерство, който включва приложение на принципите на INCOSE[1] за оценка на архитектурите на C-UAS, като се набляга на необходимостта от интегрирани и многопластови системи за защита, а не решения на парче.

• Сравнителен анализ на различните C-UAS технологии – от класическите средства за противовъздушна отбрана (ПВО), като зенитни управляеми ракети и артилерийски/картечни системи, до съвременни специализирани решения за кинетичен прехват, радио-електронна борба, оръжия с насочен пренос на енергия спрямо тактико-технически изисквания и показателите за рентабилност.

Интегрирането на изброените подходи е насочено към изграждане на методика за подбор на оптимизирани C-UAS решения за нуждите на всеки потребител.

II. Глобален преглед на конфликтните региони

В тази част са анализирани открити данни за заплахата от дронове и C-UAS подходите в различни „горещи точки“ по света. Целта е да се извлекат добри практики и успешни модели.

2.1. Войната в Украйна

Украинският конфликт се превърна в основна „лаборатория“ за съвременна „война на дроновете“ и тяхното противодействие.[2] Както Русия, така и Украйна използват широко дронове не само за разузнаване, а и като средство за поразяване, като демонстрират тактическата, оперативната и стратегическата стойност на безпилотните системи от различен клас във високоинтензивна конвенционална война.

Паралелна еволюция на C-UAS във войната в Украйна

В съвременния военен конфликт с висока интензивност иновациите живеят изключително кратко – от порядъка на две седмици.[3] Това води до устойчивост на фронтовата линия и технологична конвергенция и от две-

те страни. Ето защо C-UAS подходите и на двете страни са практически сходни. Може отчетливо да се проследи системност, при която борбата с дронове е разделена териториално и функционално:

• *Фронтова защита от дронове.* Тя не може да се разглежда отделно от воденето на военни действия и ударното използване на дронове само по себе си. В „малкото небе“ се разиграват истински дуели между FPV-дроновете. Те успешно се използват срещу по-големи дронове като украинската „Баба Яга“ и руския „Вампир“ („Упырь“). Паралелно с това се използват пасивни, а по рядко и активни средства за радиоелектрона борба (РЕБ). Причината за това е, че тяхното местонахождение лесно се идентифицира и по активните уреди бива нанесен удар. Заедно с това активно се използват средства за маскировка, включително защита от термовизионни камери, както и пасивни защитни средства, като мрежи и решетки. Техниката и транспортните средства се разсредоточават и тяхното придвижване става квазихаотично, за да намали вероятността за среща с неприятелски дрон.

• *Защита от дронове в тила.* В момента и двете страни разчитат на изграждането на ешелонирана C-UAS система в допълнение на съществуващите средства за ПВО.[4] На ниско ниво (до около 1000 м височина) действат мобилни огневи групи (МОГ). Руската федерация, аналогично на Украйна, сформира мобилни огневи групи (МОГ) за борба с дронове, които използват леки проходими пикапи. Използват се модели като *Toyota Hylux*, „Газела“ и „УАЗ Фармер“, които оборудва със сдвоени двойни 7,62-милиметрови тежки картечници ПКТ, термовизионни мерници, лазерни целеуказатели и детектори за дронове „Булат-4“ за нощни операции. За тях се използват специализирани боеприпаси На височина до 3000 м действат хеликоптери и самолети, като вече има стремеж да се ползват не реактивни изтребители, а леки самолети, като Як-52, Як-18т или *Cessna*. В Украйна се увеличава развръщането на бойни хеликоптери в мисии за противовъздушна отбрана. Главнокомандващият украинските въоръжени сили ген.-полк. Олександър Сирски съобщи, че „в зависимост от времето, нашите хеликоптери понякога свалят до 40% от дроновете в своите сектори“.[5] И двете страни се борят да защитят критичната си инфраструктура от все по-значимите вражески удари с дронове от самолетен тип с далечен обсег.

Иновационна политика и алтернативни решения

Взимащите решения от украинска страна успешно възприемат иновациите, като разглеждат приложението на дронове прехващачи като основен бъдещ тренд за развитие на C-UAS системите. Дроновете за кинетичен

прехват се оказват по-ефективни от зенитните управляеми ракети и зенитната артилерия. Способни са да преследват и унищожават вражески БЛА отвъд линията на пряка видимост и по време на полет на ниска цена, като минимизират рисковете за гражданското население.

Друго иновационно средство за борба с дронове е използването на лазерно оръжие. На фронта платформите и захранването на лазерните системи биха били твърде тромави, но в тила и като прикритие на критична инфраструктура такива системи вършат работа, като намаляват разходите за поразяване на единичен дрон до около 50 €. И двете страни активно разработват лазерно оръжие, което да позволи на неговата основа да се изгражда ефективно система за защита на критичната инфраструктура.

2.2. Близкият изток и Персийският залив

Близкият изток се очерта като друг критичен театър (Bill 1989) за оценка на ефективността на C-UAS. Благодарение на военните действия, водени от Израел, регионът се сблъсква с дроновете още от далечната 1982 г., когато те са активно използвани срещу сирийската армия в Ливан. Впоследствие, след двете войни в Ирак, войната срещу тероризма и срещу Ислямска държава, западната коалиция активно използва БЛА като ефективно средство за въздушно доминиране над слабо въоръжените иррегулярни части. Бурното развитие на малките дронове обаче още от гражданската война в Сирия ги прави достъпни за всеки играч, който желае да се изправи срещу големите сили в региона.

Ролята на Иран като доставчик на дронове за регионални посредници допълнително усложни средата със заплахи. Трансферът на барикадиращи боеприпаси и въоръжени безпилотни летателни апарати на Хизбула, силите на хусите и други групировки създаде разпределена мрежа от заплахи, която изисква усъвършенствани възможности за откриване и реагиране. Иран разширява спектъра на използване на дроновете, като ефективно използва баражиращ дрон за противовъздушна отбрана – снаряд 358, откриван често при мисии за противодействие на пропаганда. Такова средство се използва активно за борба с ударните дронове на западните държави. Над Йемен и Иран с него са свалени много *MQ-9 Reaper*.

2.3. Афганистан, Пакистан и Индия

Регионът Афганистан – Пакистан е свидетел на обширни операции с безпилотни летателни системи (БЛС), предимно от държавни субекти, които извършват мисии за борба с тероризма и наблюдение. Макар че тези

операции са с по-малка интензивност от конфликта в Украйна, те доведоха до значителни инвестиции в способностите на местните национални въоръжени сили да използват дронове.

В контекста на отношенията между Индия и Пакистан взаимните нарушения на въздушния суверенитет от дронове се превърнаха в постоянно предизвикателство. И двете държави инвестираха в средства за откриване и противодействие на електронната война, въпреки че планинският терен и сложното въздушно пространство създават уникални оперативни предизвикателства. Според съобщенията Индия е ускорила разработването на местни контролни безпилотни летателни системи (C-UAS) след инциденти по линията на контрол.

През 2025 г. за три дни имаше сериозен конфликт между двете ядрени държави.[6] Инцидентът, наречен Операция „Синдур“, в отговор на терористична атака на 22 април 2025 г. в Кашмир, при която загиват 26 туристи, Индия нанася въздушни удари срещу лагерите на терористичните групировки „Джайш-и-Мохамед“ и „Лашкар-е-тайба“. В отговор на тези действия Пакистан започва масирана контраатака с дронове, артилерия и въздушни удари. Скоро след това, конфликтът затихва. Този конфликт е ключов момент, който показва, че дроновете се превръщат в самостоятелен инструмент за демонстрация на сила между две ядрени държави.

2.4. Югоизточна Азия и Африка

Югоизточна Азия е свидетел на нарастващо разпространение на безпилотни летателни системи (БЛС), въпреки че противодействието на дроновете, използвани от инсургентите, все още е в начален стадий. В Мианмар се съобщава, че бунтовнически групировки използват търговски дронове за разузнаване и ограничени настъпателни операции, докато военната хунта предприема контрамерки.[7] Граничният конфликт между Тайланд и Камбоджа[8] по подобен начин отбеляза засилена активност на БЛС, въпреки че възможностите на различните фракции в региона изостават спрямо другите конфликтни зони.

В цяла Африка, регионът на Сахел е свидетел на нарастващо използване на дронове както от държавни сили, така и от недържавни участници, особено в антитерористични операции.[9] Подробните доклади за използването на C-UAS в Африка обаче остават ограничени, което отразява както по-ниския профил на тези конфликти, така и ограничените възможности на много регионални военни. Африканският съюз започна да обсъжда не-

обходимостта от координирани стратегии за C-UAS, но прилагането им остава предизвикателство.

2.5. Латинска Америка

Латинска Америка е преживяла значителна активност в областта на БЛС, предимно за наблюдение и разузнаване. Съобщава се, че наркокартели и престъпни организации използват дронове за ситуационна осведоменост и ограничени атаки.[10] Националните армии са започнали да инвестират във възможности за борба с неидентифицирани дронове (C-UAS), макар и не толкова сериозно, колкото във военна зона като Украйна. Разнообразният терен на региона – от гъсти дъждовни гори до градски центрове, представлява уникални тактически и оперативни предизвикателства, които изискват гъвкави решения.

III. Анализ на глобалното състояние

Сравнението между различните „горещи зони“ по света показва няколко критични особености:

1. Нито един подход за борба с безпилотните летателни апарати (C-UAS) сам по себе си не е доказал своята универсална ефективност самостоятелно.

2. Икономическата ефективност е доминиращото оперативно ограничение. Финансовата асиметрия между евтините атакуващи дронове и скъпите зенитни ракети е довела до търсене на по-достъпно противодействие.

3. Пасивните и преносими средства за електронно разузнаване (само един аспект на електронната война) се оказват изключително ефективни, докато активните системи, поради демаскиращите свойства на електромагнитното лъчение, сами са уязвими и стават актив с голяма стойност под ударите на атакуващи средства с ниска цена.

4. Заплахата също се развива изключително бързо. Появяват се рояци от дронове, които атакуват от различни направления и на различни височини. Много от дроновете стават автономни или управлението става по сателитен канал или през оптично влакно.

Ефективните C-UAS изискват подход на „защита в дълбочина“, който да комбинира откриване, проследяване и множество механизми за поражение в различни обхвати и височини, интегриран в многослойна система за отбрана.

3.1. Най-използвани и най-успешни методи за C-UAS

Въз основа на наличните данни тук са оценени най-ефективните подходи за борба с вражески дронове (Subramaniam, Lynch 2025). На първо място, това е електронната война, която има своите особености.

Радиочестотното заглушаване и *GPS spoofing* са най-широко използваните методи за борба с вражески дронове. От няколко години тези методи не работят, въпреки широко разпространеното спиране на мобилната връзка, даже в дълбокия тил на Русия. Причините са няколко и се крият в дизайна на дроновете и системите им за управление, в наличието на сателитна връзка като *Starlink*, *Irridium* и др. Управляваните по оптично влакно дронове са неуязвими за РЕБ, освен за бъдещи разработки, които въобще да изгарят електрониката и каквито се създават в Китай. Остро насоченият сигнал от спътниците на *Starlink* също е много трудно да бъде смутен на ниво дрон. В Русия експериментират с локално заглушаване на сателитния интернет на ниво спътник чрез система от мощни смутители с остро насочени антени, но това е решение за критична инфраструктура от дълбокия тил. За сметка на това, радиоелектронното разузнаване работи добре. Пехотата от двете страни използва детектори, които откриват присъствието на дронове в близката околност, с изключение на управляваните по оптичен кабел.

Много активно се работи по внедряването на дронове прехващачи от Украйна и Русия. Обикновено такива дронове се ползват на фронта и в прифронтовата зона. Иран успешно демонстрира дрон за ПВО и постига успехи срещу израелски и американски дронове. Ако на украинския фронт това са обикновени FPV дронове с несвойствена мисия или други мултироктори, то в Иран това е дрон от самолетен тип с турбореактивен двигател и инфрачервена камера, управляван от земята посредством таблет.

IV. Алтернативни високотехнологични решения за борба с дронове

Нарастващата необходимост от нови средства за борба с неприятелски дронове води до разработването на все нови и нови технически решения. Ако първоначално активно се използват насочени микровълнови излъчватели и такива системи се ползват добре за мирновременни задачи по сигурност на критични обекти и полицейски задачи, то военните дронове стават все по-устойчиви на подобно въздействие. Необходими са решения, които да позволяват ефективна борба с много дронове при ниска цена на единичен изстрел. Ето основните направления, в които се работи:

– специализирани боеприпаси против дронове;
– дронове прехващачи;
– лазерно оръжие;
– микровълново оръжие с висока мощност;
– електромагнитен катапулт;
– вихрово оръдие;

4.1. Оръжия с насочено предаване на енергията

Терминът „оръжие с насочено предаване на енергията“ (*directed energy weapons – DEW*) (Bloembergen, Patel et al. 1987) се появява по време на Студената война, придобивайки обществена известност през 80-те години на XX век в хода на Инициативата за стратегическа отбрана (*strategic defense initiative – SDI*) на президента на САЩ Роналд Рейгън. Наречена в медиите „Звездни войни“ – по името на популярната тогава научнофантастична филмова поредица, *SDI* предвижда базирани в космоса лазери и източници на снопове елементарни частици като противодействие на съветските и китайски ядрени ракети. Грандиозна концепция, която остава до голяма степен експериментална, но дава началото на десетилетия последващи изследвания.

Днес лазерното оръжие намира своята ниша не в космоса, а на земята като решение за противодействие на роящите от дронове. Войната в Украйна се превърна в голям полигон, в който и двете страни тестват лазерни прототипи за противодействие на разузнавателни и атакуващи дронове. Украинската страна тества системи като „Тризуб“[11] и *Sunray*[12], докато Русия експериментира с „Перун“[13] и „Задира“[14]. На практика всички водещи производители в отбранителния сектор разработват собствено лазерно оръжие.

Тази тактическа революция става възможна благодарение на преминаването от обемисти химически лазери към диодно напомпвани твърдотелни лазери. Чрез използването на полупроводникови диоди вместо светкавични лампи за захранване на кристална или влакнеста среда тези системи драстично подобряват ефективността, намаляват отпадъчната топлина и значително редуцират своя размер. По същество това са същите индустриални лазери, които заваряват шасита на автомобили и режат ламарина, а сега се използват за създаване на прототипи на оръжие.

Ключова иновация, свързваща индустриалните лазери и мобилните платформи, е появата на плоски лазерни геометрии. Чрез създаване на ин-

версна квантова заселеност в тънка и плоска плоча от лазерна среда вместо в традиционния цилиндър инженерите могат да извлекат висока мощност с превъзходно качество на лъча и минимално термично изкривяване. Тази „плоска“ архитектура позволява изход от киловатов клас при изненадващо компактен корпус, което прави лазера достатъчно мощен, за да заварява стомана, и достатъчно малък, за да се монтира на превозно средство. Двойната употреба на тази технология, при която един и същ основен модул може да обслужва фабричен цех и мобилна платформа за противовъздушна отбрана, бързо запълва разликата между индустриалното производство и развръщането на фронтовата линия.

Лазерните системи се утвърждават като водещо усъвършенствано решение, което обещава ниска цена на атака и мащабируеми отбранителни възможности.

4.2. Високомощно микровълново оръжие

Друго интересно технологично решение за борба с рояци от вражески дронове са високомощните микровълнови (*HPM*). Те също в технологично отношение се класифицират като оръжия с насочен пренос на енергията (*DEW*). Подобни средства се създават от всички страни с водеща оръжейна индустрия.[15] Въпреки широкия набор от технологично достъпни източници на микровълново лъчение, най-използваният източник за създаване на *DEW* е релативисткият магнетрон, който може да генерира импулси с висока пикова мощност.

Първоначално микровълновото оръжие се разработва за противодействие на импровизирани взривни устройства, но възможността да се увеличи мощността на лъчението и да се управлява насоченият лъч го прави перспективно средство за борба срещу рояк от дронове. Все още високата цена е пречка за това такова средство да бъде използвано масово.

4.3. Вихрови оръдия

Вихровите оръдия, които генерират вискоскоростни въздушни вихри, са предложени като некинетично средство за дестабилизиране или деактивиране на дронове. Подобно оръжие е създавано на територията на Австрия по времето на нацистка Германия през Втората световна война като част от програмата за създаване на „оръжие чудо“ (*wunderwaffe*) като средство за противодействие на нисколетящи самолети. В интернет има демонстрации на експерименти с въздействието на вихрови оръдия срещу дронове, както и научни анализи (Vanhorn 2026) по темата, които показват,

че при импулс с енергия над праговата дронът е дестабилизиран и пада от небето.

V. Заключение

Разпространението на безпилотни летателни системи коренно променя характера на военните конфликти и заедно с тях – характера на гражданската сигурност и устойчивост. Това, което някога е нишова способност, се трансформира в основен тактически инструмент, използван от разнообразни участници – от големи сили, до недържавни групировки и престъпни организации. Използваните навсякъде мултиротори, като продукцията на *DJI*, са стандартен инструмент за въздушна фотография, геодезия и фотограмметрии: те съчетават маневреност, точна автоматизация и обмислена екосистема от хардуер и приложения. За въздушна фотография дроновете на *DJI* (комерсиално достъпни граждански изделия като Mavic 3 Enterprise или Matrice 4E) позволяват бързо да се добиват качествени кадри от нужната височина и с припокриване, а благодарение на механичните затвори и стабилното окачване снимките са достатъчно контрастни и ясни, което е критично при последващо изграждане на цифрови модели. За задачи по геодезия са особено важни версиите с *RTK (*на англ. *real-time kinematic* – инерциална навигация в реално време). Те дават сантиметрова точност на геопривързването директно в метаданните на всеки кадър, като решително редуцират нужните наземни опорни точки. Във фотограмметриията целият цикъл е удобно затворен вътре в екосистемата на *DJI*: планирането на полета става директно в приложението за управление, а последващата обработка – в *DJI Terra*, където от снимките генерират ортофотокарти и цифрови модели на релефа, 3D-модели и облаци от точки. Всичко това е достатъчно компактно средство за придобиване на информация, която в ръцете на недоброжелател се превръща в критична опасност.

Конфликтът в Украйна убедително демонстрира, че сме „твърдо в ерата на война с дронове“ и икономическото смятане на отбраната сега е под безпрецедентен натиск.

Асиметрията между разходите и размяната, която характеризира войната с дронове, представлява структурно предизвикателство за традиционните архитектури на противовъздушната отбрана. Когато дрон за 400 долара може да наложи разходите за ракета за 4,75 милиона долара, защитникът е изправен пред по своята същност неустойчива динамика. Тази икономическа уязвимост се утежнява от адаптивността на противниците –

бързо променящи се тактики, височини и модели на атака, за да победят статични или предвидими защитни системи.



Фигура 1. Критични способности за придобиване на чувствителни георе-ферирани данни от граждански дронове като *DJI Matrice 4E* със сателитна навигация и инерциална *RTK* система

Ефективната C-UAS изисква отклонение от мисленето за „точково решение“ и приемане на истински системен подход. Доказателствата от глобалните конфликти са ясни:

• **Няма универсално решение.** Това, което работи в откритите равнини на Украйна, може да не е подходящо за гъстите джунгли на Югоизточна Азия, градската среда на Близкия изток или разнообразния терен на Латинска Америка. Системите за борба с безпилотни летателни апарати трябва да могат да се адаптират към местните оперативни условия и профили на заплахите.

• **Рентабилността трябва да бъде централният критерий за проектиране на C-UAS системи.** Икономиката на войната с дронове изисква отбранителните системи да бъдат достатъчно достъпни, за да могат да бъдат разгръщани в голям мащаб. Това предполага даване на приоритет на електронната война, насочената енергия и кинетичните системи, базирани на оръжия, пред скъпите ракетни прехващачи за мащабни заплахи.

• **Многопластовата защита е от съществено значение.** Нито една технология не предлага цялостна защита. Ефективните архитектури комбинират откриване, проследяване и множество механизми за поражение в различни обхвати, височини и видове заплахи – подход на „защита в дълбочина“, който отразява успешните рамки за противовъздушна отбрана.

Адаптивността и обучението трябва да бъдат институционализирани. Заплахата се развива непрекъснато и контрамерките трябва да се развиват заедно с нея. Създаването от САЩ на *JIATF 401* за унифициране на доктрината и ускоряване на внедряването на технологии, проектът *Synergia* на Обединеното кралство за гъвкаво разполагане и бързите иновации на Украйна в прихващането на дронове демонстрира важността на организационното обучение и гъвкавата адаптация.

Прилагането на методологията за системно инженерство *INCOSE*, комбинирана с принципи като рамката на любопитството *KEEN*, позволява структурирано разработване на устойчиви, адаптивни, достъпни и мащабируеми C-UAS решения.

Предизвикателството на противодействието на безпилотните летателни системи е в крайна сметка системно предизвикателство. То изисква не просто по-добри технологии, но и по-добра интеграция – на сензори и ефектори, на военни и граждански способности, на анализ на разходите и оперативната доктрина, на глобален опит и локална адаптация. Държавите и организациите, които овладеят това системно мислене, ще бъдат най-добре позиционирани да се ориентират в новата ера на войната с дронове.

Благодарности. Публикацията е разработена с подкрепата на Българската национална научна програма „Сигурност и отбрана: научна подкрепа за трансформация на сектора за сигурност“ от Министерството на образованието и науката на Република България в изпълнението на Националната стратегия за развитие на научните изследвания 2017 – 2030 и е приета с Решение на Съвета на министрите № 731 от 21 октомври 2021 г. съгласно Споразумение № ДО1-74/19.05.2022.

БЕЛЕЖКИ

1. Incose, 2025. Homepage. *Incose* [online] [last viewed 14.07.2026]. Available from: https://www.incose.org

2. PETERSON, N., 2026. Six Key Lessons from Ukraine’s Drone War. *Irregular Warfare Center* [online] [last viewed 04.09.2026]. Available from: https://irregularwarfarecenter.org/publications/insights/six-key-lessons-from-ukraines-drone-war

3. KATSIMON, Olha, 2026. Former Pentagon chief: Ukraine's military innovation cycle is two weeks. *LIGA.net* [online] [last viewed 15.07.2026]. Available from: https://news.liga.net/en/war/news/former-pentagon-chief-ukraines-military-innovation-cycle-is-two-weeks

4 FORREST, F., 2024. The critical role of C-UAS in the Russia/Ukraine conflict. *ArmyTechnology* [online] [last viewed 04.09.2026]. Available from: https://www.army-technology.com/sponsored/the-critical-role-of-c-uas-in-the-russia-ukraine-conflict

5. LITNAROVYCH, Vlad, 2025. Moscow's Last Resort: Machine Gun GAZelles Deployed to Defend Oil Refineries from Drone Barrage. *UNITED24* [online] [last viewed 2026-07-14]. Available from: https://united24media.com/latest-news/moscows-last-resort-machine-gun-gazelles-deployed-to-defend-oil-refineries-from-drone-barrage-12047

6. PIERCE, L., 2025. What Is Operation Sindoor? Purpose, Forces, and Outcome. *Defence Feeds* [online] [last viewed 04.09.2026]. Available from: https://defensefeeds.com/analysis/conflicts/operation-sindoor

7. MON, S., 2025. The War from the Sky: How Drone Warfare Is Shaping the Conflict in Myanmar. *Left Renewal Blog* [online] [last viewed 04.09.2026]. Available from: https://leftrenewal.org/articles-en/su-mon-war-from-the-sky

8. ThairathOnline, 2025. Revealed: Why Cambodian Drones Intensely Attacked for 5 Days Using High Ground and Fiber Optic Systems, Mirroring Ukraine–Russia Battlefield Tactics. *ThairathOnline* [online] [last viewed 04.09.2026]. Available from: https://en.thairath.co.th/news/local/2901381; ENCARNACION, E. M., 2025. Thailand Unleashes Own 'Shahed' Kamikaze Drone in Border War With Cambodia. *The Defense Post* [online] [last viewed 04.09.2026]. Available from: https://thedefensepost.com/2025/12/18/thailand-shahed-kamikaze-drone

9. NATE, A., 2025. Military Drone Proliferation Marks Destabilizing Shift in Africa's Armed Conflicts. *Africa Center for Strategic Studies* [online] [last viewed 04.09.2026]. Available from: https://africacenter.org/spotlight/drone-proliferation-africa-destabilizing

10. ZIEMER, H., 2025. The Future of Criminal Drone Use in Latin America. *War on the Rocks* [online] [last viewed 04.09.2026]. Available from: https://warontherocks.com/the-future-of-criminal-drone-use-in-latin-america

11. KOZATSKYI, Sania, 2026. Tryzub Laser Integrated into a Trailer-Mounted Anti-Drone System. *Militarnyi* [online] [last viewed 04.09.2026]. Available from: https://militarnyi.com/en/news/tryzub-laser-trailer-anti-drone-system

12. PRYHODKO, Roman, 2026. The Atlantic: Ukraine Develops Sunray Laser Air Defense System. *Militarnyi* [online] [last viewed 04.09.2026]. Available from: https://militarnyi.com/en/news/the-atlantic-ukraine-develops-sunray-laser

13. ROSENKRANZ, Martin, 2026. Russia Tests the "Perun" Anti-Drone Laser. *Militär Aktuell* [online] [last viewed 04.09.2026]. Available from: https://militaeraktuell.at/en/russia-tests-the-perun-anti-drone-laser

14. ШЕВЦЕВ, Никита, 2023. Лазерный комплекс «Задира»: передовое российское оружие для уничтожения беспилотников. *Techinsider* [online] [last viewed 04.09.2026]. Available from: https://www.techinsider.ru/weapon/1545053-

lazernyy-kompleks-zadira-kak-peredovoe-rossiyskoe-oruzhie-unichtozhaet-celi-v-ukraine

15. Office of Naval Research, N/A. Directed Energy Weapons: High Power Microwaves (HPM). *Office of Naval Research* [online] [last viewed 04.09.2026]. Available from: https://www.onr.navy.mil/organization/departments/code-35/division-353/directed-energy-weapons-high-power-microwaves; SINHA, Sujita, 2026. China reveals 100-gigawatt microwave weapon that could fry US satellites in orbit. *InterestingEngineering* [online] [last viewed 04.09.2026]. Available from: https://interestingengineering.com/military/china-100-gigawatt-microwave-weapon

ЛИТЕРАТУРА

BILL, J.A., 1989. *The Eagle and the Lion: The Tragedy of American-Iranian Relations.* Yale Univestity Press, ISBN 9780300044126.

BLOEMBERGEN, N.; PATEL, C. K. N. et al., 1987. Report to the american physical society of the study group on science and technology of directed energy weapons. *Reviews of Modern Physics* [online], vol. 59, no 3. Available from: https://doi.org/10.1103%2frevmodphys.59.S1.

BOYLE, M.J., 2020. *The Drone Age: How Drone Technology Will Change War And Peace.* Oxford University Press. ISBN 9780190635862.

LIN-GREENBERG, E., 2025. *The Remote Revolution: Drones and Modern Statecraft*. Cornell University Press, ISBN 9781501783852.

POKORNY, L., 2026. Cost-Effectiveness Analysis of Counter-Unmanned Aircraft Systems Technologies: A Comparative Study of Kinetic, Electronic Warfare, and Directed Energy Countermeasures (2022-2026). New Jersey, USA: ICL Institute. *Zenodo* [online]. Available from: https://doi.org/10.5281/zenodo.18928365.

SUBRAMANIAM, S.; LYNCH, A.C., 2025. Curiosity Driven Counter UAS Solution. In: *2025 ASEE -GSW Annual Conference*. Texas: Arlington, TX. DOI: 10.18260/1-2–55039.

VANHORN, KYLE, T., 2026. Experimental Characterization of a Quadrotor's Response to an Air Vortex Cannon. In: *AIAA SCITECH 2026 Forum 12-16 January 2026.* Available from: 10.2514/6.2026-1282.

SYSTEMS APPROACH TO C-UAS OPERATIONS

Abstract. The proliferation of low-cost unmanned aerial systems (UAS) has fundamentally changed the nature of modern conflict and created an unprecedented "cost and power asymmetry" in air defense. This article examines the global landscape of counter-UAS (C-UAS) through a systems lens, analyzing operational experience from Ukraine, the Middle East, and other conflict zones to identify patterns, failures, and emerging solutions. Based on quantitative cost-effectiveness analysis and

recent operational data, we argue that an effective C-UAS strategy requires a multi-layered, knowledge-based approach that integrates advanced directed energy systems with proven practical measures. The article evaluates both exotic technical solutions, including laser systems, electromagnetic and vortex weapons, and pragmatic approaches such as mobile drone interception fire teams. In conclusion, no single technology offers a panacea. Success requires a system architecture that balances cost, scalability, and operational adaptability.

Keywords: anti-drone protection; C-UAS operations; directed anergy weapons; efficiency analysis; electronic warfare; systems engineering

Dr. Lyubosvet Stoev, Assoc. Prof.
SCOPUS ID: 58191524400
WoS ID: AAQ-1350-2020
ORCID iD: 0000-0002-2014-4402
Defense Advanced Research Institute
Rakovski National Defense College
82, Evlogi and Khristo Georgievi Blvd.
1504 Sofia, Bulgaria
E-mail: l.stoev@rndc.bg

Colonel Dr. Zhivo Petrov, Assoc. Prof.
SCOPUS ID: 57204311383
WoS: H-1227-2016
ORCID iD: 0000-0003-2757-0030
Defense Advanced Research Institute
Rakovski National Defense College
82, Evlogi and Khristo Georgievi Blvd.
1504 Sofia, Bulgaria
E-mail: zh.petrov@rndc.bg

https://doi.org/10. 66334/annu26_screenriskstate

СКРИНИНГ НА РИСКОВИТЕ ПРОФИЛИ НА ДЪРЖАВНАТА ГРАНИЦА НА РЕПУБЛИКА БЪЛГАРИЯ КАТО ИНСТРУМЕНТ ЗА ПРЕВЕНЦИЯ НА ЗАПЛАХИ ЗА НАЦИОНАЛНАТА СИГУРНОСТ

Мохамед Насри, докторант
Академия на Министерство на вътрешните работи

Абстракт. Докладът разглежда скрининга на рискови профили на държавната граница като структурирана експертна дейност за ранно разпознаване на основания за допълнителна проверка и насочване към компетентна процедура. Изследването отчита пълното участие на България в Шенген и прилагането от 12 юни 2026 г. на Регламент (ЕС) 2024/1356. Чрез нормативен анализ и функционално моделиране е предложен пететапен процес, който разделя установяването на факти, оценката на несигурността, уязвимостта, сигурностните индикации и институционалното решение. Научноприложният резултат е модел за документирана и проверима преценка, който не допуска извод за опасност единствено от неспецифичен признак. Моделът съчетава ранната превенция с човешки контрол, пропорционалност, защита на данните и право на корекция. SIRS (Security Incident Reporting System) е посочена единствено като авторски прототип за техническо

подпомагане на този процес, без да се разглежда вътрешната ѝ архитектура.

Ключови думи: граничен скрининг; рисков профил; национална сигурност; външна граница; професионална преценка; Security Incident Reporting System

I. Увод

От 1 януари 2025 г. Република България участва изцяло в Шенгенското пространство. Премахването на проверките по вътрешните сухопътни граници увеличава значението на надеждния контрол по външната граница[1]. Той трябва да защитава сигурността при спазване на международната закрила, забраната за връщане и основните права.

От 12 юни 2026 г. Регламент (ЕС) 2024/1356 въвежда общи правила за скрининг на определени граждани на трети държави. Той обхваща проверка на здравето и уязвимостта, самоличността, биометричните данни и сигурността, последвана от формуляр и насочване към подходяща процедура[2]. Така несвързаните проверки се превръщат в проследим процес.

Практическият проблем възниква там, където служителят трябва за ограничено време да различи факт от твърдение, неизвестност от противоречие и уязвимост от сигурностна индикация. При смесени потоци едно наблюдение може да има различно значение според здравето, преживяното насилие, маршрута, превода и документите. Неструктурираното впечатление крие риск и от пропусната заплаха, и от неоправдано третиране на уязвимо лице като заплаха.

Целта на доклада е да предложи приложим модел за скрининг на индивидуалния рисков профил на държавната граница, който подпомага ранното разпознаване и институционалното насочване, без да замества компетентния орган. Използвани са нормативен анализ, анализ на официални документи и функционално моделиране. Докладът е теоретико-приложен; предложените критерии са за пилотно изпитване, а не доказателство за прогностична точност.

Обект на изследването е организацията на граничния скрининг, а предмет – връзката между качеството на информацията, експертната преценка и институционалното насочване. Изследователският въпрос е при какви условия стандартизирането на аналитичния запис може да направи решението по-проверимо, без да превърне несигурността в презумпция за опасност. Работната теза е, че подобрение може да се търси чрез проследи-

мост на основанията и разграничаване на процедурите. Тази теза подлежи на последващо изпитване.

Методологичният подход включва извеждане на процедурни изисквания от официалните източници, съпоставянето им с потребностите на индивидуалния случай и формулиране на критерии за проверка на модела. Нормативните задължения са разграничени от авторските предложения. Анализът не използва класифицирани данни, не представя реални оперативни случаи и не измерва вероятност конкретно лице да извърши престъпление.

II. Теоретична и нормативна основа

2.1. Рискът като основание за управленско решение

В монографията си за анализа и оценката на риска в контрола на държавната граница Фердов разглежда връзката между опасност, заплаха, риск и система (Ferdov 2012). В настоящия модел тази теоретична отправна точка се използва за обвързване на оценката с конкретно управленско решение. Скринингът следва да установи дали наличната информация обосновава проверка, защитна мярка или насочване, вместо да приписва трайна характеристика на лицето.

В настоящия доклад индивидуалният рисков профил се определя като временно, структурирано и проверимо описание на факти, неизвестности, защитни фактори и източници за конкретно решение. Той не е присъда за бъдещо поведение, актуализира се при нови данни и посочва границите на увереността. Националност, етнос, религия, пол или самият факт на миграция не са самостоятелни основания за риск.

Понятието уязвимост има две различни приложения. Уязвимостта на граничната система се отнася до слабости в организацията, ресурсите или обмена на информация. Уязвимостта на човека означава потребност от подкрепа и специални гаранции. Смесването им би довело до погрешен извод, че лицето, което се нуждае от защита, представлява заплаха за системата. В предложения модел двете значения се описват отделно и водят до различни действия.

2.2. Разграничаване на стратегическия риск и индивидуалния скрининг

Общият интегриран модел за анализ на риска на Frontex разглежда риска чрез взаимодействието между заплаха, уязвимост и въздействие[3, 4]. При стратегическото му използване се анализират обстановката, марш-

рутите и капацитетът на системата. Индивидуалният скрининг свързва случая с тази обстановка, без автоматично да пренася риска на район или група върху отделното лице.

Това разграничение е съществено. Повишеният натиск по даден маршрут може да обоснове повече ресурси, проверки или готовност, но не доказва намерение на конкретен човек. Индивидуален извод изисква относимо поведение, проверима информация и законова цел. Така стратегическата осведоменост подпомага проверката, без да се превръща в групово подозрение.

2.3. Новата европейска рамка за скрининг

Регламент (ЕС) 2024/1356 се прилага към определени категории граждани на трети държави, включително лица, установени във връзка с неразрешено преминаване на външна граница, лица, свалени на брега след операции по търсене и спасяване, и лица, поискали международна закрила на граничен пункт, без да изпълняват условията за влизане. Поради това нормативният скрининг не бива да се смесва с обикновената гранична проверка на всеки пътник. Първата стъпка на всеки приложен модел трябва да бъде определяне на правното основание и приложимата процедура.

Европейската рамка изисква скринингът по външната граница да приключи без забавяне и по правило до седем дни. Резултатът се отразява във формуляр, който разграничава потвърдената от органите информация от заявеното от лицето и трябва да позволява административен и съдебен преглед. Преди предаването на формуляра лицето има възможност да посочи неточности[5]. Тези изисквания показват, че проследимостта не е техническо удобство, а процедурна гаранция.

Скринингът завършва с насочване към компетентната процедура: регистрация и разглеждане на молба за международна закрила, производство по връщане, механизъм за преместване или друга процедура, когато са налице съответните законови предпоставки[6]. Самият скрининг не решава основателността на молбата за закрила, не установява наказателна отговорност и не създава правомощия извън закона. Практическата му стойност е в ранното насочване и в качеството на предадената информация.

2.4. Българската външна граница като обща граница на Шенген

Главна дирекция „Гранична полиция“ е националната специализирана структура на МВР за граничен контрол и охрана на държавната граница[7]. След пълното присъединяване към Шенген качеството на проверките

по външната граница се свързва пряко с взаимното доверие между държавите членки. Измененият Кодекс на шенгенските граници подчертава общата отговорност и координираното действие при заплахи за обществения ред и вътрешната сигурност[8, 9].

За България това предполага съвместимост между тактическата работа на първа линия, оперативния анализ и стратегическата оценка в рамката на европейското интегрирано управление на границите[10]. Информацията се предава по компетентност, в необходимия обем и с посочен източник. Прекалено общата оценка предава предположения, а прекалено тясната може да пропусне уязвимост, трафик на хора, документна измама или сигурностна индикация.

III. Авторски модел за скрининг на рискови профили

3.1. Принципи на модела

Предложеният модел подрежда скрининга около решението, което законът допуска, а не около стремежа да се събере максимална информация. Той използва шест принципа: законова цел и компетентност; индивидуална оценка; разграничаване на факт, твърдение и аналитичен извод; проверка чрез повече от един източник; човешка преценка с мотиви; възможност за корекция и последващ контрол. Принципите се прилагат едновременно.

Основно правило е забраната един признак да решава случая. Липсата на документ може да е свързана със загуба, принуда или прикриване на самоличност, а непоследователността – от превод, травма или невярно твърдение. Скринингът записва конкуриращите се обяснения и начина за проверката им. Изводът се основава на относимостта и надеждността на данните, а не на механично натрупване на признаци.

Изискването за проверка чрез повече от един източник е стандарт за надеждност, а не абсолютна предпоставка за всяко действие. Един достоверен факт може да е достатъчен за предвидена в закона незабавна защитна мярка или конкретна проверка. Следва да се различава такъв факт от неспецифичен признак – като притеснение, езиково затруднение или необичаен външен вид. Мотивировката посочва защо избраното действие е необходимо и съразмерно именно при наличните данни.

3.2. Пет етапа на граничния скрининг

Първият етап е правното и фактическото очертаване на случая. Установява се къде и при какви обстоятелства лицето е срещнало граничния

орган, приложим ли е нормативният скрининг, заявено ли е намерение за международна закрила и има ли непосредствена медицинска или защитна необходимост. Този етап предотвратява пренасянето на сигурностната логика върху въпроси, които законът възлага на друга процедура.

Вторият етап е установяване или проверка на самоличността и оценка на качеството на данните. За всяко обстоятелство се отбелязва дали е потвърдено чрез документ или регистър, заявено е от лицето, получено е от друг орган или остава непроверено. Отделно се записват техническите и човешките ограничения: нечетлив документ, липса на достъп до информационна система, проблем с превода или непълнота на интервюто. Така неизвестното не се представя като отрицателен факт.

Третият етап е контекстуална проверка на маршрута и времето. Данните за държава на произход, места на пребиваване, транзит и цел се съпоставят с актуална и датирана информация. Контекстът насочва въпросите, но не определя самостоятелно индивидуалния риск. Пребиваването в конфликтна зона може да означава принуда, разселване или защитна потребност и се тълкува конкретно.

Четвъртият етап е структурирана експертна оценка. Аналитикът разглежда съвместно пет области: надеждност на идентификационната информация; последователност на маршрута и хронологията; конкретни индикации, относими към вътрешната сигурност; уязвимости и защитни фактори; необходимост от действие на друг компетентен орган. За всяка област се посочват подкрепящите данни, противоречащите данни, алтернативните обяснения и степента на несигурност. Не се използва автоматичен сбор, който да замени аргументацията.

Петият етап е документиран резултат и насочване. Възможните процесуални изходи са: продължаване по обичайния ред; допълнителна проверка; медицинска или друга защита; международна закрила; връщане при законовите предпоставки; или уведомяване на компетентна служба при документирани основания. Един случай може да изисква едновременно защита и сигурностна проверка: уязвимостта не изключва риска, а рискът не отменя защитата.

Етапите представляват аналитична последователност, а не задължителен график, който отлага неотложната помощ. Медицинското насочване и гаранциите за дете могат да започнат още при първия контакт; проверката на самоличността може да продължи успоредно. Когато информацията не достига, резултатът е конкретно формулирана задача за проверка, с отговорник и срок по приложимата процедура, а не произволно завишена степен на риск.

3.3. Минимален стандарт за аналитичния запис

За да бъде резултатът проверим, аналитичният запис трябва да съдържа: предмет и правно основание на скрининга; дата и място; потвърдени и заявени данни; източници и актуалност; уязвимости и сигурностни индикации; алтернативни обяснения и липси; мотиви за насочването; отговорен служител; и възможност за корекция. Съдържанието следва чл. 17 от Регламент (ЕС) 2024/1356 и го доразвива за професионалната оценка.

Статусът на информацията трябва да бъде видим. Формулировките „установено“, „заявено“, „потвърдено от втори източник“, „противоречиво“ и „непроверено“ имат различно значение. Без това разграничение предположението лесно се предава като факт. Затова всяко съществено заключение се свързва с източник и конкретна законова цел.

Препредаването на една и съща първична информация от няколко звена не я превръща в независимо потвърдена. Записът следва да позволява установяване на първоизточника и на извършените проверки. При корекция се запазват предишната версия, основанието за промяната и авторът ѝ; актуалният извод се обозначава ясно. Това позволява последващият орган да установи дали оценката е променена поради нов факт, отстранена грешка или различно професионално тълкуване.

3.4. Ограничено технологично подпомагане чрез SIRS

SIRS (Security Incident Reporting System) е авторска разработка, която може да служи като технически прототип за прилагане на описания процес. В рамките на настоящия доклад значението ѝ е ограничено до четири функции: подреждане на информацията по случая; ясно отбелязване на нейния източник и статус; подпомагане на съпоставката между наличните данни; и изготвяне на проследим проект на аналитичен запис за преглед от компетентен служител. Технологичният инструмент не определя приложимата процедура, не установява вина и не взема крайно решение.

Това ограничение е съзнателно. Надеждността на граничния скрининг зависи преди всичко от правната основа, данните, подготовката и контрола. Софтуерът може да подобри проследимостта, но не компенсира неправилна цел или критерий. Реалната употреба изисква независимо изпитване, оценка за основните права и данните, правна проверка и контролиран пилот.

3.5. Илюстративен случай и институционална приемственост

В условен учебен сценарий лице без документ заявява намерение да потърси закрила, а при първоначалния превод посочва различни дати на

едно пътуване. Това не е емпиричен резултат, а пример за проверка на логиката. Записват се липсата на документ, съдържанието на заявлението и конкретното разминаване. Проверява се дали датите означават напускане на населеното място или преминаване на границата. При нужда се осигурява подходящ превод. До изясняването разминаването остава непроверено обстоятелство, без автоматичен извод за прикриване.

Ако след уточняването противоречието отпадне, аналитичният запис се коригира. Ако остане, се определя каква законна проверка може да го изясни. Заявената потребност от международна закрила се обработва по компетентност независимо от наличието на неяснота. При отделен проверен факт, относим към сигурността, се документира и съответното уведомяване. Така моделът допуска паралелни действия, но изисква различни основания за всяко от тях.

Предаването на случая трябва да съдържа конкретен въпрос към получаващия орган и разграничение между извършеното и предстоящото. Не е достатъчно обозначение „рисково лице“. Необходими са основанието за уведомяването, проверените източници, оставащата неяснота и спешността. Получаването и последващото действие се проследяват в рамките на допустимия обмен. Предложеният процес не определя нови правомощия на институциите и не замества националните правила за взаимодействие.

IV. Резултати и условия за прилагане

4.1. Научноприложни резултати

Първият резултат е ясно разграничение между три равнища: стратегически анализ на риска по границата, индивидуален скрининг и правно решение. Така общата оценка за маршрут не става автоматичен извод за лицето, а определя ресурсите и въпросите за проверка.

Вторият резултат е пететапен процес, който започва с правното основание и завършва с мотивирано насочване. Той добавя към европейските елементи изрична оценка на качеството, алтернативите и несигурността, за да не се превръщат непълните данни в привидно доказателство.

Третият резултат е минимален стандарт за аналитичен запис. Той създава основа за институционална приемственост и контрол. Източниците, ограниченията и мотивите позволяват на следващия орган да продължи проверката, без да приема предположението за факт.

Четвъртият резултат е рамка за измерване на бъдещ пилот. Ефективността не трябва да се оценява само по броя на сигналите. Показате-

ли са: пълнота, време до правилно насочване, съгласие между оценители, корекции, проследими източници, необосновани сигнали и нарушения на минимизирането на данни. Съвкупната им оценка показва дали моделът подобрява работата безопасно.

4.2. Правни и етични гаранции

Регламент (ЕС) 2024/1356 задължава държавите членки да осигурят независимо наблюдение на спазването на основните права и механизъм за твърдения за нарушения[11]. Моделът изисква контрол на достъпа, журнал, срокове за съхранение, разграничени роли и минимизиране на данните. Приложимият режим за личните данни се определя според дейността и целта. Принадлежността на структурата към МВР сама по себе си не е достатъчна. Разграничават се приложното поле на Общия регламент относно защитата на данните и обработването от компетентни органи за целите по Директива (ЕС) 2016/680[12, 13].

Специално внимание изискват децата, жертвите на трафик, лицата с медицински потребности, преживелите насилие и лицата, които не разбират процедурата. Необходими са обучен персонал, участие на органите за закрила и ясна информация за достъпа до международна закрила[14].

Човешкият контрол трябва да бъде съдържателен. Служителят следва да може да оспори предложена съпоставка, да добави контекст и да мотивира извода. Отговорността не се прехвърля на система. При неблагоприятно действие трябва да са установими данните, проверилият ги служител и правната процедура.

4.3. Ограничения и програма за проверка

Предложеният модел е концептуален. Той не е изследван върху представителна извадка от реални гранични случаи и няма установена прогностична точност. Не се предлагат числови прагове за опасност на лице. Ако при последващо изследване се обсъждат количествени показатели, те изискват отделна обосновка на допустимостта, измеримия резултат и начина на валидиране. Контекстуалната информация изисква дата, версия и оценка на надеждността.

Пилотното изпитване следва да започне със синтетични учебни сценарии. Двама или повече оценители прилагат модела независимо, а различията се анализират. Следваща фаза може да бъде ограничено паралелно използване без самостоятелно правно действие, при изпълнени правни и организационни предпоставки. Проверяват се проследимостта, междуоценъчното съгласие и евентуалните необосновани различия в третирането.

За първата фаза се предлага предварително описан набор от учебни случаи с различна пълнота на данните и различни потребности от защита. Всеки случай има независимо изготвен референтен анализ с допустими варианти на действие. Оценителите работят първо по обичайния подход, а след обучение – със структурирания запис; използват се съпоставими, но различни сценарии, за да се ограничи ефектът от запомняне. Редът се разпределя между участниците, а референтният анализ се съобщава след приключване на оценяването.

За всеки сценарий се измерват делът на съществените изводи с проследим източник, делът на правилно обозначените неизвестности и времето до обосновано насочване. Междуоценъчното съгласие се отчита отделно от съответствието с референтния анализ: еднаквото решение може да бъде еднакво погрешно. Документират се пропуснатите защитни потребности и необоснованите сигурностни насочвания. Показателите се представят с ясно определен знаменател, а не като изолирани проценти.

Преминаването към ограничен пилот изисква предварително определени критерии за приемане и прекратяване, разрешено използване на данните и независим преглед. Нарушен достъп, системно неправилно насочване или невъзможност за възстановяване на мотивите са основания да се спре изпитването и да се отстрани причината. Положителният резултат върху учебни сценарии доказва най-много приложимост в тези условия; той не установява ефективност в реалния миграционен поток и не оправдава автоматично внедряване.

V. Заключение

Скринингът на рискови профили на държавната граница може да подпомогне превенцията на заплахи за националната сигурност, когато е свързан с конкретна законова цел и завършва с мотивирано действие на компетентен орган. Неговата надеждност не произтича от количеството събрани данни, а от ясното разграничение между потвърден факт, заявено обстоятелство, неизвестност и аналитичен извод.

Предложеният пететапен модел превежда европейските изисквания към логика, приложима в българската гранична среда: определя процедурата, проверява самоличността и качеството на информацията, поставя маршрута в контекст, оценява индикациите и уязвимостите и завършва с документирано насочване. Приносът е свързването на стратегическия риск с индивидуалната преценка, без презумпция срещу лицето.

SIRS може да подпомогне тази организация като авторски технологичен прототип, но легитимността на резултата остава в закона и човешката отговорност. Внедряването изисква пилотно изследване, независима методологична и правна оценка и постоянен контрол за основните права.

Благодарности. Авторът изказва благодарност на научния си ръководител проф. д-р Ставри Фердов за научното ръководство и методологичните насоки.

NOTES

1. COUNCIL OF THE EUROPEAN UNION, 2024. *Schengen: Council decides to lift land border controls with Bulgaria and Romania*. 12 December 2024. [online]. Available from: https://www.consilium.europa.eu/en/press/press-releases/2024/12/12/schengen-council-decides-to-lift-land-border-controls-with-bulgaria-and-romania/. [Last viewed: 15 September 2026].

2. EUROPEAN PARLIAMENT AND COUNCIL, 2024. Regulation (EU) 2024/1356 introducing the screening of third-country nationals at the external borders , art. 8. *Official Journal of the European Union,* L, 2024/1356, 22 May 2024. [online]. Available from: https://eur-lex.europa.eu/eli/reg/2024/1356/oj.

3. FRONTEX, 2021. *Common Integrated Risk Analysis Model 2.1*., 18 November 2021. [online]. Available from: https://prd.frontex.europa.eu/document/common-integrated-risk-analysis-model-2-1/. [Last viewed: 15 September 2026].

4. FRONTEX, n.d. *Strategic risk analysis*. [online]. Available from: https://www.frontex.europa.eu/what-we-do/monitoring-and-risk-analysis/risk-analysis/strategic-risk-analysis/. [Last viewed: 15 September 2026].

5. EUROPEAN PARLIAMENT AND COUNCIL, 2024. Regulation (EU) 2024/1356 introducing the screening of third-country nationals at the external borders, arts. 8, 17. *Official Journal of the European Union,* L, 2024/1356, 22 May 2024. [online]. Available from: https://eur-lex.europa.eu/eli/reg/2024/1356/oj.

6. EUROPEAN PARLIAMENT AND COUNCIL, 2024. Regulation (EU) 2024/1356 introducing the screening of third-country nationals at the external borders , art. 18. Official *Journal of the European Union,* L, 2024/1356, 22 May 2024. [online]. Available from: https://eur-lex.europa.eu/eli/reg/2024/1356/oj.

7. MINISTRY OF INTERIOR OF THE REPUBLIC OF BULGARIA, n.d. *Directorate General Border Police*. [online]. Available from: https://mvr.bg/gdgp/. [Last viewed: 15 September 2026].

8. EUROPEAN PARLIAMENT AND COUNCIL, 2016. Regulation (EU) 2016/399 (Schengen Borders Code). *Official Journal of the European Union*, L 77, 23 March 2016, pp. 1 – 52. [online]. Available from: https://eur-lex.europa.eu/eli/reg/2016/399/oj.

9. EUROPEAN PARLIAMENT AND COUNCIL, 2024. Regulation (EU) 2024/1717 amending Regulation (EU) 2016/399. *Official Journal of the European Union,* L, 2024/1717, 20 June 2024. [online]. Available from: https://eur-lex.europa.eu/eli/reg/2024/1717/oj.

10. EUROPEAN PARLIAMENT AND COUNCIL, 2019. Regulation (EU) 2019/1896 on the European Border and Coast Guard. *Official Journal of the European Union,* L 295, 14 November 2019, pp. 1 – 131. [online]. Available from: https://eur-lex.europa.eu/eli/reg/2019/1896/oj.

11. EUROPEAN PARLIAMENT AND COUNCIL, 2024. Regulation (EU) 2024/1356 introducing the screening of third-country nationals at the external borders , art. 10. *Official Journal of the European Union,* L, 2024/1356, 22 May 2024. [online]. Available from: https://eur-lex.europa.eu/eli/reg/2024/1356/oj.

12. EUROPEAN PARLIAMENT AND COUNCIL, 2016. Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 4 May 2016, pp. 1 – 88. [online]. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

13. EUROPEAN PARLIAMENT AND COUNCIL, 2016. Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities. *Official Journal of the European Union,* L 119, 4 May 2016, pp. 89 – 131. [online]. Available from: https://eur-lex.europa.eu/eli/dir/2016/680/oj.

14. EUAA, 2026. *Practical Guide on Access to the Asylum Procedure*. Third edition. February 2026. [online]. Available from: https://www.euaa.europa.eu/publications/practical-guide-access-to-asylum-procedure. [Last viewed: 15 September 2026].

REFERENCES

FERDOV, S., 2012. *Analiz i otsenka na riska v kontrola na darzhavnata granitsa na Republika Bulgaria*. Sofia: Akademia na MVR. [in Bulgarian].

SCREENING OF RISK PROFILES AT THE STATE BORDER OF THE REPUBLIC OF BULGARIA AS AN INSTRUMENT FOR PREVENTING THREATS TO NATIONAL SECURITY

Abstract. The paper examines risk-profile screening at the state border as a structured professional activity for the early identification of grounds for further verification and referral to the competent procedure. It considers Bulgaria‘s full participation in the Schengen area and the application of Regulation (EU) 2024/1356 from 12 June 2026. Based on legal analysis and functional modelling, the paper proposes a five-stage process separating fact establishment, uncertainty assessment, vulnerability, security indications and institutional decision-making. The applied contribution is a model for documented and reviewable professional judgement which does not infer dangerousness from a nonspecific indicator alone. The model combines early prevention with meaningful human control, proportionality, data protection and a

right to correction. SIRS (Security Incident Reporting System) is mentioned solely as the author‘s prototype for technical support of this process; its internal architecture is outside the scope of the paper.

Keywords: border screening; risk profile; national security; external border; professional judgement; Security Incident Reporting System

Mohamed Nasri, PhD Student
Department of Border Control and Public Order
Academy of the Ministry of Interior
1, Alexander Malinov Blvd.
1712 Sofia, Bulgaria
E-mail: box_nasri@abv.bg

https://doi.org/10. 66334/annu26_peristratrole

ПЕРИФЕРИЯ ИЛИ СТРАТЕГИЧЕСКИ КРЪСТОПЪТ: ПРОМЕНЯ ЛИ СЕ РОЛЯТА НА ЮГОИЗТОЧНА ЕВРОПА В ЕВРОПЕЙСКАТА СИГУРНОСТ

гл. ас. д-р Невена Алексиева
Военна академия „Георги Стойков Раковски“

Абстракт. Югоизточна Европа (ЮИЕ) традиционно е възприемана като периферна зона по отношение на развиващите се в Европа процеси. Променящата се геополитическа среда и нарастващото стратегическо значение на Черноморския регион извеждат на преден план необходимостта от преосмисляне на ролята на региона за гарантиране на европейската сигурност. Той е разгледан като пространство на взаимодействие и конкуренция между различни геополитически интереси, както и от гледна точка на важността му за свързаността, регионалната устойчивост и стабилността на Европа. Основната теза е, че Югоизточна Европа постепенно се превръща от периферия в стратегически кръстопът с нарастваща стойност за европейската и евроатлантическата сигурност.

Ключови думи: Европейски съюз; сигурност; трансформация; Югоизточна Европа

Повече от три десетилетия след края на Студената война регионът на Югоизточна Европа е изправен пред редица предизвикателства за сигурността, неравномерно протичане на реформите и наличие на нерешени исторически въпроси. ЮИЕ е смятан по-скоро за консуматор на външни активности, а не толкова за инициатор на автентични регионални политики и позиции. Стратегическото ѝ разположение до голяма степен предопределя интереса на различни ключови актьори с различен тип очаквания, амбиции и подходи към регионалните проблеми, особено в сферата на сигурността и енергетиката.

Статията има за цел да изследва дали и доколко се променя ролята на Югоизточна Европа в европейската сигурност. За постигане на целта са поставени следните изследователски задачи:

• Оценка на ролята и мястото на Югоизточна Европа в съвременната европейска архитектура за сигурност.

• Анализ на факторите за потенциална промяна на значението на региона.

• Оценка на степента, в която Югоизточна Европа се превръща от периферно пространство в стратегически кръстопът за европейската и евроатлантическата сигурност.

Дълго време се налага схващането, че ЮИЕ е един от най-проблемните от гледна точка на европейската сигурност региони, ситуиран в нейната политическа периферия. Това извежда на преден план въпроса дали в контекста на актуалната геополитическа ситуация ще продължава да се следва традиционния модел на възприятие за региона като уязвима зона, или динамиката в съседните региони налага преоценка на неговите роля, потенциал и възможности.

Методологичното ядро на изследването е ориентирано основно към анализ на ролята на ЮИЕ като потенциален стратегически кръстопът за европейската и евроатлантическата сигурност, разгледан посредством четири основни вектора. Първият е географският вектор, свързан с възможностите, които географското положение предоставя – като пресечна точка между Европа, Черноморския регион, Източното Средиземноморие и Кавказ. На второ място, военно-стратегически вектор – позицията ѝ на Югоизточния фланг на НАТО[1], ролята на Западните Балкани[2] и на Черно море. Третият вектор е геополитическият, който произтича от пресичането на интересите на ЕС, НАТО, САЩ, Русия, Китай, Турция и регионалните държави. Последният е свързан с инфраструктурата и регионалната свързаност – развитието на транспортни, енергийни и комуникационни мрежи,

военната мобилност и инфраструктурата с двойно предназначение, които във все по-голяма степен се превръщат във водещ фактор за гарантиране устойчивостта на европейската система за сигурност.

В доклада са използвани сравнителен метод, синтез, преглед на научни публикации на български и чуждестранни автори, сред които проф. Динко Динков, Димитър Бечев, Любомир Кючуков, Флориан Бибер, Найъл Мълчинок и др., както и на стратегически документи на ЕС и НАТО.

Югоизточна Европа: от периферия към стратегически кръстопът

При анализа следва да се отчитат няколко основни момента, свързани с вътрешната диференциация и специфика на региона. На първо място, обхватът на страните от ЮИЕ продължава да поражда дискусии сред експертите. В настоящата разработка ще се има предвид широкото понятие за ЮИЕ като динамичен конструкт, който се развива в съответствие с политико-икономическите условия на средата. В този смисъл в него се включват Албания, Босна и Херцеговина, България, Гърция, Кипър, Косово, Молдова, Румъния, Северна Македония, Словения, Сърбия, Турция, Хърватия, Черна гора.

На следващо място, не бива да се пропуска фактът, че ЮИЕ е неформално вътрешно разделена на държави членки на ЕС и страни от Западните Балкани, които се намират в различен етап на европейска интеграция[3], което в редица аспекти затруднява постигането на общ регионален консенсус.

Руската агресия в Украйна от февруари 2022 г. изведе на преден план до голяма степен необходимостта от преосмисляне на значимостта на широкия регион ЮИЕ и на отделни подрегиони или групи държави в контекста на европейската и евроатлантическата система за сигурност. В този контекст ролята на Югоизточна Европа следва да се разглежда в по-широката рамка на европейската сигурност, в която ЕС и НАТО изпълняват взаимно допълващи се функции по отношение на отбраната, сигурността и устойчивостта на региона.

Тази динамика допринася за възприемането на Югоизточна Европа като регион с повишена дългосрочна уязвимост, който изисква трайно съюзническо присъствие и по-тясна координация. В този контекст сухопътните и речните транспортни коридори се очертават като съществен компонент на регионалната сигурност, осигурявайки допълнителни възможности за военна мобилност, снабдяване и укрепване на критичната инфраструктура. Недостатъчната им интеграция в по-широкото отбрани-

телно планиране обаче ограничава потенциала им като елемент на регионалната устойчивост. Това подчертава важността от по-интегриран подход към сигурността на ЮИЕ, при който взаимодействието между инфраструктурата, енергийните мрежи и военната мобилност се разглежда като основен за засилване на сигурността по източния и югоизточния фланг на НАТО и за стабилността на европейския континент.

Западните Балкани: поле на уязвимост или допълнителна възможност

Югоизточна Европа придобива нарастваща стойност, но тази трансформация не протича равномерно във всички нейни части. Особено показателен в това отношение е субрегионът на Западните Балкани, който съчетава две на пръв поглед противоположни характеристики. От една страна, географското положение и непосредствената близост до държавите членки на ЕС и НАТО увеличават значимостта му за европейската сигурност, свързаност и военна мобилност. От друга страна, държавите от региона продължават да бъдат пространство на политическа фрагментация, нерешени двустранни и вътрешнополитически въпроси, институционални слабости и ограничена регионална интеграция.

Икономическите уязвимости са характерни за всички страни макар и с нееднакъв интензитет. Те са свързани със сравнително ограничен икономически потенциал и инвестиционна привлекателност, както и с инфраструктурна изостаналост.

Съществена слабост остава състоянието на демократичния процес. Макар и с различни специфики за отделните страни, върховенството на правото продължава да е проблематично в региона. В различна степен шестте държави от Западните Балкани изпитват проблеми с прилагане на принципите на правовата държава, опазване на основните права и свободи, корупция по високите етажи на властта, организирана престъпност и независимостта на медиите. [4]

Несъмнено проблемите в ЮИЕ имат и съществени исторически измерения, свързани с наследството от разпадането на Югославия, несъвпадението между държавни граници и етнически пространства и въпросите, свързани с националната идентичност и малцинствата. Военните конфликти от 90-те години оставят дългосрочни политически и институционални последици, които продължават да влияят върху регионалната сигурност.

Нерешените въпроси, свързани с териториални и гранични претенции, защитата на правата на малцинствата, възраждането на исторически и нововъзникващ национализъм и редица двустранни претенции продължават да стимулират политическата фрагментация и да ограничават възможностите за изграждане на общи регионални позиции.

Забавената европейска перспектива в определени периоди допринася за обезсърчаване на обществата и елитите на съответните държави. Това води до подхода на търсене на индивидуални решения, както и до излизане на преден план на различни формати – от инициативи за регионално сътрудничество като Берлински процес и Отворени Балкани, до политически концепции, свързани с идеите за „сръбски свят“[5] или „Велика Албания“[6].

Тези характеристики обаче не изчерпват стратегическата роля на Западните Балкани. Те могат да бъдат разгледани по три взаимосвързани направления: като пространство на продължаващи политически уязвимости и слабости в сферата на сигурността; като зона на конкуриращи се външни интереси; като все по-важен елемент от европейската инфраструктурна, транспортна и военно-стратегическа свързаност.

Външни влияния в Югоизточна Европа

До голяма степен Югоизточна Европа се очертава като пространство на взаимодействие между различни външни актьори, които проектират своите интереси чрез политически, икономически, енергийни и културни инструменти в сферата на сигурността.

От една страна, Русия разчита на културно-езиковите и религиозни връзки, както и на енергийната зависимост на отделни части на региона. Историческите отношения продължават да имат значение в политическите нагласи, макар и тяхното влияние да варира значително между отделните държави и обществени групи. Русия запазва значимо влияние в отделни държави, като особено тесни са отношенията ѝ със Сърбия. Важен елемент е и руската позиция в Съвета за сигурност на ООН по въпроса за статута на Косово.

На следващо място е Китай, който превръща икономическото си присъствие в инструмент за политическо влияние и разширява интересите си в сферата на сигурността. Посредством своята стратегическа инициатива „Пояс и път“[7] (в рамките на която се разпростира китайското икономическо, а и политическо влияние към Европа) Китай предлага сериозни инвестиционни, индустриални и търговски компоненти, които да осигурят дъл-

госрочност и стабилност на китайското присъствие. За Китай Западните Балкани са коридор с неоползотворен икономически потенциал и възможност за свързване на европейските и азиатските пазари.

Турция се стреми към утвърждаване на ролята си на регионален лидер и глобален фактор, съчетавайки дипломатически, икономически, културни и отбранителни инструменти. Част от изследователите свързват тези амбиции с концепцията за „неоосманизъм“, разбирана като стремеж към засилване на политическото, икономическото и културното влияние на Турция в пространства, исторически свързани с Османската империя (Davutoglu 2015). Акцентът е поставен върху обществата и хората – на основата на общност на религията (ислямът) и етноса (турските малцинства в балканските страни).

Съществено място в тази конфигурация заемат САЩ, НАТО и Европейският съюз, чиито интереси и инструменти в Югоизточна Европа в значителна степен се пресичат, но не са идентични – те са насочени не само към политическото влияние, а и към изграждането на средата за сигурност, устойчивост и свързаност в региона.

Политиката на САЩ към региона следва да се оценява в по-широкия геополитически контекст, като двустранните отношения с отделните страни са част от по-общите приоритети на Вашингтон. В подхода на САЩ след края на Студената война условно могат да бъдат разграничени три периода. Първият е участието в управлението на конфликтите и процесите на стабилизиране след разпадането на Югославия. Вторият етап е свързан с приобщаването на страните към системата за сигурност и дейността по интегрирането им в НАТО. Включва последователното приемане в НАТО на България, Румъния, Словения, Албания, Хърватия, Черна гора и Република Северна Македония. Третият етап се характеризира с нарастващ акцент върху възпирането на Русия и ограничаване на нейното влияние основно в сферата на енергетиката и сигурността.

НАТО от своя страна представлява основната институционална рамка за колективната отбрана на държавите членки в региона.[8] Нарастващата важност на Черно море, необходимостта от укрепване на източния и югоизточния фланг, развитието на оперативната съвместимост и военната мобилност превръщат Югоизточна Европа във ключова зона за изпълнение на съюзнически отбранителни и възпиращи функции, включително чрез КФОР (Сили на НАТО в Косово)[9] в Косово.

Обединението на европейския континент след падането на Берлинската стена даде сериозни надежди на страните от Югоизточна Европа

преди всичко чрез заявената ангажираност на Европейския съюз за интегрирането на региона. С течение на времето обаче забавянето на процеса на разширяване и различната скорост на реформите в отделните държави доведоха до нарастваща несигурност относно европейската перспектива на Западните Балкани. Наред с политиката на разширяване ЕС постепенно разшири инструментариума си спрямо региона, включвайки финансово подпомагане, подкрепа за реформи, инфраструктурна и енергийна свързаност и взаимодействие в областта на сигурността. Така европейската политика към ЮИЕ все по-ясно се развива на пресечната точка между интеграция, свързаност и сигурност.

Значение на ЮИЕ за европейската свързаност

В този смисъл значението на ЮИЕ произтича не само от вътрешните му уязвимости, а и от способността му да свързва различни пространства за сигурност и да осигурява условия за военна мобилност, инфраструктурна обезпеченост и взаимодействие между ключови фактори.

Оперативното измерение се фокусира върху развитието на практическата координация в областта на сигурността и отбраната. Това включва засилена военна съвместимост, структури за предно присъствие, многонационални бойни групи, инициативи за морска сигурност и механизми за реагиране на хибридни и информационни заплахи.[10]

Съществен елемент в укрепването на морската сигурност е създаването през 2024 г. на Противоминна военноморска група в Черно море (България, Румъния, Турция)[11], в съчетание с Постоянните военноморски сили на НАТО и други активности на Алианса за опазване на морската сигурност.[12] Това отразява засиленото внимание към повишаване на информираността за обстановката в морето, морските комуникационни линии и защитата на критичната подводна и крайбрежна инфраструктура.

На следващо място, измерението на свързаността отразява нарастващата необходимост от логистична интеграция за гарантиране на сигурността. Коридорите за военна мобилност, инфраструктурата с двойно предназначение и регионалните транспортни и енергийни мрежи допринасят едновременно за оперативната готовност на НАТО и за стратегическата устойчивост на европейския континент. Тази взаимовръзка между транспортната инфраструктура и отбранителните способности е изрично подчертана и в Плана за действие за военна мобилност 2.0 на Европейската комисия[13], който предвижда развитие на транспортни коридори, инфра-

структура с двойно предназначение и хармонизиране на административните процедури за придвижване на военни сили. В това отношение районите на Черно море и Дунав функционират не като отделни пространства, а като допълващи се трасета.

Ключов компонент на тази рамка е Европейският фонд за отбрана (ЕФО), чиято цел е да повиши конкурентоспособността, иновационния капацитет и технологичната съгласуваност на европейската отбранително-промишлена база. Структурните ограничения на Фонда могат да бъдат допълнени от появата на нови финансови механизми на ниво ЕС, сред които инструментът „Мерки за сигурността на Европа“ (SAFE). За разлика от ЕФО, който е насочен към научни изследвания, иновации и развитие на капацитет в ранна фаза, SAFE поставя приоритет върху мащабни инвестиции, включително за укрепване на отбранителната инфраструктура.[14]

В рамките на SAFE редица държави от ЮИЕ получават достъп до значителни финансови ресурси за отбранителни инвестиции. Сред тях са Румъния, България, Хърватия и Гърция.[15] За Румъния е одобрена една от най-мащабните финансови рамки в целия Европейски съюз (16,68 милиарда евро под формата на нисколихвени дългосрочни заеми, което я поставя сред държавите с най-голям достъп до ресурс по SAFE след Полша). Тя насочва значителна част от ресурсите си към транспортната свързаност и логистичните коридори и по този начин засилва своята развиваща се роля на регионален център за военна мобилност и стратегически транзит по югоизточния фланг на НАТО. България, Гърция и Хърватия също насочват ресурс към модернизация на отбранителните способности, противовъздушната отбрана, комуникациите и други ключови способности, което допълнително укрепва военно-стратегическата свързаност на региона.[16]

Необходимостта от бързо изграждане на капацитет и улесняване на военната мобилност може да бъде потърсено и в регионалните проекти за транспортна свързаност. Тази логика е допълнително институционализирана чрез Меморандума за разбирателство между България, Румъния и Гърция[17], с който се създава Платформата за коридора „Черно море – Егейско море“. Споразумението е стъпка към координиране на транспортната политика, развитието на инфраструктурата и трансграничната координация между трите държави. Чрез ускоряване на развитието на железопътните, пътните, пристанищните и вътрешните водни транспортни връзки инициативата укрепва стратегическата ос север – юг между Егейско море, Черно море и река Дунав. Същевременно тя включва съображения за двойна функционалност при регионалното инфраструктурно планиране. В този

смисъл коридорът може да функционира не само като инструмент за икономическа интеграция, а и като ключов фактор за оперативната мобилност на НАТО и ЕС.

В тази рамка все по-често се използва неформалният термин „военен Шенген“. Той отразява текущите усилия в рамките на Европейския съюз за намаляване на административните, правните и инфраструктурните бариери пред бързото придвижване на военен персонал, оборудване и средства в държавите членки. Въвеждането на такива механизми е от особено голямо значение, тъй като пряко засяга скоростта на реакция при кризи и общата ефективност на възпирането.

Тук следва да се отчита и значението на Паневропейския транспортен коридор VIII за свързването на Адриатическо и Черно море, както и необходимостта изискванията за военна мобилност да бъдат интегрирани в транспортната инфраструктура. В този смисъл заслужава да бъде отбелязано и подписаното от Албания, България, Италия и Република Северна Македония писмо за намерения за създаване на хармонизиран коридор за военна мобилност по трасето на Коридор VIII по време на срещата на върха на НАТО във Вашингтон през юли 2024 г. Основната цел е разработване на синхронизирани мерки за преодоляване на административните, инфраструктурните и информационните препятствия пред придвижването на военни товари и личен състав, включително различията в националните правила за преминаване на границите, неефективната система за обмен на информация и недостатъчната съгласуваност между механизмите на НАТО и ЕС.

Основни изводи

Югоизточна Европа постепенно променя своето значение за европейската и евроа-атлантическата сигурност. Стратегическото значение на региона произтича преди всичко от неговата свързваща функция. Географското ѝ положение позволява взаимодействие между Западните Балкани, Черно море, Източното Средиземноморие, Дунавското пространство и Кавказ. Това значение се засилва от развитието на транспортни, енергийни и комуникационни мрежи, както и от необходимостта от изграждане на инфраструктура с двойно предназначение, способна да подпомага както икономическата свързаност, така и военната мобилност.

Западните Балкани остават едновременно зона на уязвимост и стратегическа възможност. Политическата фрагментация, нерешените двус-

транни и вътрешнополитически въпроси, институционалните слабости и различната скорост на европейската интеграция ограничават възможностите за общи регионални политики. Същевременно непосредствената им близост до държавите от ЕС и НАТО увеличават значението за европейската сигурност, свързаност и мобилност.

Югоизточна Европа се превръща във все по-значимо пространство на конкуренция и взаимодействие между външни актьори. По този начин значението на региона се определя не само от неговите вътрешни характеристики, но и от пресичането на различни външни интереси.

Направеният анализ показва, че промяната в стратегическото значение на Югоизточна Европа не се дължи на един-единствен фактор, а на наслагването на геополитически, военно-стратегически, инфраструктурни и икономически измерения. Войната в Украйна, засилената конкуренция между външни актьори, динамиката в Западните Балкани и нарастващата роля на Черноморския регион променят начина, по който ЮИЕ се вписва в европейската среда за сигурност. Регионът остава пространство на уязвимост, но именно съчетанието между географска и инфраструктурна свързаност, военни способности, регионални процеси и интереси на външни актьори го превръща от периферно пространство в стратегически кръстопът.

БЕЛЕЖКИ

1. NATO 2022 Strategic Concept. Available from: https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf

2. В документи на ЕС изразът е използван за първи път през 1998 г., за да се предефинира отношението на Съюза към държавите от ЮИЕ, които в онзи момент не членуват в него: Хърватия, Босна и Херцеговина, Македония, Съюзна република Югославия (СРЮ, съставена от Сърбия и Черна Гора) и Албания. След отказа от първоначалния „регионален подход“ към тази част от Европа ЕС формулира „Процес на стабилизиране и асоцииране“, където използва и израза „Западни Балкани“ за онези държави, които не са обхванати от него.

3. Отношения между ЕС и Западните Балкани. Available from: https://www.consilium.europa.eu/bg/policies/eu-western-balkans-relations

4. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2025 Communication on EU enlargement policy, 4.11.2025, COM(2025) 690 final. Available from: https://enlargement.ec.europa.eu/document/download/eb69a890-40d6-4696-801e-612d51709fdd_en?filename=2025%20Communication%20on%20EU%20Enlargement%20Policy.pdf

5. BANDOVICH, I. Serbian World – A Threat to European Integration and Stability of the Western Balkans. Available from: https://reunir-horizon.eu/serbian-world-a-threat-to-european-integration-and-stability-of-the-western-balkans

6. GAVRILIS, G. The Making of a Greater Albania? Institute on East Central Europe, Columbia University, 1999. Available from: https://ciaotest.cc.columbia.edu/conf/iec03/iec03_15-96.html

7. Belt and Road Portal. Available from: https://eng.yidaiyilu.gov.cn/

8. NATO 2022 Strategic Concept. Available from: https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf

9. Kosovo Force. Available from: https://jfcnaples.nato.int/kfor

10. https://www.nato.int/en

11. Създадена с подписването на Меморандум за разбирателство между България, Румъния и Турция за създаване на противомина военноморска група в Черно море (11.01.2024 г., актуализиран 08.07.2026 г.)

12. NATO maritime activities. Available from: https://www.nato.int/en/what-we-do/operations-and-missions/natos-maritime-activities

13. План за действие за военната мобилност 2.0, Европейска комисия, 10.11.2022, JOIN(2022) 48 final

14. Инструмент „Мерки за сигурността на Европа“ (SAFE). Available from: https://www.consilium.europa.eu/bg/policies/safe

15. Defence Industry and Space, European Commission. Available from: https://defence-industry-space.ec.europa.eu/eu-defence-industry/safe-security-action-europe_en

16. Словения не кандидатства за национален заем по програма SAFE и няма да получи директно европейско финансиране. Тя ще участва единствено в съвместните европейски обществени поръчки за боеприпаси, дронове и системи за противовъздушна отбрана. Държавата ще покрива своя дял в тези общи проекти изцяло със собствени средства от националния си бюджет за отбрана.

17. Меморандум за разбирателство между правителствата на България, Гърция и Румъния за засилено трансгранично сътрудничество в рамките на Платформата за коридор Черно море – Егейско море, 03.12.2025 г. Available from: https://www.mtc.government.bg/bg/category/1/blgariya-grciya-i-rumniya-razvivat-uskoreno-transportnata-os-mezhdu-egeysko-i-cherno-more

ЛИТЕРАТУРА

АЛЕКСИЕВА, Н., 2024. Югоизточна Европа – сътрудничество и/или интеграция? *Военен журнал*, том 131, № 4.

АЛЕКСИЕВА, Н.; ДИМИТРОВ, А.; ДУРЕВ, Г., 2022. *Балканите в българската външна политика: приоритет или „паралелна реалност*. София: Фондация „Фридрих Еберт“, Бюро България. ISBN 978-619-7666-25-0.

БАКАЛОВ, Й., 2018. Нови геополитически предизвикателства на Балканите. *Политика и сигурност*, том 2, № 1, с. 13 – 33.

ДАВУТОГЛУ, А., 2015. *Стратегическа дълбочина.* София: Изток-Запад. ISBN 978-619-152-674-1.

ДИНКОВ, Д., 2011. *Неоидентичности в постмодерния свят.* София: Авангард Прима.

КЮЧУКОВ, Л., 2018. Западните Балкани: колко високо в дневния ред на ЕС?. *Дипломация*, № 21.

BECHEV, D., *2011. Constructing South East Europe: The Politics of Balkan Regional Cooperation*. Palgrave Macmillan.

BIEBER, F. et al., 2019. *Rethinking Stability in the Western Balkans: A View from the Region*. Balkans in Europe Policy Advisory Group.

KMEZIĆ, M.; BIEBER, F., 2018. *The Crisis of Democracy in the Western Balkans: An Anatomy of Stabilitocracy and the Limits of EU Democracy Promotion*. Balkans in Europe Policy Advisory Group.

MULCHINOCK, N., 2017. *NATO and the Western Balkans: From Neutral Spectator to Proactive Peacemaker*. London: Palgrave Macmillan.

REFERENCES

ALEKSIEVA, N., 2024. Yugoiztochna Evropa – satrudnichestvo i/ili integratsia?. *Voenen zhurnal*, vol. 131, no 4 [in Bulgarian].

ALEKSIEVA, N.; DIMITROV, A.; DUREV, G., 2022. *Balkanite v balgarskata vanshna politika: prioritet ili „paralelna realnost“*. Sofia : Fondatsia „Fridrih Ebert“, Byuro Bulgaria. ISBN 978-619-7666-25-0 [in Bulgaria].

BAKALOV, Y., 2018. Novi geopoliticheski predizvikatelstva na Balkanite. *Politika i sigurnost*, vol. 2, no 1, pp. 13 – 33 [in Bulgarian].

BECHEV, D., *2011. Constructing South East Europe: The Politics of Balkan Regional Cooperation*. Palgrave Macmillan.

BIEBER, F. et al., 2019. *Rethinking Stability in the Western Balkans: A View from the Region*. Balkans in Europe Policy Advisory Group.

DAVUTOGLU, A., 2015. *Strategicheska dalbochina*. Sofia: Iztok-Zapad. ISBN 978-619-152-674-1 [in Bulgarian].

DINKOV, D., 2011. *Neoidentichnosti v postmodernia svyat*. Sofia: Avangard Prima [in Bulgarian].

KMEZIĆ, M.; BIEBER, F., 2018. *The Crisis of Democracy in the Western Balkans: An Anatomy of Stabilitocracy and the Limits of EU Democracy Promotion*. Balkans in Europe Policy Advisory Group.

KYUCHUKOV, L., 2018. Zapadnite Balkani: kolko visoko v dnevnia red na ES?. *Diplomatsia*, no 21 [in Bulgaria].

MULCHINOCK, N., 2017. *NATO and the Western Balkans: From Neutral Spectator to Proactive Peacemaker*. London: Palgrave Macmillan.

PERIPHERY OR STRATEGIC CROSSROADS: IS THE ROLE OF SOUTHEASTERN EUROPE IN EUROPEAN SECURITY CHANGING

Abstract. Southeast Europe has traditionally been considered as a peripheral region with regard to the processes unfolding in Europe. The changing geopolitical environment and the growing strategic importance of the Black Sea region highlight the need to reconsider the region's role in ensuring European security. It is approached as a region of interaction and competition among various geopolitical interests, as well as in terms of its importance for connectivity, regional resilience, and stability in Europe. The main argument is that Southeast Europe is gradually transforming from a periphery into a strategic crossroads of growing importance for European and Euro-Atlantic security.

Keywords: European Union; security; Southeastern Europe; transformation

Dr. Nevena Aleksieva, Assist. Prof.
ORCID iD: 0009-0004-4303-7345
National and International Security Department
National Security and Defence Faculty
Rakovski National Defence College
82, Evlogi i Hristo Georgiev Blvd.
1504 Sofia, Bulgaria
E-mail: n.aleksieva@rndc.bg

https://doi.org/10. 66334/annu26_cyberproch

ИЗПОЛЗВАНЕ НА ВИРТУАЛНАТА РЕАЛНОСТ В ТАКТИЧЕСКОТО ИЗГРАЖДАНЕ НА ОТБРАНАТА И СИГУРНОСТТА

Невяна Петкова

Абстракт. Виртуалната реалност е особено полезен съвременен инструмент за модулация, модификация и прогнозна симулация на биполярни и особено опасни ситуации. Изключителните условия, в които се намираме, предикират възможността за креативност и в областта на отбраната, с цел запазване на мира и сигурността. Освен съвременен модерен способ за реакция, виртуалната реалност е и изключително интерактивен, технологичен, бърз, рационален образователен инструмент, предлагащ гъвкавост и адаптивност. Предразполага към множество вариации, проектното разработване на които спестява много време и разходи. Поляризацията на мненията носи дискусионност, но и богати възможности за сътрудничество и партньорство за постигане на реципрочност. Настоящият доклад не претендира за пълна изчерпателност, но представлява синтез на постигнатото в областта и се надява да осветли проблема.

Ключови думи: отбрана; сигурност; тактики; оперативни дейности; дигитални технологии

I. Въведение

Виртуалната реалност има способността за генерална трансформация на сектора по отбрана и сигурност на страната. Тя представлява ефективно съчетание между модерни технологии, безопасност и сигурност, икономическа рационалност, ефективни избори и решения, тактическо обучение, планиране, прогнозиране, симулиране на операции и действия. Нейната роля е основополагаща, а приносът ѝ – висок. Симулационните сценарии носят усещане за контролирана и безопасна среда. Виртуалната реалност е модерен подход, достатъчно ефективно функциониращ в усложнена обстановка, елиминиращ или силно намаляващ вредни отрицателни последици. Намалява физическата и увеличава менталната мащабируемост. Носи консистентност и целенасоченост. Подпомага възприемането на съвременната отбрана от нов ъгъл (Aleksandrova et al. 2024).

Целта на настоящия доклад е да извърши обзорен и систематичен преглед на възможностите за тактическо изграждане на отбраната и сигурността, посредством новите технологии, а именно виртуалната реалност.

Основни задачи:

1. Да се разгледат теоретичните аспекти на темата.

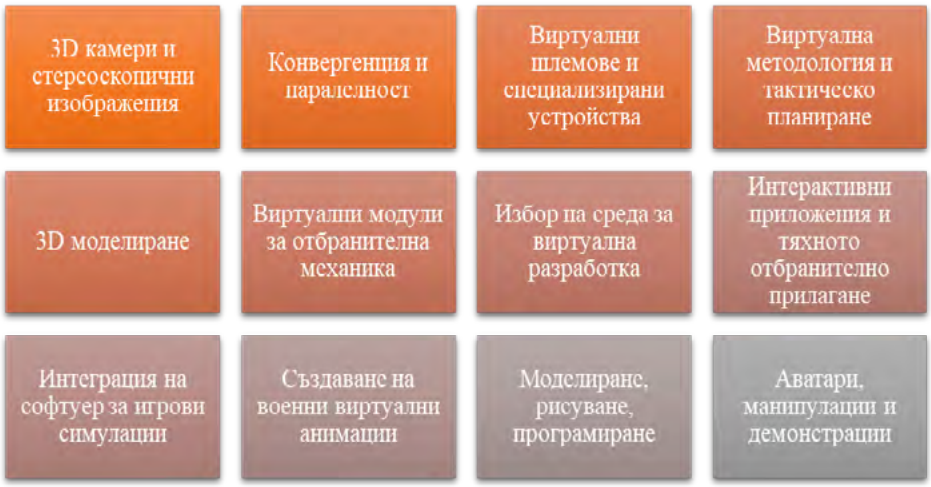
2. Да се представят възможности, перспективи и добри практики за виртуално тактическо изграждане.

3. Да се обобщи и канселира представената информация.

II. Насоки за приложение

За първи път виртуалната реалност в областта на военното дело е представена през 80-те години на миналия век – документиран виртуален симулатор на полет за обучение на пилоти. Оттук насетне виртуалната реалност започва своето ефективно развитие в областта на отбраната и сигурността – обучителна методология, симулационни операции, VR изпитания и експерименти, гъвкави тренировки, договорни спогодби, обучение на служители, завладяващи преживявания, свързани с психо-емоционалната готовност и човешко поведение. Тя повишава продуктивността на военните операции, посредством засилване честотата на практическите сесии, намаляването на разходите, повишаване на безопасността и мотивацията на служителите. Реалните бойни операции, постигнати чрез виртуалните симулации, усъвършенстват адаптацията и човешката организираност. Сгъстените тренировъчни сесии подобряват общата пространствена

осведоменост, както и способността за взимане на решения в условията на криза и напрежение. Травматичните рестрикции подобряват вътрешната увереност на военномедиците и им гарантират прецизност във всяка ситуация. Предоставяйки визуализация и упражнения, виртуалната реалност презентира интерактивно стратегиране, безрисково практикуване, усъвършенствана тактическа динамика. Достига до идентификация и верификация на потенциални опасности и затруднения. Търси тяхната решителна реализация[1].

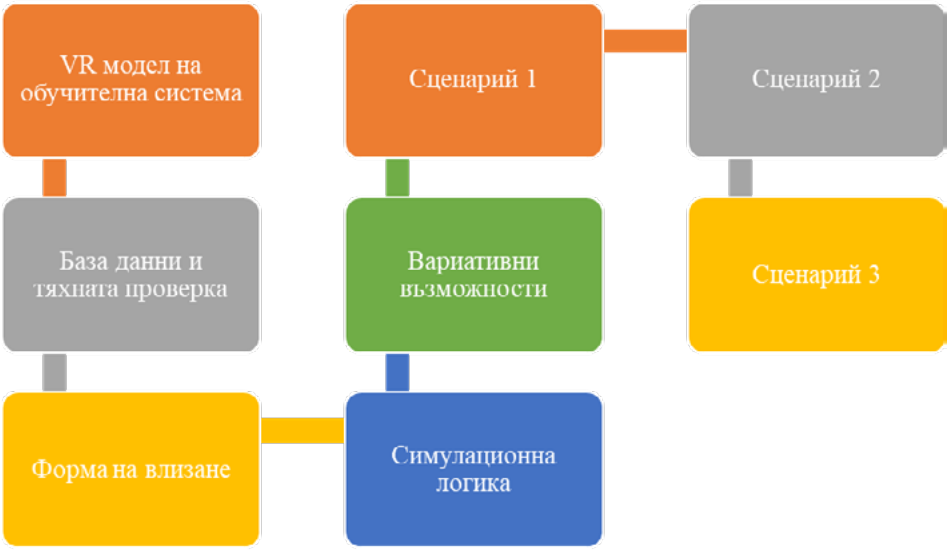


Фигура 1. Основни направления за приложение на виртуалната реалност в отбраната и сигурността[2]

Учебните тренировки с виртуална реалност ще продължат своето съществуване и активно развитие. Ролите, които тя предикира обаче, отнемат своето съществено време и съобразяване със специфични съдържателни, структурни и организационни особености. Но като основно предимство на виртуалната реалност за тактически операции може да се определи нейната потенциална готовност, спестяваща множество нежелани последствия.

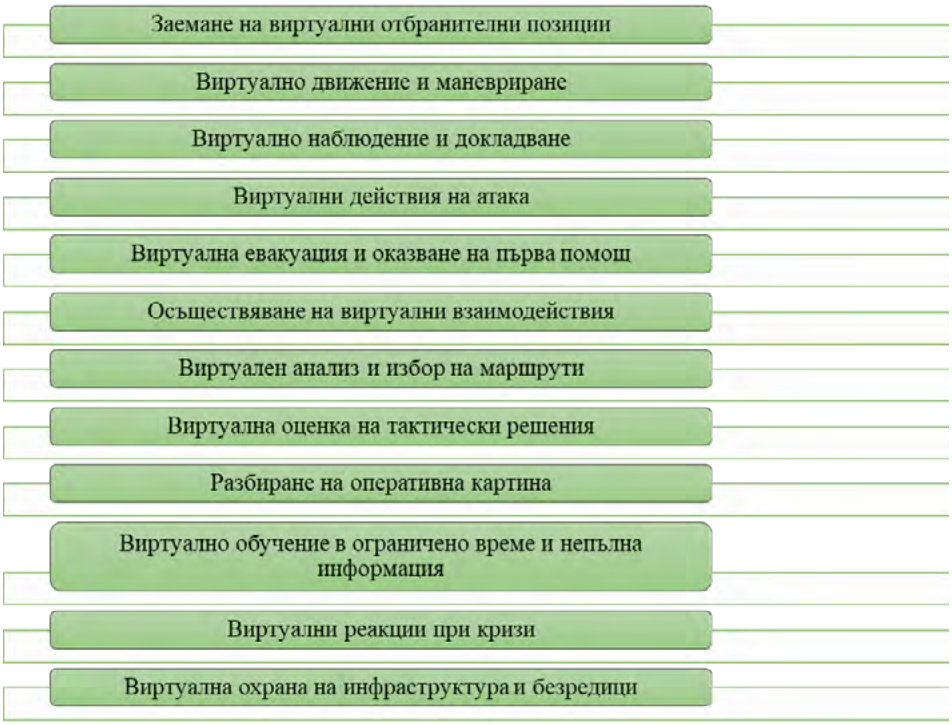
Прилагането и изграждането на виртуални модели в тактическата отбрана и сигурност налага архитектурно описание на системите с множество рамки и модели на приложение. За целта се прилагат специализирани програми, изискващи проектантска среда и интегрирани комуникационни и информационни системи. Те са свързани с отворени стандарти за прак-

тикуване и проследяване. Така се постига повече моделиране и по-добро управление на процесите по оперативно действане.



Фигура 2. Модел на VR за обучение (Todorova 2026)

Практическото приложение включва проверка на съставите и командването, създаване на реалистични терени, проиграване на действия, трениране на взаимодействия между щабове и подразделения, симулиране на обстановка и непредвидими действия, многократно повторения на едни и същи ситуации, варианти, възможности, действия за развитие. Посредством сензори се обследва заобикалящата среда и нейното тактическо състояние. Проектира се и се конструира интересна, предизвикателна, вълнуваща и особено мотивираща среда за отбранително обучение. Могат да се симулират полети, да се обучават медици, да се създаде виртуален тренировъчен лагер, да се симулира бойното поле, да се симулира превозно отбранително средство. Виртуалната реалност в отбраната и сигурността лекува посттравматични стресови разстройства (Georgiev 2024).



Фигура 3. Примерни виртуални тактики на отбрана (Mitkov 2025)

III. Ползи и трудности пред технологичния процес

Виртуалната реалност в толкова сензитивна сфера, като отбраната и сигурността позволява експериментиране, допускане на грешки, множество корекции и трансформации, без риск от наранявания и други произшествия. От особена важност е премереното и разумно управление и тактическо дозиране на отделните оперативни действия и техники. Освен поставянето на различни виртуални средства по различни части на тялото, други неудобства от виртуалната реалност не са установени и писмено документирани (Petkov 2023).

Основни ползи от използването на виртуална реалност в тактическите операции на отбраната и сигурността са:

- скъсено време за обучение;
- канселиране на разходите;

• добри паметови възможности;

• ефективен бюджет и рационално разпределение на разходите;

• без физическо ограничение и широка адаптогенност;

• гъвкава информационна осведоменост;

• реална обратна връзка;

• лекота на разбиране и приемане;

• ниски рискове, заплахи и опасности;

• висока ангажираност на обучаемите служители;

• съвместимост, партньорство и сътрудничество;

• повишаване на доверието, собствените убеждения и способности, както и съпротивителните сили за отвръщане;

• разширяване на обхвата от умения и знания;

• тестване на множество разработки и стратегии в проектен план;

• проиграване на множество сценарии и вариативни ситуации (Georgiev 2024).

Като основни трудности и предизвикателства при използването на виртуална реалност в тактическите операции на отбраната и сигурността можем да определим:

• първоначални инвестиции в софтуер и хардуер;

• разработване на методологии, стратегии и сценарии за виртуална реалност;

• настъпване на ранна умора при дълговременно използване на компютърни средства за симулации;

• виртуалната реалност не пресъздава в пълна изрядност физическата такава;

• прекомерната употреба на дигиталните технологии обикновено води до зависимост;

• качеството на обучението зависи от цифровизацията и реализма;

• необходимост от психо-емоционална адаптация;

• факторна предпоставеност от съвместимост и хармонизация;

• високи нива на риск за киберсигурността и защитата на лични данни;

• използване на безжични устройства и свързани сензори, създаващи предпоставки за пряко проследяване и компрометиране на системата;

• риск от настъпване на свръхидеализация;

• законови и нормативни ограничения (Aleksandrova et al. 2024).

IV. Интеграция и взаимодействие

Като особено ефективен подход за постигане на интеграция и ползотворно взаимодействие между отделните звена и ресори се смята комбинаторният. Той е особено полезен, защото допуска различни вероятности, възможности и разширени перспективи. Позволява изборен резултат, разбиране, приемане, проиграване, контрол, мониторинг, корекция. Важна е теоретичната подготовка, но и практическата насоченост. Отделните ситуации изискват синхрон и взаимни действия между отбранителните звена. Високата степен на взаимодействие се постига посредством сензибилизацията за цел, резултати и мотивация на усилията. Мултифункционалността изисква съвместна колаборация между време, условия на средата и тактически сценарии. За целта успешно се съвместява с изкуствения интелект за създаване на умни и непредсказуеми виртуални противници за постигане на адекватни ответни реакции, тактически технологии, позволяващи сензорни усещания, боравене и умения, смесена реалност за директни бойни действия, наслагване на тактики и термовизионна визуализация[3].

V. Заключение

В резултат на извършения кратък обзорен преглед на известната справочна и електронна информация по така обследвания проблем става ясно, че виртуалната реалност е новата реалност и в сферата на отбраната и сигурността. Тя включва своеобразни дизайни, интерактивни детайли, системи за анализ и обратна връзка, виртуална среда, хардуерни подобрения, поверителна и сигурна информация. Технологията изцяло позволява реалистично отработване на рискови ситуации без непосредна опасност за служителите и техниката. В последните години се възприема, като важен и кумулативен инструмент за модернизиране на тактическото изграждане в отбраната и сигурността. Особено добър помощник е на командирите при управленските механизми и проиграването на ситуации. Тя е неизменна част от цялостна интегрирана система за симулации, подготовка, анализ и екстраполация на техниката.

Предложените примери и предложения със сигурност не изчерпват окончателния списък с тях за отбраната и сигурността, но представляват обобщен актуален план на съвременната виртуална ситуация в отбраната и сигурността.

БЕЛЕЖКИ

1. *Виртуалната реалност във военното обучение* [онлайн]. Достъпно на: https://drawandcode.com/learning-zone/how-can-virtual-reality-be-used-in-military-training/. [Последно видян: 30.09.2026].

2. *Инвестиции в обучението по виртуална реалност* [онлайн]. Достъпно на: https://drawandcode.com/learning-zone/what-is-the-roi-on-virtual-reality-training/. [Последно видян: 30.09.2026].

3. *Програма за развитие на отбранителните способности на въоръжените сили на Република България 2032* [онлайн]. Достъпно на: https://www.strategy.bg/bg/strategy-documents/1402. [Последно видян: 30.09.2026].

4. *Виртуална реалност в обучението на служители* [онлайн]. Достъпно на: https://www.online-learning.bg/virtualna-realnost-v-obuchenieto. [Последно видян: 30.09.2026].

5. *Предимства на VR във военното обучение* [онлайн]. Достъпно на: https://business.vive.com/us/stories/vr-in-military-training./. [Последно видян: 30.09.2026].

ЛИТЕРАТУРА

АЛЕКСАНДРОВА, В.; ХРИСТОЗОВ, И.; ЙОРДАНОВ, Ж.; ДИМИТРОВ, Т. & КОСТАДИНОВ, К., 2024. Приложение на съвременните информационни технологии за симулации и архитектурно описание на взаимодействието на системите от националната сигурност при кризисни ситуации, свързани с киберсигурността и киберотбраната. В: *Сборник с доклади от научна конференция „Национална научна програма „Сигурност и отбрана – състояние и постигнати резултати“*, [5– 6 ноември 2024 г.], т. 10, бр. 1, с. 215 – 225. София: ВА „Г. С. Раковски“. ISSN 1310-9278 (ID № 4715).

ГЕОРГИЕВ, Х., 2024. *Силите за специални операции и приноса им към националната сигурност в мирно време.* София: ВА „Г. С. Раковски“. ISBN 978-619-7711-57-8.

МИТКОВ, В., 2025. Тактически действия на полицейските служители при овладяване на помещения. В: *Сборник с доклади от Първата международна научна конференция „Актуални тенденции и проблеми в областта на борбата с киберсигурността, тероризма, тежката и организираната престъпност“*, [26 – 28 ноември 2024 г.]., с. 235 – 243. София: АМВР.

ПЕТКОВ, Е., 2023. *Обучение във виртуална реалност с пълно потапяне.* Велико Търново: ВТУ „Св. Св. Кирил и Методий“.

ТОДОРОВА, М., 2026. *Виртуалната и добавената реалност като инструмент за развитие на образованието.* [онлайн]. Достъпно на: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.unwe.bg/doi/iited/2024/IITED.2024.33.pdf. [Последно видян: 30.09.2026].

REFERENCES

ALEKSANDROVA, V.; HRISTOZOV, I.; YORDANOV, ZH.; DIMITROV, T. & KOSTADINOV, K., 2024. Prilozhenie na savremennite informatsionni tehnologii za simulatsii i arhitekturno opisanie na vzaimodeystvieto na sistemite ot natsionalnata sigurnost pri krizisni situatsii, svarzani s kibersigurnostta i kiberotbranata. In: *Sbornik s dokladi ot nauchna konferentsia „Natsionalna nauchna programa „Sigurnost i otbrana – sastoyanie i postignati rezultati“,* [5– 6 noemvri 2024 g.], vol. 10, no. 1, pp. 215 – 225. Sofia: VA „G. S. Rakovski“. ISSN 1310-9278 (ID № 4715). [in Bulgarian].

GEORGIEV, H., 2024. *Silite za spetsialni operatsii i prinosa im kam natsionalnata sigurnost v mirno vreme.* Sofia: VA „G. S. Rakovski“. ISBN 978-619-7711-57-8. [in Bulgarian].

MITKOV, V., 2025. Takticheski deystvia na politseyskite sluzhiteli pri ovladyavane na pomeshtenia. In: *Sbornik s dokladi ot Parvata mezhdunarodna nauchna konferentsia „Aktualni tendentsii i problemi v oblastta na borbata s kibersigurnostta, terorizma, tezhkata i organiziranata prestapnost“*, [26 – 28 noemvri 2024 g.]., pp. 235 – 243. Sofia: AMVR. [in Bulgarian].

PETKOV, E., 2023. *Obuchenie vav virtualna realnost s palno potapyane*. Veliko Tarnovo: VTU „Sv. Sv. Kiril i Metodiy“. [in Bulgarian].

TODOROVA, M., 2026. *Virtualnata i dobavenata realnost kato instrument za razvitie na obrazovanieto*. [onlayn]. Dostapno na: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.unwe.bg/doi/iited/2024/IITED.2024.33.pdf. [Posledno vidyan: 30.09.2026]. [in Bulgarian].

THE USE OF VIRTUAL REALITY IN THE TACTICAL DEVELOPMENT OF DEFENSE AND SECURITY

Abstract. Virtual reality is a particularly useful modern tool for the modulation, modification, and predictive simulation of bipolar and especially dangerous situations. The exceptional circumstances in which we find ourselves create opportunities for creativity in the field of defense as well, with the aim of preserving peace and security. Beyond serving as a modern method of response, virtual reality is also a highly interactive, technological, rapid, and rational educational tool that offers flexibility and adaptability. It facilitates numerous variations, the project development of which saves significant time and costs. The polarization of opinions fosters debate but also offers significant opportunities for cooperation and partnership to achieve reciprocity. This report does not claim to be

exhaustive; rather, it presents a synthesis of achievements in the field and aims to shed light on the issue.

Keywords: defense; security; tactics; operational activities; digital technologies

Neviana Petkova
Autor/Writer
ORCID iD: 0009-0009-2589-5481
EIC: 180114700
Web of Science Researcher ID KFS-3859-2024
6, Stoyan Mihaylovski St.
7015 Ruse, Bulgaria
E-mail: nevi_84@abv.bg

https://doi.org/10. 66334/annu26_vlivrefakt

ВЛИЯНИЕ НА ПРОСТРАНСТВЕНО-ВРЕМЕВИТЕ ФАКТОРИ, ХИДРОМЕТЕОРОЛОГИЧНАТА СРЕДА И ЛОГИСТИЧНИЯ ДЕФИЦИТ ВЪРХУ ОПЕРАТИВНИТЕ СПОСОБНОСТИ ПРИ ДАЛЕЧНИ ПОЛЯРНИ ПЛАВАНИЯ

капитан I ранг Николай Данаилов
ВВМУ „Никола. Й. Вапцаров“

Абстракт. Разработката представя емпирично изследване, базирано на прекия команден опит от историческото първо плаване на българския военен научноизследователски кораб „Св. св. Кирил и Методий“ до Антарктика и последващите ежегодни експедиции за надграждане на придобитите способности. Реализираните презокеански мисии маркират безпрецедентен парадигмален скок в развитието на Военноморските сили, дефиниращ прехода от опериране в затворени морски театри към генериране на присъствие в Световния океан и в отдалечени райони. Анализирано е комплексното въздействие на пространствено-времевите и екстремните хидрометеорологични фактори върху устойчивостта на платформата. Разгледани са предизвикателствата на експлоатацията в условия на екстремна отдаленост и затруднено логистично осигуряване, налагащи поддържането на абсолютна автономност поради липсата на изградена брегова инфраструктура.

На базата на реални експлоатационни условия се предлага оптимизиран управленски модел за минимизиране на риска и институционална адаптация на системите за отбрана и сигурност.

Ключови думи: далечни плавания; логистичен дефицит; оперативни способности; полярни експедиции; пространствено-времеви фактори; управление на риска

1. Увод

Съвременната архитектура на международната сигурност се намира в епоха на безпрецедентна динамика, характеризираща се с хиперсвързаност и нарастваща уязвимост на морските комуникации (Mednikarov 2008; Till 2018). В този контекст Световният океан престава да бъде разглеждан единствено като транспортна артерия и се утвърждава като критичен домейн за проектиране на държавен суверенитет, интегрирано възпиране и стратегическо влияние (Humpert, Raspotnik 2012; Till 2018). Според „Доктрина за морски операции“ (НП-3.1) морският домейн, освен чисто физическите си измерения, включва търговски пътища, възлови точки и критична инфраструктура, като осигуряването на свободата на корабоплаване и безопасността на морските маршрути е неотменна част от морския суверенитет на страната.[1]

За отворени икономики като тази на Република България гарантирането на националните интереси налага преосмисляне на традиционните отбранителни парадигми (Mednikarov 2008). Ограничаването на военноморското присъствие до литоралната зона на Черно море вече не е достатъчно за адекватен отговор на новите глобални предизвикателства (Till 2018). Придобиването на военния научноизследователски кораб „Св. св. Кирил и Методий“, ник 421 и неговото развръщане в Световния океан в рамките на националната полярна програма бележи повратен момент в институционалното развитие на Военноморските сили на Република България (Rogan-Finnemore et al. 2021). Същевременно международните регулации подчертават, че операциите в полярни води налагат допълнителни изисквания към системите и управлението на корабите, надхвърлящи стандартните конвенции SOLAS и MARPOL, поради високата уязвимост на екосистемите и суровите условия.[2] Тези презокеански плавания служат като стратегически катализатор, който тества и разширява границите на оперативните възможности на флота (Vego 2009).

Антарктика и полярните региони се утвърждават не само като безценни лаборатории за глобалните климатични и научни изследвания, но и като своеобразна арена за демонстриране на високотехнологични национални способности и логистична зрялост (Coronado-Hernandez et al., 2024; Rogan-Finnemore et al. 2021). Спецификата на антарктическите плавания се обуславя от уникалния международен правен режим на Антарктическия договор[3] и строгите екологични норми на Мадридския протокол[4], които налагат експлоатацията на специализирани платформи, гарантиращи минимален екологичен отпечатък и максимална безопасност за крехките екосистеми (Rogan-Finnemore et al. 2021).[5] Оперирането в тези крайни южни ширини е свързано с преодоляването на безпрецедентни предизвикателства, които произтичат от динамичната ледова обстановка, ниските температури, липсата на надеждни хидрографски данни и критичната отдаленост от брегова инфраструктура и центрове за търсене и спасяване.[6] В този смисъл всяка полярна експедиция прераства от рутинен транспортен преход в изключително сложна мултидомейн операция (Coronado-Hernandez et al. 2024). Тя изисква сигурна корабна автономност и налага изграждането на устойчива военно-цивилна синергия, чрез която въоръжените сили предоставят критичната логистична и платформена база за успешното реализиране на държавните научни програми в Световния океан (Rogan-Finnemore et al. 2021).

2. Предизвикателства на пространствено-времевия мащаб и комуникационните бариери

Експедициите до ледения континент изискват преодоляване на големи дистанции – често надхвърлящи 20 хиляди морски мили в двете посоки, което поставя кораба в условия на продължителна автономност (Vego 2009). Пространственият мащаб налага поетапното пресичане на коренно различни морски зони – от навигационно натоварените и осигурени райони на Средиземноморието, до голямата географска изолираност на трансатлантическия преход до бреговете на Патагония и „враждебната“ среда на юг от 55-ия паралел (Ivanov 2019). От гледна точка на времевия фактор продължителността на дългосрочното плаване прави стандартните методи за краткосрочно тактическо планиране неособено актуални (Vego 2009). Големите разстояния драстично увеличават времето за потенциална реакция при възникване на инциденти, което превръща натренираността на екипажа за самостоятелна борба за живучест

и продължителната автономност на кораба в единствена гаранция за оцеляване (Angelov 2024; Angelov 2023).

Изграждането на способности за проектиране на сила и присъствие отвъд националните зони на отговорност изисква и динамична адаптация на системата за командване и управление.[7] За да се гарантира безопасността на плаването/мисията или операцията, съвременното оперативно изкуство налага стриктното внедряване на специализирано „Ръководство за експлоатация в полярни води – PWOM".[8] То предоставя на командира предварително дефинирани алгоритми за вземане на решения, включително планиране на маршрути за избягване на лед и екстремни температури, както и процедури в случай на инциденти в отдалеченост от логистични бази.[9]

Ключов елемент в проектирането на експедиционен потенциал е устойчивостта на системата за командване и управление. В затворени морски театри комуникационната осигуреност се приема за базова функция, която зависи от сигурността на средата, но трансокеанският преход и навлизането в полярните зони разкриват сериозни технологични празноти. Основното предизвикателство е свързано с физичните и геометричните ограничения на традиционните геостационарни сателити. Тъй като те са позиционирани над земния екватор, с увеличаване на географската ширина ъгълът на видимост (елевацията) прогресивно намалява. Теоретичната граница, отвъд която тези спътници стават напълно невидими при нулева елевация на антената, е 81-ият паралел (Fjørtoft, Bekkadal, Kabacik 2013; Szalkai 2024). В реални експлоатационни морски условия обаче, дори при използването на високотехнологични жиростабилизирани антени, компенсиращи бордовото и киловото клатене на кораба, практическата нестабилност и деградация на геостационарния сигнал започват да се проявяват осезаемо още при преминаването на 70°–76° ширина (Fjørtoft, Bekkadal, Kabacik 2013; Szalkai 2024). Това създава огромни зони на „комуникационна сянка", които силно възпрепятстват изграждането на мрежово-центрична война, чиито нужди от специализирана сателитна инфраструктура във високите ширини се изтъкват и в доклади на ВМС на САЩ (Fjørtoft, Bekkadal, Kabacik 2013; Szalkai 2024).

Този технологичен дефицит се задълбочава допълнително от специфичните геофизични процеси, които произтичат от сложното взаимодействие между литосферата, атмосферата и йоносферата. Полярната йоносфера се характеризира с високо ниво на насищане с електрони и изключителна динамика, която генерира резки електромагнитни смущения

(Szalkai 2024). Тези явления не само влошават качеството на конвенционалните високочестотни (HF) радиовръзки, а и причиняват дисперсия на сигналите и сериозни времеви закъснения, които водят понякога и до осезаеми грешки в глобалните навигационни сателитни системи (Fjørtoft, Bekkadal, Kabacik 2013; Szalkai 2024). В съвкупност, ограничената спътникова видимост и йоносферните аномалии превръщат поддържането на устойчива C2 система в едно от сериозните оперативни изпитания. Както се посочва в „Доктрина за морски операции“ (НП-3.1), Комуникационно-информационната система на ВМС е основна поддържаща система на C2, чиято задача е да осигурява на командира и щаба непрекъснат достъп до информация за вземане на решения.[10]

Доскоро в тези екстремни условия комуникацията бе ограничена до нестабилен и нискоскоростен обмен на данни през класически спътникови мрежи като *Inmarsat* и *Iridium*, които често генерират значителни времеви закъснения (Fjørtoft, Bekkadal, Kabacik 2013; Szalkai 2024). Практическият експлоатационен опит от последните полярни кампании обаче категорично отчита мащабен технологичен скок. Наблюдава се масово навлизане на широколентови нискоорбитални сателитни съзвездия от ново поколение, като *Starlink*, които коренно променят комуникационната архитектура на море. Тези системи осигуряват висока стабилност и висикоскоростен обмен на данни, превръщайки се в основен комуникационен канал, докато традиционните системи преминават в ролята на надежден стратегически резерв. Преодоляването на комуникационните бариери се финализира чрез интегрирането на интелигентни хибридни мрежи, които автоматично превключват между наличните спътникови и брегови канали според тяхната наличност и качество (Fjørtoft, Bekkadal, Kabacik 2013). Тази технологична адаптация осигурява постоянен поток на данни за нуждите на командването и получаване на метеорологични прогнози в реално време, превръщайки далечното плаване във високотехнологична проекция на националната морска мощ (Till 2018).[11]

3. Въздействие на средата и динамичната хидрометеорология

При реализирането на полярни експедиции природната среда престава да бъде просто пасивен навигационен фон и се трансформира в първостепенен източник на агресивна кинетична и термодинамична заплаха, която действа като своеобразен асиметричен противник (Ivanov 2019). Анализът дефинира няколко критични групи опасности, които се проявяват в

логическа последователност при навлизането в полярните ширини (Ivanov 2019). Първоначалното предизвикателство е свързано с екстремната хидродинамика и засилената циклонална активност (Ivanov 2019). В зоните на западните ветрове, известни като „Ревящите четиридесет“ и „Яростните петдесет“, липсата на континентални прегради способства за формирането на големи океански вълни, често надвишаващи 8 – 9 метра (Ivanov 2019). Това може да предизвика критично бордово и килево клатене и подлага корпуса на кораба на сериозни механични напрежения (Ivanov 2019). Едновременно с това, при силни и неблагоприятни ветрове се редуцира и ефективната скорост на съда, което от своя страна предизвиква повишаване на разхода на гориво и създава пряка опасност за енергийната автономност в условия на пълна географска изолация (Till 2018; Vego 2009).

На следващ етап навигационната обстановка се усложнява допълнително от ледовите динамични бариери (Karahalil, Ozsoy 2025; Fjørtoft, Bekkadal, Kabacik 2013). Процесите на образуване и топене на паковия лед превръщат океанското полярно пространство в динамично променящ се лабиринт (Karahalil, Ozsoy 2025; Fjørtoft, Bekkadal, Kabacik 2013). Парадоксално, редуцирането на ледената покривка вследствие на глобалното затопляне не улеснява прехода, а увеличава рисковете, тъй като води до по-често откъсване на ледени полета и повишено наличие на плаващи ледени отломки по утвърдените маршрути (Humpert, Raspotnik 2012). Изключително коварна заплаха в тази среда представляват полупотопените ледени късове с висока плътност и нисък профил, наречени „гроулъри“ (Karahalil, Ozsoy 2025). Тяхното засичане чрез корабните радиолокационни станции е силно затруднено, особено когато мощното океанско вълнение маскира радарното ехо (Karahalil, Ozsoy 2025).

Специфичен критичен фактор е породен от отдръпването на ледниците, което разкрива нови, некартографирани водни пространства (Karahalil, Ozsoy 2025). В тези участъци съществуващите електронни навигационни карти често дават сериозни отклонения от реалната батиметрия, като са регистрирани случаи, при които реална дълбочина от едва 5 метра е отбелязана като 14 метра (Karahalil, Ozsoy 2025). За военен кораб със значително газене подобни разминавания генерират перманентна и критична опасност от засядане (Karahalil, Ozsoy 2025).

Съвкупността от тези сурови хидрометеорологични условия създава предпоставки за изключително бързо обледяване на надстройките.[12] При съчетание на отрицателни температури, ураганен вятър и морски пръски върху най-високите части на кораба могат много бързо да се натрупат то-

нове ледена маса (Szalkai 2024).[13] Според стриктните изисквания на Полярния код изчисленията за стабилност трябва задължително да предвиждат потенциално натрупване на лед от 30 кг/м^2 върху откритите палуби, както и до 7 кг/м^2 по страничните повърхности над водолинията.[14] Тази добавена непланирана тежест измества центъра на тежестта на кораба (KG) нагоре, редуцира метацентричната височина (GM) и създава реална опасност от загуба на напречна устойчивост (Ivanov 2019; Szalkai 2024).[15] Ситуацията може да ескалира допълнително, ако т.нар. „ледена супа“ запуши кингстоните, причинявайки аварийна загуба на ход в ключови моменти от плаването (Ivanov 2019).

За да се гарантира изпълнението на поставените задачи, корабните системи и механизми трябва да функционират безотказно в широк температурен диапазон, надвишаващ с поне 10° С по-висока от екваториалните температури и поне 10° С по-ниски от предполагаемите работни температури в Антарктика.[16] Успоредно с това, екстремно ниските температури водят до скъсяване на живота на литиево-йонните батерии и нарушават работата на хидравличните системи, което силно ограничава използването на автономни безпилотни апарати и външна комуникационна техника на открито (Szalkai 2024).

4. Лидерство в екстремна среда и исторически уроци

Оперативното изкуство при далечни плавания не може да бъде разглеждано изолирано от историческия опит. Британската кралска трансантарктическа експедиция на сър Ърнест Шакълтън (1914 – 1917 г.) предоставя два безценни модела за лидерство и вземане на решения в условия на пълен логистичен дефицит и географска изолация.

Първият модел е свързан с „Гения на Шакълтън“ и съдбата на неговия кораб „Ендюрънс“ (Till 2018; Vego 2009; Elleman, Paine 2015). След като корабът е смазан от ледовете в море Уедъл, Шакълтън демонстрира изключителната способност да преформулира целите (Vego 2009). Когато първоначалният план за прекосяване на континента става неизпълним поради обективни обстоятелства, той дефинира нова, жизненоважна цел – спасяването на екипажа (Vego 2009). Този гъвкав и прагматичен подход към създалата се кризисна ситуация поддържа морала на хората му и довежда до тяхното спасяване (Vego 2009).

Вторият модел произтича от съдбата на втората група от същата експедиция в море Рос и техния кораб „Аврора“, които оперират от дру-

гата страна на континента (Vego 2009; Elleman, Paine 2015). След като техният кораб е откъснат от ледовете по време на свирепа буря, брегoвият отряд остава напълно изолиран, без почти никакви провизии и адекватно зимно облекло (Vego 2009). Въпреки невъзможността от среща на двете групи и на своя експедиционен командир, тоталния срив на логистичното осигуряване, екипажът не само оцелява, но и изпълнява поставената си задача – изграждане на депа с провизии на протежение от над 360 морски мили (Vego 2009). Този преход със шейни, продължил 199 дни в условия на постоянен дефицит, остава ненадминат в аналите на полярните изследвания (Vego 2009).

Урокът за съвременното военноморско лидерство е категоричен – дори при пълна загуба на технологичното и логистичното осигуряване, желязната дисциплина, психологическата адаптивност на командването и човешкият дух остават крайният гарант за изпълнението на мисията (Till 2018; Vego 2009).

5. Военно-цивилна синергия и „мека сила“ (*soft power*)

В епохата на засилена геополитическа конкуренция развръщането на военноморски сили в Световния океан надхвърля традиционните отбранителни функции и се превръща в ключов механизъм за интегрирано възпиране и стратегическо влияние (Humpert, Raspotnik 2012; Elleman, Paine 2015). Въпреки че Антарктическият договор от 1959 г. дефинира Ледения континент като демилитаризирана зона, посветена на мира, той изрично регламентира правото на държавите да използват военен персонал и оборудване за логистична и научноизследователска подкрепа.[17] Подобно участие на въоръжените сили в хуманитарни и изследователски мисии е класическо проявление на държавната „мека сила“ (Elleman, Paine 2015). Синхронизирането на флотските операции с дипломатическия потенциал на държавата отговаря напълно на заложеното в „Доктрина за морски операции“ (НП-3.1), където се предвижда изпълнението на мисии в мирно време извън националната територия, базирани на международни ангажименти и целящи утвърждаване на суверенитета (Ivanov 2019).

Експлоатацията на специализирани морски платформи представлява високо постижение на военно-цивилната синергия (Rogan-Finnemore et al. 2021).[18] Съвременните изследователски кораби са конструирани като мултифункционални съоръжения, които трябва да постигнат сложен инженерен баланс между структурната здравина и високите критерии на научната

общност (Rogan-Finnemore et al. 2021).[19] За да отговорят на високите екологични императиви на Протокола за опазване на околната среда (Мадридския протокол), съдовете се изграждат със задължителен двоен корпус, който осигурява максимална протекция на танковете срещу евентуални ледови пробойни.[20] Успоредно с това, за минимизиране на негативното въздействие върху чувствителната полярна фауна, корабните системи се оптимизират за драстично редуциране на подводния шум и отделяните въглеродните емисии, покривайки строги сертификационни стандарти (Rogan-Finnemore et al. 2021).[21]

Предоставянето на военен логистичен капацитет в услуга на науката води до оптимизация на държавните ресурси и генерира устойчиви международни партньорства (Elleman, Paine 2015). Взаимодействието с крайбрежните държави по време на транзитните преходи се трансформира във високорезултатна инфраструктурна дипломация, която изгражда институционално доверие и превръща логистичните маршрути в инструмент на активната външна политика (Elleman, Paine 2015). Този бързо натрупващ се безпрецедентен експедиционен опит категорично диктува необходимостта от концептуално надграждане. Актуализирането на „Доктрина за морски операции“ (НП-3.1) ще интегрира новите реалности на глобалното присъствие, спецификите на управлението в екстремни среди и стратегическото значение на военно-цивилната синергия като мощен лост на националната морска мощ (Ivanov 2019; Till 2018).

6. Заключение и изводи

Извършеният анализ категорично показва, че проектирането на експедиционен потенциал чрез далечни полярни плавания маркира безпрецедентен парадигмален и концептуален преход в развитието на родните Военноморски сили. Обективната морска среда във високите ширини функционира като постоянен, безкомпромисен асиметричен противник, при който съществува нулев марж на допустимо отклонение спрямо каквито и да е навигационни, технически или логистични пропуски.

Успешната реализация на подобни мащабни плавания и проекцията на реално присъствие се основават на прецизно динамично управление на риска. Това изисква изграждането на дълбока синергия между съвременно оперативно изкуство, технологично адаптирани системи за командване и управление, гъвкаво експедиционно логистично осигуряване, както и безупречна психофизиологична подготовка на екипажите. Внедряването

на стриктните стандарти на Полярния код, абсолютното съблюдаване на Антарктическия договор и Мадридския протокол, както и извличането на поуки от историческите лидерски модели са не просто препоръчителни, а задължителни условия за минимизиране на оперативния риск и гарантиране на оцеляването.

Практическата значимост на този безценен емпиричен опит диктува необходимостта от актуализиране на нормативната и доктринална рамка на Въоръжените сили. Спецификите на подобни операции изискват „Доктрина за морски операции“ (НП-3.1) да бъде надградена, за да се регламентират официално процесите по глобално експедиционно развръщане.

В обобщение, чрез генерирането на реално присъствие в най-отдалечените региони на планетата военно-цивилната синергия се утвърждава като високоефективен инструмент на глобалната научна дипломация и сигурност. Това стратегическо надграждане на оперативните способности маркира категоричен еволюционен скок, превръщайки държавата от пасивен консуматор на сигурност в активен, способен и авторитетен субект на международните морски отношения.

Благодарности: Формулираните в настоящата разработка изводи са плод на системен анализ, пречупен през призмата на непосредствената експертиза на автора от управлението на ник 421 в полярните ширини. Използвам случая да засвидетелствам своята най-искрена признателност към личния състав на кораба – тяхната психическа устойчивост, непоколебима субординация и експертност са истинският фундамент на българския военноморски успех в Антарктика.

БЕЛЕЖКИ

1. Министерство на отбраната, 2022. *Доктрина за морски операции на въоръжените сили на Република България (НП-3.1)*. Изд. А. Варна: Министерство на отбраната

2. IMO, 2015. *International Code for Ships Operating in Polar Waters (Polar Code)*. MEPC 68/21/Add.1, Annex 10. London: International Maritime Organization

3. *The Antarctic Treaty*. Washington, D.C., 1959

4. *Protocol on Environmental Protection to the Antarctic Treaty*. Madrid, 1991

5. IMO, 2015. *International Code for Ships Operating in Polar Waters (Polar Code)*. MEPC 68/21/Add.1, Annex 10. London: International Maritime Organization

6. IMO, 2015. *International Code for Ships Operating in Polar Waters (Polar Code)*. MEPC 68/21/Add.1, Annex 10. London: International Maritime Organization

7. NATO, 2021. *Allied Joint Doctrine for Maritime Operations (AJP-3.1)*. Edition C, Version 1. Brussels: NATO Standardization Office

8. IMO, 2015. *International Code for Ships Operating in Polar Waters (Polar Code)*. MEPC 68/21/Add.1, Annex 10. London: International Maritime Organization

9. IMO, 2015. *International Code for Ships Operating in Polar Waters (Polar Code)*. MEPC 68/21/Add.1, Annex 10. London: International Maritime Organization

10. Министерство на отбраната, 2022. *Доктрина за морски операции на въоръжените сили на Република България (НП-3.1)*. Изд. А. Варна: Министерство на отбраната

11. IMO, 2015. *International Code for Ships Operating in Polar Waters (Polar Code)*. MEPC 68/21/Add.1, Annex 10. London: International Maritime Organization

12. IMO, 2015. *International Code for Ships Operating in Polar Waters (Polar Code)*. MEPC 68/21/Add.1, Annex 10. London: International Maritime Organization

13. IMO, 2015. *International Code for Ships Operating in Polar Waters (Polar Code)*. MEPC 68/21/Add.1, Annex 10. London: International Maritime Organization

14. IMO, 2015. *International Code for Ships Operating in Polar Waters (Polar Code)*. MEPC 68/21/Add.1, Annex 10. London: International Maritime Organization

15. IMO, 2015. *International Code for Ships Operating in Polar Waters (Polar Code)*. MEPC 68/21/Add.1, Annex 10. London: International Maritime Organization

16. IMO, 2015. *International Code for Ships Operating in Polar Waters (Polar Code)*. MEPC 68/21/Add.1, Annex 10. London: International Maritime Organization

17. Министерство на отбраната, 2022. *Доктрина за морски операции на въоръжените сили на Република България (НП-3.1)*. Изд. А. Варна: Министерство на отбраната; *The Antarctic Treaty*. Washington, D.C., 1959

18. IMO, 2015. *International Code for Ships Operating in Polar Waters (Polar Code)*. MEPC 68/21/Add.1, Annex 10. London: International Maritime Organization

19. IMO, 2015. *International Code for Ships Operating in Polar Waters (Polar Code)*. MEPC 68/21/Add.1, Annex 10. London: International Maritime Organization

20. IMO, 2015. *International Code for Ships Operating in Polar Waters (Polar Code)*. MEPC 68/21/Add.1, Annex 10. London: International Maritime Organization; *Protocol on Environmental Protection to the Antarctic Treaty*. Madrid, 1991

21. IMO, 2015. *International Code for Ships Operating in Polar Waters (Polar Code)*. MEPC 68/21/Add.1, Annex 10. London: International Maritime Organization

22. GONCHAROV, V. K., et al., 2024. Analysis of the impact of Arctic environment conditions on the psychophysical status of navigators and the safety of ice navigation. *Transportation Safety and Environment*, vol. 6.

ЛИТЕРАТУРА

АНГЕЛОВ, К., 2024. Времеви параметър при определяне състоянието на системата за безопасност на военен кораб. В: *Сборник доклади от научна конференция с международно участие „20 години България в НАТО и НАТО в България“ на ВА „Г. С. Раковски“*. София: ВА „Г. С. Раковски“, с. 320 – 326. ISBN 978-619-7711-52-3.

АНГЕЛОВ, К.,2023. Дескриптивен анализ на инциденти с кораби на страни от Европейския съюз. В: *Сборник доклади от годишната университетска научна конференция на НВУ „Васил Левски“*. Велико Търново: НВУ „Васил Левски“, с. 495 – 504. ISSN 1314-1937; ISSN 2367-7481.

ИВАНОВ, В., 2019. *Военногеографски фактори и тяхното влияние върху оперативната среда*. София: ВА „Г. С. Раковски“.

МЕДНИКАРОВ, Б., 2008. *Сигурност на морската транспортна система*. Варна: ВВМУ „Н. Й. Вапцаров“.

CORONADO-HERNANDEZ, J. R., et al., 2024. Naval Antarctic Supply Chain Modeling and Simulation. *Procedia Computer Science*, vol. 238, pp. 1023-1028.

ELLEMAN, B.A.; PAINE, S.C.M., 2015. *Navies and Soft Power: Historical Case Studies of Naval Power and the Nonuse of Military Force.* Newport Paper 42. Newport: Naval War College Press.

FJØRTOFT, K.E.; BEKKADAL, F.; KABACIK, P., 2013. Maritime Operations in Arctic Waters. In: *OCEANS 2013*. IEEE.

HUMPERT, M.; RASPOTNIK, A., 2012. The Future of Arctic Shipping Along the Transpolar Sea Route. *Arctic Yearbook*, vol. 1, pp. 281-307.

KARAHALIL, M.; OZSOY, B.; OKTAR, O., 2025. Navigational challenges in Svalbard: insights from a research expedition. *WMU Journal of Maritime Affairs*, vol. 24, pp. 201-224. Available оидп: https://doi.org/10.1007/s13437-025-00364-x.

ROGAN-FINNEMORE, M. et al., 2021. Icebreaking polar class research vessels: New Antarctic fleet capabilities. *Polar Record*, vol. 57(e46).

SZALKAI, P., 2024. The Unique Environmental Features of the Arctic That Affect Military Capabilities. *HDR*, № 1-2, pp. 108-121.

TILL, G., 2018. *Seapower: A Guide for the 21st Century*. 4th ed. London: Routledge. ISBN 978-1138657670.

VEGO, M., 2009. *Joint Operational Warfare: Theory and Practice*. Newport: U.S. Naval War College.

REFERENCES

ANGELOV, K., 2023. Deskriptiven analiz na intsidenti s korabi na strani ot Evropeyskia sayuz. In: *Sbornik dokladi ot godishnata universitetska nauchna konferentsia na NVU „Vasil Levski“*, pp. 495 – 504. Veliko Tarnovo: NVU „Vasil Levski“. ISSN 1314-1937; ISSN 2367-7481 [in Bulgarian].

ANGELOV, K., 2024. Vremevi parametar pri opredelyane sastoyanieto na sistemata za bezopasnost na voenen korab. In: *Sbornik dokladi ot nauchna konferentsia s mezhdunarodno uchastie „20 godini Bulgaria v NATO i NATO v Bulgaria“ na VA „G. S. Rakovski“*, pp. 320 – 326. Sofia: VA „G. S. Rakovski“. ISBN 978-619-7711-52-3 [in Bulgarian].

CORONADO-HERNANDEZ, J. R. et al., 2024. Naval Antarctic Supply Chain Modeling and Simulation. *Procedia Computer Science*, vol. 238, pp. 1023-1028.

ELLEMAN, B.A.; PAINE, S.C.M., 2015. *Navies and Soft Power: Historical Case Studies of Naval Power and the Nonuse of Military Force.* Newport Paper 42. Newport: Naval War College Press.

FJØRTOFT, K.E.; BEKKADAL, F.; KABACIK, P., 2013. Maritime Operations in Arctic Waters. In: *OCEANS 2013*. IEEE.

HUMPERT, M.; RASPOTNIK, A., 2012. The Future of Arctic Shipping Along the Transpolar Sea Route. *Arctic Yearbook*, vol. 1, pp. 281-307.

IVANOV, V., 2019. *Voennogeografski faktori i tyahnoto vliyanie varhu operativnata sreda*. Sofia: VA „G. S. Rakovski“ [in Bulgarian].

KARAHALIL, M.; OZSOY, B.; OKTAR, O, 2025. Navigational challenges in Svalbard: insights from a research expedition. *WMU Journal of Maritime Affairs*, vol. 24, pp. 201-224. Available оидп: https://doi.org/10.1007/s13437-025-00364-x.

MEDNIKAROV, B., 2008. *Sigurnost na morskata transportna sistema*. Varna: VVMU „N. Y. Vaptsarov“ [in Bulgarian].

ROGAN-FINNEMORE, M. et al., 2021. Icebreaking polar class research vessels: New Antarctic fleet capabilities. *Polar Record*, vol. 57(e46).

SZALKAI, P., 2024. The Unique Environmental Features of the Arctic That Affect Military Capabilities. *HDR*, № 1-2, pp. 108-121.

TILL, G., 2018. *Seapower: A Guide for the 21st Century*. 4th ed. London: Routledge. ISBN 978-1138657670.

VEGO, M., 2009. *Joint Operational Warfare: Theory and Practice*. Newport: U.S. Naval War College.

INFLUENCE OF SPATIAL-TEMPORAL FACTORS, THE HYDROMETEOROLOGICAL ENVIRONMENT, AND LOGISTICAL DEFICITS ON OPERATIONAL CAPABILITIES DURING LONG-DISTANCE POLAR SAILINGS

Abstract. The report presents an empirical study based on direct command experience from the historic maiden voyage of the Bulgarian naval research vessel to Antarctica and the subsequent annual expeditions for capability enhancement. The executed transoceanic missions mark an unprecedented paradigm shift in the development of the Naval Forces, defining the transition from operating in closed maritime theaters to generating a presence in the World Ocean and remote regions. The complex impact of spatial-temporal and extreme hydrometeorological factors on platform resilience is analyzed. The challenges of exploitation under conditions of extreme distance and hindered logistical support are examined, necessitating the maintenance of absolute autonomy due to the lack of established coastal infrastructure. Based on real operational conditions, an optimized management model is proposed for risk minimization and institutional adaptation of defense and security systems.

Keywords: logistical deficit; long-distance sailings; operational capabilities; polar expeditions; risk management; spatial-temporal factors

Captain (N) Nikolay Danailov
Nikola Vaptsarov Naval Academy
73, Vasil Drumev St.
Varna 9002, Bulgaria
E-mail: n.danailov@nvna.eu

https://doi.org/10. 66334/annu26_priprizagu

ПРИЧИНЕН ПРИНОС И ГРАНИЦИ НА ПРИЧИННИЯ ИЗВОД ПРИ ИЗСЛЕДВАНЕТО НА РЕАЛИЗИРАНИ ЗАГУБИ В ОБЛАСТТА НА НАЦИОНАЛНАТА СИГУРНОСТ

доц. д-р инж. Николай Илиев
Национален военен университет „Васил Левски“

Абстракт. Изследването разглежда причинния анализ като самостоятелна операция след установяването на неблагоприятно изменение и се съсредоточава върху границата между фактическа последователност, причинна свързаност и доказуем причинен принос. Целта е да се предложи приложима постановка за формулиране на причинни изводи при многофакторни развития, релевантни за националната сигурност. Използвани са системен анализ, причинно и времево проследяване, съпоставка на методологични постановки и аналитична реконструкция. Разграничени са причина, условие, задействащ фактор, междинно състояние и последващ резултат. Предлага се проверка на причинния принос чрез пет аналитични позиции, обхващащи времева съвместимост, механизъм на предаване, действащи условия, конкуриращи се обяснения и доказателствен предел. Основният резултат е правило, което свързва силата на причинния извод с доказателствената основа и ограничава приписването до доказания причинен принос.

Ключови думи: загуба; причинност; причинен принос; национална сигурност; доказателствен предел

1. Въведение

При изследването на реализирани загуби в областта на националната сигурност въпросите какво фактически е настъпило и защо е настъпило имат различен аналитичен предмет. Неблагоприятното изменение може да бъде надеждно установено по отношение на конкретен ресурс, функция или друга позиция, докато причинната му реконструкция може да остане частична. Възможна е и ситуация, при която релевантният фактор е известен, а доказателствата позволяват само ограничено отнасяне на последващия резултат към него. Поради това причинният анализ се разглежда като самостоятелна проверка след установяването на загубата.

Проблемът се комплицира при сложни и взаимнозависими системи, в които едновременно действат технически, човешки, организационни, информационни и фактори на средата. ISO 31000 допуска едно събитие да има множество причини и множество последствия, а съвременните постановки за риска отделят събитието, последствията и неопределеността като различими елементи на анализа (Aven 2016).[1] Класическата постановка на Kaplan и Garrick свързва пълното описание на риска със сценария, вероятността и последствията (Kaplan & Garrick 1981). В приложните оценки Националният институт по стандарти и технологии на САЩ проследява риска чрез заплахи, уязвимости, предразполагащи условия и въздействия, което подкрепя разграничаването на отделните причинни роли[2].

Съществуващите подходи осигуряват средства за отделни части на причинния анализ. Самостоятелният методологичен проблем възниква при определянето на границата, до която причинният извод може да бъде разширен след вече установено неблагоприятно изменение. При многофакторни и взаимнозависими развития тази граница зависи от времевата съвместимост, механизма, действащите условия, алтернативните обяснения и доказателствения предел. Именно съвместното им разглеждане формира фокуса на настоящото изследване (Pearl 2009; Halpern 2016; Rinaldi, Peerenboom & Kelly 2001).

Целта му е да се формулира приложима методологична постановка за установяване на причинния принос на конкретна реализирана загуба или друг релевантен фактор към последващо неблагоприятно състояние. Научният въпрос е при какви условия причинната свързаност позволява обоснован причинен извод, съответстващ на наличната доказателствена основа. Тезата е, че времевата последователност и наличието на зависимост дават начални ориентири, а обоснованият причинен принос се формира

чрез съвместна проверка на механизма, действащите условия, конкуриращите се обяснения и доказателствения предел (Kaplan & Garrick 1981; Pearl 2009; Halpern 2016).

За целите на анализа реализираната загуба се използва в операционен смисъл като фактически установено неблагоприятно изменение на определим носител (референт) или на релевантна негова характеристика спрямо фактическо сравнително състояние. Причинната проверка започва след установяването на това изменение и е насочена към обяснението на последващото състояние. Използван е концептуален и сравнителен анализ на постановки от теорията на причинността, анализа на риска, аварийната отчетност и инфраструктурните взаимозависимости, от които са изведени общи контролни условия за формулиране на причинен извод.

2. Условия за причинен извод след установена загуба

Установяването на причинна връзка запазва аналитичната идентичност на свързаните изменения. Ако първоначална загуба поражда последващо функционално ограничение, двете позиции могат да бъдат причинно свързани и едновременно да останат различими по референт, характеристика, време и равнище. Това разграничение е особено важно при каскадни процеси. Изследванията на инфраструктурните взаимозависимости показват, че промяна в една система може да се предава към други чрез физически, кибернетични, географски или логически зависимости (Rinaldi, Peerenboom & Kelly 2001). Наличието на зависимост очертава възможния път на разпространение, а фактическото му активиране и приносът към целевия резултат се установяват отделно.

Причинният анализ започва с точно индивидуализиране на състоянието, което подлежи на обяснение. Определят се референтът, времевият интервал и съдържанието на наблюдаваното изменение. Тази начална фиксация държи причинното проследяване в границите на конкретния резултат и отделя непосредственото въздействие, условията за разпространение, управленските решения и последващите ефекти.

В причинната структура се разграничават пет основни позиции: разглеждан причинен фактор; условия, които позволяват, ограничават или усилват действието му; непосредствен задействащ момент, когато такъв може да бъде отделен; механизъм на предаване и установен резултат. Отделният случай може да съчетава някои от тези позиции, като аналитичната им функция остава различима. Така условието, времевото предхождане

и причинният механизъм запазват собственото си значение. Подобна дисциплина е съвместима с разграничението между обща причинна структура и “actual causality”, при което се проверява ролята на конкретни фактори в конкретно реализиран резултат (Pearl 2009; Halpern 2016).

Практическите системи за регистриране и надзор също разграничават причинните фактори от последствията. Европейската система eMARS организира информацията за големи промишлени аварии така, че причинните фактори, обстоятелствата и човешките, екологичните и други последствия да могат да се проследяват разграничено[3]. В банковото регулиране загуби, породени от общ основен тригер или root cause, могат да бъдат групирани за определени цели, като общият причинен произход се съчетава с ясно определяне на отделните записи[4]. Същият принцип е приложим и при изследването на загуби в областта на националната сигурност, където един факт може да участва в няколко аналитични линии с различна роля.

3. Причинен принос при многофакторни развития

При многофакторно развитие формулировката „А причини Б“ е обоснована в степента, в която доказателствата установяват ролята на А за достигането на Б. Поради това като работна категория се използва „причинен принос“. Той означава доказуемо участие на фактор, загуба или конфигурация във формирането на определен резултат, като обхватът и силата на това участие се определят според доказателствената основа.

Тази постановка позволява да се запази причинният извод и когато действат съпричинители. Прекъсването на инфраструктурна услуга може да бъде свързано с физическо увреждане, но продължителността и мащабът му да зависят и от достъпа до резервни ресурси, състоянието на други инфраструктури и организацията на възстановяването. Изследванията на инфраструктурните взаимозависимости показват, че функционалните ефекти могат да се пренасят през физически, кибернетични, географски и логически зависимости (Rinaldi, Peerenboom & Kelly 2001; Ouyang 2014). При такава структура приписването на целия последващ резултат на един първоначален фактор би надхвърлило доказаното.

Причинният принос се разграничава от корелацията. В системи с множество взаимозависимости две изменения могат да се наблюдават едновременно поради общ външен фактор, а времевото предхождане може да съвпадне с действие на трета позиция. Времевата последователност служи като ориентир, докато обоснованият причинен извод изисква механизъм,

който прави прехода между състоянията обясним и проверим, както и съпоставка с конкуриращи се обяснения.

Важно е да се отчита и ролята на интервенциите. След първоначална загуба може да бъде взето решение за преразпределяне на ресурси, ограничаване на дейност, заместване или промяна на организацията. Тези решения са последващи фактори и изменят развиващата се причинна структура. Анализите на аварията във „Фукушима Даиичи“ показват многофакторно развитие, в което природното въздействие, техническите зависимости, предварителните уязвимости и последващото аварийно управление имат различни причинни роли[5,6]. Крайното състояние след интервенцията се обяснява чрез съвместното действие на първоначалното въздействие и последващите решения.

4. Проверка на причинния принос

Проверката започва с времевата съвместимост между разглеждания фактор и целевото състояние. Установяват се времевият ред и интервалът, в който факторът може да участва във формирането на резултата. След това се проследява механизмът на предаване – процесът, чрез който въздействието достига до целевото състояние. При физическо въздействие този преход може да бъде кратък, докато организационните, информационните и инфраструктурните процеси често включват поредица от междинни състояния. С увеличаването на междинните звена нараства и необходимата конкретност на доказателствата за всеки преход.

Следващата част на проверката обхваща условията, при които механизмът действа. Уязвимостта, натоварването, наличният резерв, организационната конфигурация и зависимостта от други системи могат да усилят, ограничат или променят причинния процес. Тяхната роля се определя според фактическото им участие в случая. Паралелно се разглеждат и конкуриращите се обяснения – други събития, решения, общи причини или съвместни въздействия, които могат да участват във формирането на същия резултат.

Завършващата позиция е доказателственият предел. Той свързва съдържанието на заключението с действително установеното участие на разглеждания фактор. Резултатът може да определи установен причинен принос, ограничен причинен принос или доказателствено неопределен причинен статус. По този начин силата на формулировката следва силата на доказателствата, а причинният извод остава конкретен по отношение на фактор, механизъм, резултат и времеви обхват.

В практическо приложение проверката образува свързана последователност: целево състояние → времева съвместимост → механизъм → действащи условия и алтернативни обяснения → доказателствен предел. Последователността позволява причинният принос да бъде формулиран с точния обхват, който доказателствата поддържат, включително при многофакторни развития и частично проследен причинен механизъм.

5. Значение за изследването на загуби в областта на националната сигурност

Предложената постановка е приложима при оценяването на каскадни последствия. Когато първоначално изменение се разпространява между взаимозависими системи, анализът разграничава възможния път от фактически реализирания преход. NIST поставя акцент върху зависимостите, услугите и възстановяването и показва, че каскадните прекъсвания могат да засягат физически и обществени системи, като конкретното отражение се установява чрез фактическото функциониране (McAllister 2015). Определенията за каскадни бедствия също подчертават последователността на взаимодействията и разширяването на последствията, а доказаният причинен път се извежда от фактическите преходи (Pescaroli & Alexander 2015).

Втора приложна област са човешките и организационните загуби, при които монокаузалното обяснение често обхваща само част от причинната структура. Индивидуалното състояние, продължителността на експозицията, своевременността на реакцията, наличната информация и медицинските или организационните действия могат да формират различни причинни конфигурации. Общият причинен фактор тогава има определим принос, чийто обхват се установява отделно за конкретните резултати.

Третата ситуация е оценяването на решения след загуба. Когато системата запази функция чрез заместване или преразпределяне, първоначалната загуба остава факт, а крайният резултат включва и действието на последващата интервенция. Причинният анализ отделя приноса на първоначалната загуба от приноса на решението. Така извличането на поуки отчита едновременно значимостта на първоначалното нарушение и ефекта от предприетата реакция.

В този смисъл причинният принос изпълнява ограничаваща функция. Системната динамика допуска обратни връзки, закъснения и множество пътища между първоначалното изменение и наблюдавания резултат, поради което причинното обяснение запазва времевата и структурната

конкретност на случая (Sterman 2000). Подходите към устойчивостта допълнително показват, че реакцията, възстановяването и адаптацията могат да изменят последващото състояние, като първоначалната загуба запазва фактическия си статус (Woods 2015). Силата на причинния извод следва доказателствената основа и ясно определената роля на останалите фактори.

6. Заключение

Причинният анализ на загубите изисква разграничаване между установеното неблагоприятно изменение и обяснението за неговото възникване и последващо отражение. Времевата линия, зависимостта между системни елементи и механизмът изпълняват допълващи роли, а обоснованият причинен извод се формира чрез съвместното им разглеждане в конкретния доказателствен обхват.

Основният резултат е проверка чрез пет аналитични позиции, която организира причинния извод чрез времева съвместимост, механизъм на предаване, действащи условия, конкуриращи се обяснения и доказателствен предел. Ограничителното правило свързва силата на заключението с доказания причинен принос и изисква допълнителна доказателствена основа за твърдения относно единствена, достатъчна или доминираща причина. Така причинността се включва в анализа на реализирани загуби при запазване на аналитичната идентичност на отделните изменения и точната граница на допустимия извод.

БЕЛЕЖКИ

1. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO), 2018. ISO 31000:2018 Risk management – Guidelines. 2nd ed. Geneva: ISO.

2. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), 2012. Guide for Conducting Risk Assessments. NIST SP 800-30 Rev. 1. Gaithersburg, MD: NIST.

3. EUROPEAN COMMISSION, JOINT RESEARCH CENTRE (JRC), 2026. eMARS – Major Accident Reporting System. Available on: https://emars.jrc.ec.europa.eu/ [viewed: 26.07.2026].

4. BASEL COMMITTEE ON BANKING SUPERVISION, 2026. Basel Framework, OPE25 – Operational risk, para. 25.29 and related FAQ on grouping operational losses caused by a common underlying trigger/root cause. Updated 23 March 2026.

5. INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA), 2015. The Fukushima Daiichi Accident. Technical Volume 1/5: Description and Context of the Accident. Vienna: IAEA.

6. THE NATIONAL DIET OF JAPAN, FUKUSHIMA NUCLEAR ACCIDENT INDEPENDENT INVESTIGATION COMMISSION, 2012. The Official Report of the Fukushima Nuclear Accident Independent Investigation Commission: Executive Summary. Tokyo.

ЛИТЕРАТУРА

AVEN, T., 2016. Risk Assessment and Risk Management: Review of Recent Advances on Their Foundation. *European Journal of Operational Research*, vol. 253, no. 1, pp. 1 – 13.

HALPERN, J. Y., 2016. *Actual Causality*. Cambridge, MA: MIT Press. DOI: 10.7551/mitpress/9780262035026.001.0001.

KAPLAN, S. & GARRICK, B. J., 1981. On the Quantitative Definition of Risk. *Risk Analysis*, vol. 1, no. 1, pp. 11 – 27. DOI: 10.1111/j.1539-6924.1981.tb01350.x.

MCALLISTER, T. P., 2015. *Community Resilience Planning Guide for Buildings and Infrastructure Systems, Volume II*. NIST SP 1190v2. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.1190v2.

OUYANG, M., 2014. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, vol. 121, pp. 43 – 60. DOI: 10.1016/j.ress.2013.06.040.

PEARL, J., 2009. *Causality: Models, Reasoning, and Inference*. 2nd ed. Cambridge: Cambridge University Press.

PESCAROLI, G. & ALEXANDER, D., 2015. A Definition of Cascading Disasters and Cascading Effects: Going Beyond the “Toppling Dominos” Metaphor. *Planet@Risk*, vol. 3, no. 1, pp. 58–67.

RINALDI, S. M.; PEERENBOOM, J. P. & KELLY, T. K., 2001. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, vol. 21, no. 6, pp. 11 – 25. DOI: 10.1109/37.969131.

STERMAN, J. D., 2000. *Business Dynamics: Systems Thinking and Modeling for a Complex World*. Boston: Irwin/McGraw-Hill.

WOODS, D. D., 2015. Four Concepts for Resilience and the Implications for the Future of Resilience Engineering. *Reliability Engineering & System Safety*, vol. 141, pp. 5 – 9.

CAUSAL CONTRIBUTION AND THE LIMITS OF CAUSAL INFERENCE IN THE STUDY OF REALIZED LOSSES IN THE FIELD OF NATIONAL SECURITY

Abstract. The study treats causal analysis as a distinct operation following the identification of an adverse change and focuses on the boundary between temporal sequence, causal linkage, and demonstrable causal contribution. Its aim is to formulate an applicable approach to causal inference in multifactor developments relevant to national security. The analysis distinguishes cause, enabling condition, trigger, transmission mechanism, intermediate

state, and subsequent result. A five-part causal contribution check is proposed, covering temporal compatibility, transmission mechanism, operating conditions, competing explanations, and the evidentiary limit of the inference. The main result is an evidentiary rule that aligns the strength of the causal conclusion with the demonstrated causal contribution.

Keywords: loss; causality; causal contribution; national security; evidentiary limit

Dr. Nikolay Iliev, Assoc. Prof.
Department of Military Sciences
Faculty of Security and Defence
Vasil Levski National Military University
76, Bulgaria Blvd.
5000 Veliko Tarnovo, Bulgaria
E-mail: ntiliev@nvu.bg

https://doi.org/10. 66334/annu26_confirealoss

КОНФИГУРАЦИИ ОТ РЕАЛИЗИРАНИ ЗАГУБИ И КОНТРОЛ СРЕЩУ ДВОЙНО ОТЧИТАНЕ В ОБЛАСТТА НА НАЦИОНАЛНАТА СИГУРНОСТ

доц. д-р инж. Николай Илиев
Национален военен университет „Васил Левски“

Абстракт. Изследването разглежда методологичния проблем за анализ на няколко едновременно или последователно установени загуби, когато между тях съществуват зависимости, причинни отношения или общи последствия. Целта е да се предложи контролна процедура за разграничаване на конфигурационния ефект, механичното сумиране на индивидуални загуби и повторното отчитане на една и съща фактическа основа на различни аналитични равнища. Използвани са системен и сравнителен анализ, проследяване на взаимозависимости и причинни отношения и синтез на приложими контролни правила. Разграничени са съвместно наличие, натрупване, причинна последователност, взаимозависимост и конфигурационен принос. Предлага се контролна последователност от шест аналитични позиции, основана на индивидуализация на всяка загуба, определяне на отношенията, отделяне на общите резултати, проследяване на междинните механизми, контрол върху повторното използване на фактическата основа и определяне на системната и времевата валидност. Резултатът е приложима рамка за прецизно оценяване на сложни загубни конфигурации с контрол върху двойното отчитане.

Ключови думи: загуба; конфигурация; взаимозависимост; двойно отчитане; национална сигурност

1. Въведение

В областта на националната сигурност неблагоприятните изменения рядко се проявяват като напълно изолирани събития. Един инцидент може да засегне няколко ресурса; загуба в една инфраструктура може да ограничи друга; последващо решение може да преразпредели натоварването и да създаде нови ограничения. При подобни развития възниква аналитичен проблем: кога няколко установени загуби образуват релевантна конфигурация и кога описанието им всъщност повтаря една и съща фактическа основа с различни наименования.

Изследванията на критичните инфраструктури показват, че системите могат да бъдат свързани чрез физически, кибернетични, географски и логически взаимозависимости, а моделите на взаимозависими мрежи показват и възможност за нелинейно каскадно разпространение (Rinaldi et al. 2001; Buldyrev et al. 2010; Ouyang 2014). При сложни инфраструктурни конфигурации отделни откази могат да се разпространяват по структурни и функционални връзки, но фактическият каскаден път следва да бъде разграничен от потенциалната мрежа на зависимостите (Dueñas-Osorio & Vemuru 2009; Pescaroli & Alexander 2015).

Съществуващите направления решават отделни части на този проблем: изследванията на взаимозависимостите проследяват пътищата на разпространение, методиките за бедствия разделят различни видове щети и загуби, операционният риск допуска групиране по общ причинен произход, а системите за интеграция на данни поставят изисквания за идентичност и проследимост на записите. Общият методологичен въпрос е как тези позиции да бъдат разглеждани съвместно при еднократно отчитане на всяка фактическа основа. Този контролен проблем определя самостоятелния фокус на настоящото изследване[1, 2] (Caetano et al. 2026).

Коректният анализ изисква всяка загубна позиция да се основава на различимо неблагоприятно изменение. Когато една и съща фактическа основа се представя последователно като компонентна, функционална и системна загуба, тя следва да бъде проследена като един факт с различни аналитични проявления. Същевременно общата причина може да свързва няколко действително различими загуби, които запазват самостоятелния си статут. Така контролът обхваща едновременно риска от завишаване чрез повторно отчитане и риска от прекомерно обединяване на отделни загубни позиции.

Целта на настоящото изследване е да предложи контролна процедура за анализ на конфигурации от вече индивидуализирани реализирани загуби. Научният въпрос е при какви условия съвместното наличие и взаимодействието между няколко загуби обосновават конфигурационен извод и как се осигурява еднократно отчитане на фактическата основа. Тезата е, че конфигурационният принос се установява чрез доказани отношения между самостоятелни загубни позиции и общо целево състояние, като броят на позициите и аритметичното им събиране изпълняват само помощна роля (Rinaldi et al. 2001; Ouyang 2014; Pescaroli & Alexander 2015).

За целите на анализа реализирана загуба се използва като фактически установено неблагоприятно изменение на определим носител (референт) или негова релевантна характеристика спрямо фактическо сравнително състояние. Входът на конфигурационния анализ е съвкупност от две или повече такива позиции. Чрез сравнителен анализ на решенията за взаимозависимости, каскадни процеси, оценка след бедствия, групиране на операционни загуби и интеграция на данни се извеждат критерии за идентичност, отношение, общ резултат и повторно използване на една и съща фактическа основа. Предназначението на процедурата е да установи основанията за съвместно разглеждане на хетерогенни загуби преди евентуално количествено агрегиране.

2. Кога множество загуби образуват аналитична конфигурация

Конфигурацията от загуби се разбира тук като съвкупност от две или повече индивидуализирани загуби, между които е установено аналитично релевантно отношение за разглеждания системен резултат. Определението поставя две условия: всяка позиция има самостоятелна доказателствена основа като реализирана загуба, а съвместното им разглеждане се обосновава чрез конкретно отношение помежду им. Така времевата близост служи като характеристика на конфигурацията, докато аналитичното ѝ значение се извежда от установените зависимости и резултати.

Това позволява да се разграничат няколко типа отношения. При съвместно наличие загубите споделят общ времеви интервал, а отношението се ограничава до времевото им съвпадение. При натрупване всяка загуба допринася към общо ограничение. При причинна последователност една загуба участва в механизма за възникване на друга. При взаимозависимост състоянието на една система или функция изменя възможността друга да работи или да се възстановява. При конфигурационен принос именно съ-

четаването на загубите и отношенията между тях е релевантно за целевия резултат.

Отделните отношения могат да се съчетават в една конфигурация. Две инфраструктурни загуби например могат едновременно да са взаимозависими и да участват в причинна последователност. Аналитичната задача е да се посочи кое отношение е доказано и какво значение има за разглеждания резултат. Така конфигурацията функционира като проверима структура от самостоятелни позиции и установени връзки.

Особено важно е разграничението между конфигурация и агрегация. Агрегацията събира величини според предварително определено правило, докато конфигурационният анализ установява отношения между самостоятелни позиции. Простото събиране има съдържателен смисъл при съпоставими референти, мерни единици и ясно определено правило за агрегиране. Изследванията на инфраструктурните зависимости и системната устойчивост показват, че съвместното действие може да поражда нелинейни и времево изменящи се резултати (McAllister 2015; Ouyang 2014). Конфигурационният принос поради това се доказва за конкретната съвкупност и конкретното целево състояние.

3. Основни механизми на двойно отчитане

Двойното отчитане възниква, когато една и съща фактическа основа участва повече от веднъж в крайния аналитичен резултат и ролята ѝ се смесва с други аналитични позиции. В анализа на загубите могат да се отделят поне четири механизма.

Първият механизъм е вертикалното двойно отчитане между аналитични равнища. Физическата загуба на компонент може да доведе до функционално ограничение, а то – до ограничение на способност. Трите позиции описват различни равнища на една причинно свързана верига. Количественото им агрегиране е обосновано само когато всяка величина измерва самостоятелен резултат и методът определя начина на съвместното им използване.

Вторият механизъм е хоризонталното двойно отчитане. Един ресурсен недостиг може да бъде описан като материална загуба, логистично ограничение и фактор за изпълнението на задача. Когато трите описания се отнасят до един и същ факт, те се регистрират като различни аналитични роли на една фактическа позиция. Това запазва съдържанието на всяко описание и еднократното участие на факта в общия резултат.

Третият механизъм възниква при каскадни процеси. Първоначалната и последващата загуба са различими, а част от крайния резултат може вече да е включена в оценката на предходна позиция. Контролът проследява къде конкретният ефект участва за първи път и как се пренася към следващото равнище. Подобен проблем възниква при оценяване на икономически загуби от инфраструктурни прекъсвания, когато преки, косвени и зависимостно породени ефекти се припокриват (Kelly 2015). Методологиите за оценка след бедствия отделят физическите щети, измененията на икономическите потоци и потребностите от възстановяване, с което запазват съдържателната различимост на величините[3, 4].

Четвъртият механизъм е повторното използване на общ причинен фактор като самостоятелна загубна позиция. Няколко загуби могат да произтичат от едно събитие, а причинителят изпълнява обяснителна функция спрямо отделните резултати. В практиката по операционен риск загуби с общ *underlying trigger/root cause* могат да бъдат групирани за конкретни регулаторни цели, като отделните записи запазват собствената си идентичност[5]. По сходна логика системите за данни за бедствия разграничават събитието, засегнатите елементи и регистрираните загуби[6, 7].

Функцията на контрола срещу двойно отчитане е да осигури точно участие на всяка фактическа позиция в крайния аналитичен резултат според ролята, която доказателствата поддържат.

4. Контрол при анализ на конфигурацията

Фигура 1 представя шестте взаимосвързани позиции на контрола – от индивидуализирането на загубите до определянето на системната и времевата валидност на общия извод.

Контролът започва с индивидуализиране на всяка загубна позиция чрез непосредствения референт, засегнатата характеристика, сравнителното състояние и времевия интервал. Съвременните подходи към интеграцията на данни за загуби показват, че семантичното разграничаване на обекта, вида на изменението, времето и източника са предварително условие за коректно съвместно използване на данни (Caetano et al. 2026). Съвпадащата фактическа основа насочва към една позиция, а различимите изменения получават самостоятелна регистрация.

След индивидуализацията се определя отношението между загубите – съвместно наличие, натрупване, причинна зависимост, взаимозависимост или друга установима връзка. Типологиите на инфраструктурните взаимо-

зависимости подпомагат разпознаването на възможните отношения, а конкретният случай определя фактически реализираната връзка (Rinaldi et al. 2001). Когато няколко позиции участват в общ функционален или системен резултат, този резултат се отделя като самостоятелна целева позиция и се свързва с доказаните приноси на отделните загуби.



Фигура 1. Контролна последователност при анализ на конфигурации от реализирани загуби *(Източник: авторска разработка)*

Проследяването продължава през междинните механизми. Каскадното разпространение се разлага на проверими преходи, което е особено важно при инфраструктурни системи и зависимости между услуги (McAllister 2015; Mednikarov et al. 2007). Паралелно се извършва контрол върху повторното използване на факт, недостиг, причинен принос, механизъм или резултат. Вече отчетената фактическа позиция участва в следващите операции като връзка или основание, а количественият ѝ принос се включва еднократно.

Завършващата позиция определя системната и времевата валидност на конфигурационния извод. Възстановяването на функция, въвеждането на заместител или промяната на зависимост може да преобразува отношенията между загубите и съответно обхвата на общия резултат. Шестте

позиции формират контролна процедура, която предхожда количественото оценяване и определя съдържателно съвместимите елементи за последващо агрегиране.

5. Конфигурационен принос при съвместно действие на загуби

Конфигурационният принос се установява, когато съчетаването или отношението между няколко загуби има доказуемо значение за целевото състояние. Той има самостоятелно аналитично основание и може да се различава от аритметичния сбор на индивидуалните приноси. В една система две относително ограничени загуби могат да засегнат различни резервни линии и съвместно да доведат до прекъсване на функция. В друга система тежка компонентна загуба може да бъде функционално компенсирана и да произведе ограничено системно отражение. Поради това конфигурационният анализ се насочва към фактически действащите зависимости и остатъчната конфигурация.

Подходите към устойчивостта насочват наблюдението към функционалното състояние във времето и към връзката му с физическото увреждане. Bruneau et al. свързват устойчивостта с изменението и възстановяването на функционалността, а Woods разграничава различни форми на устойчиво и адаптивно поведение (Bruneau et al. 2003; Woods 2015). Управлението на критичната инфраструктурна устойчивост също изисква отчитане на взаимозависимостите, продължителността на прекъсването и приоритетите за възстановяване[8]. За анализа на конфигурации това означава, че една и съща изходна съвкупност може да има различно отражение според времето, резервите и последващата реорганизация.

Наличието на взаимозависимости очертава карта на потенциални преходи, а системният резултат се определя чрез фактически активираните връзки. NIST отбелязва, че физическите инфраструктури и обществените услуги могат да бъдат свързани чрез множество зависимости и че каскадните прекъсвания могат да засягат различни сектори (McAllister 2015). В този контекст конфигурационният принос се извежда от конкретно реализираното разпространение и достигнатото целево състояние.

Това разграничение има пряко значение при вземане на решения. Контролът действа двупосочно: ограничава завишаването на резултата чрез повторно отчитане и подпомага откриването на зависимости, които придобиват значение при съвместно отпадане на няколко позиции. По този

начин приоритизирането на ресурси може да се основава както на индивидуалните загуби, така и на доказания им конфигурационен принос.

6. Приложимост към анализа на националната сигурност

Предложената процедура е приложима при хетерогенни загуби, като запазва специфичните им мерни единици и предметно съдържание. Човешка, материална, информационна и организационна загуба могат да бъдат разглеждани в обща конфигурация при установено участие в един и същ целеви резултат. Така системният анализ се основава на отношенията между позициите и допуска количествено агрегиране само при съдържателно съвместими величини.

При анализ на способности процедурата свързва компонентните загуби с фактическото състояние на функцията, задачата и необходимия резултат. Няколко компонентни загуби могат да имат конфигурационен принос към ограничаването на функция или задача, когато фактическото състояние на целевия резултат потвърждава тази връзка. Наличието на остатъчни ресурси, от своя страна, придобива значение чрез начина, по който тяхната конфигурация осигурява необходимото функциониране.

При критична инфраструктура процедурата разграничава прякото увреждане от зависимостно породеното прекъсване. Физически запазен обект може да загуби функция поради отпадане на електрозахранване, комуникации или транспортен достъп. Съвременните рамки за инфраструктурна устойчивост изискват проследяване на зависимостите и на услугите, които трябва да бъдат поддържани или възстановени[9, 10]. Физическата загуба в една система и функционалната загуба в друга се запазват като различими, причинно свързани позиции, а крайният резултат се отчита еднократно в съответната целева позиция.

При последващо възстановяване конфигурацията се актуализира спрямо новото фактическо състояние. Възстановяването на една зависимост може да прекъсне каскадния механизъм, докато първоначално загубеният компонент остава в предходното си състояние. Конфигурационният извод поради това има собствена времева валидност и се преразглежда при промяна на фактическите отношения.

7. Заключение

Анализът на множество загуби изисква разграничаване между съвместно наличие, натрупване, причинна последователност, взаимозависи-

мост и конфигурационен принос. Единна аналитична конфигурация се формира чрез доказани отношения между самостоятелните загубни позиции и тяхното участие в общо целево състояние.

Основният резултат е контролна последователност от шест аналитични позиции, която започва с индивидуализиране на всяка загуба и завършва с определяне на системната и времевата валидност на общия извод. Между тях се установяват отношенията, общите резултати, междинните механизми и повторното използване на една и съща фактическа основа. Конфигурационният принос се доказва чрез отношенията между загубите и фактическото им участие в целевото състояние. Така процедурата едновременно ограничава завишаването чрез двойно отчитане и подпомага откриването на действително реализирани системни взаимодействия.

БЕЛЕЖКИ

1. ECONOMIC COMMISSION FOR LATIN AMERICA AND THE CARIBBEAN (ECLAC), 2014. Handbook for Disaster Assessment. Santiago: United Nations.

2. BASEL COMMITTEE ON BANKING SUPERVISION, 2026. Basel Framework, OPE25 – Operational risk, para. 25.29 and related FAQ on grouping operational losses caused by a common underlying trigger/root cause. Updated 23 March 2026.

3. ECONOMIC COMMISSION FOR LATIN AMERICA AND THE CARIBBEAN (ECLAC), 2014. Handbook for Disaster Assessment. Santiago: United Nations.

4. EUROPEAN UNION; WORLD BANK; UNITED NATIONS DEVELOPMENT GROUP, 2013. Post-Disaster Needs Assessments: Volume A – Guidelines. [online]. Available from: https://www.gfdrr.org/en/publication/post-disaster-needs-assessments-guidelines-volume-2013. [last viewed: 13 January 2025].

5. BASEL COMMITTEE ON BANKING SUPERVISION, 2026. Basel Framework, OPE25 – Operational risk, para. 25.29 and related FAQ on grouping operational losses caused by a common underlying trigger/root cause. Updated 23 March 2026.

6. UNITED NATIONS OFFICE FOR DISASTER RISK REDUCTION (UNDRR), n.d. DELTA Resilience: Disaster Losses and Damages Tracking System. [online]. Available from: https://www.undrr.org/building-risk-knowledge/disaster-losses-and-damages-tracking-system-delta-resilience. [last viewed: 7 July 2025].

7. UNITED NATIONS OFFICE FOR DISASTER RISK REDUCTION (UNDRR), 2017. Technical Guidance for Monitoring and Reporting on Progress in Achieving the Global Targets of the Sendai Framework for Disaster Risk Reduction 2015–2030. Geneva: UNDRR.

8. OECD, 2019. Good Governance for Critical Infrastructure Resilience. OECD Reviews of Risk Management Policies. Paris: OECD Publishing. DOI: 10.1787/02f0e5a0-en.

9. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), 2025. Infrastructure Resilience Planning Framework (IRPF). March 2025. [online]. Available from: https://www.cisa.gov/sites/default/files/2025-03/IRPF_3.17.2025.pdf. [last viewed: 1 June 2026].

10. OECD, 2019. Good Governance for Critical Infrastructure Resilience. OECD Reviews of Risk Management Policies. Paris: OECD Publishing. DOI: 10.1787/02f0e5a0-en.

REFERENCES

BRUNEAU, M.; CHANG, S.; EGUCHI, R.; LEE, G.; O'ROURKE, T.; REINHORN, A.; SHINOZUKA, M.; TIERNEY, K.; WALLACE, W. & VON WINTERFIELDT, D., 2003. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra*, vol. 19, no. 4, pp. 733 – 752. DOI: 10.1193/1.1623497.

BULDYREV, S. V.; PARSHANI, R.; PAUL, G.; STANLEY, H. E. & HAVLIN, S., 2010. Catastrophic cascade of failures in interdependent networks. *Nature*, vol. 464, pp. 1025 – 1028. DOI: 10.1038/nature08932.

CAETANO, L.; SKEIE, K. S.; KIND, R.; TIME, B. & LUQUE, O., 2026. An Ontology-Centered Approach to Climate Loss Data Integration and Analytics. *International Journal of Disaster Risk Reduction*, vol. 137, pp. 1 – 16. DOI: 10.1016/j.ijdrr.2026.106096.

DUEÑAS-OSORIO, L. & VEMURU, S. M., 2009. Cascading failures in complex infrastructure systems. *Structural Safety,* vol. 31, no. 2, pp. 157 – 167. DOI: 10.1016/j.strusafe.2008.06.007.

KELLY, S., 2015. Estimating economic loss from cascading infrastructure failure: a perspective on modelling interdependency. *Infrastructure Complexity*, vol. 2, no. 7. DOI: 10.1186/s40551-015-0010-y.

MCALLISTER, T. P., 2015. *Community Resilience Planning Guide for Buildings and Infrastructure Systems*, vol. II. NIST SP 1190v2. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.1190v2.

MEDNIKAROV, B.; DIMITROV, N. & KALINOV, K., 2007. Applying the System Approach to the Study of Critical Infrastructure. *Information & Security: An International Journal,* vol. 22, pp. 138 – 150.

OUYANG, M., 2014. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, vol. 121, pp. 43 – 60. DOI: 10.1016/j.ress.2013.06.040.

PESCAROLI, G. & ALEXANDER, D., 2015. A Definition of Cascading Disasters and Cascading Effects: Going Beyond the "Toppling Dominos" Metaphor. *Planet@Risk,* vol. 3, no. 1, pp. 58 – 67. Davos: GRF. ISSN 2296-8172.

RINALDI, S. M.; PEERENBOOM, J. P. & KELLY, T. K., 2001. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, vol. 21, no. 6, pp. 11 – 25. DOI: 10.1109/37.969131.

WOODS, D. D., 2015. Four Concepts for Resilience and the Implications for the Future of Resilience Engineering. *Reliability Engineering & System Safety*, vol. 141, pp. 5 – 9.

CONFIGURATIONS OF REALIZED LOSSES AND DOUBLE-COUNTING CONTROL IN THE FIELD OF NATIONAL SECURITY

Abstract. The study addresses the methodological problem of analysing several simultaneous or sequential losses when dependencies, causal relations, or shared consequences exist between them. Its aim is to distinguish configurational effects, mechanical aggregation, and repeated use of the same factual basis across analytical levels. The study differentiates co-occurrence, accumulation, causal sequence, interdependence, and configurational contribution. A six-part control procedure is proposed: individual identification of each loss; verification of relations among losses; separation of shared outcomes; tracing of intermediate mechanisms; control over repeated use of the same fact, shortage, mechanism, or result; and determination of systemic and temporal validity. The main result is an analytical rule that derives configurational contribution from demonstrated relations and factual participation in the target state.

Keywords: loss; configuration; interdependence; double counting; national security

Dr. Nikolay Iliev, Assoc. Prof.
ORCID iD: 0009-0007-0215-7182
Security and Defence Faculty
Vasil Levski National Military University
76, Bulgaria Blvd.
5000 Veliko Tarnovo, Bulgaria
E-mail: ntiliev@nvu.bg

https://doi.org/10. 66334/annu26_cyberproch

УПРАВЛЯЕМОСТ В ЕРАТА НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ: КИБЕРНЕТИЧЕН ПРОЧИТ НА РИСКОВЕТЕ

д-р Николай Николов

Абстракт. Предлага се кибернетичен прочит на управляемостта в ерата на изкуствения интелект, изведен от закона на Ешби за необходимото разнообразие и теоремата на Конант – Ешби. Централната теза е, че сигурността е управляемост и информация, а управляемостта е съответствие между разнообразието на смущенията, и разнообразието на регулатора. Разгледани са два системни ефекта, които подкопават това съответствие: спонтанната синхронизация на популации от езикови модели по модела на Курамото, водеща до фазов преход над критичен праг и клъстеризация на изходите; и емерджентността в мрежите от свързани ИИ системи, която увеличава разнообразието на средата, „разкъсва“ вътрешния модел на регулатора и понижава разделителната му способност. Това позволява рисковете да се преразглеждат като атенюиране на разнообразието и се извежда принципът „усилване, а не концентрация“ като операционен подход.

Ключови думи: управляемост; кибернетика; закон на Ешби; модел на Курамото; синхронизация; емерджентност; изкуствен интелект; когнитивна сигурност

I. Увод

Съвременните пазари и информационни среди все по-често се използват не от хора, а от автономни ИИ агенти, които анализират, вземат решения и генерират съдържание в реално време. Класическата теория на управлението оценява една система по нейната управляемост, устойчивост, предвидимост и обхват на засегнатите отношения. Когато обектът на оценяване не е единичен модел, а нарастваща популация от взаимодействащи агенти, тези оценки губят релевантността си: свойствата на съвкупността не се свеждат до свойствата на отделния участник. Оттук възниква и водещият въпрос – доколко държавата, обществото и командването остават управляеми в среда, наситена с изкуствен интелект.

Тезата, която следва да бъде обоснована, е кибернетична: сигурността е управляемост и информация, а управляемостта е съответствие между разнообразието на смущенията и разнообразието на регулатора. Статията защитава тази теза, като анализира два слабо разпознати, но структурно определящи ефекта. Първият е спонтанната синхронизация на езиковите модели по модела на Курамото; вторият – емерджентността и възникващите ефекти в мрежите от свързани ИИ системи. И двата ерозират именно разнообразието, върху което почива управляемостта, и затова изискват преосмисляне на рисковете и на самата логика на управляващото въздействие.

II. Кибернетичната рамка: управляемост като съответствие на разнообразията

Изходната точка е законът на Ешби за необходимото разнообразие: само разнообразие може да поглъща разнообразие (Ashby 1956). Ако означим с $V(D)$ разнообразието на смущенията, с $V(R)$ – разнообразието на регулатора, и с $V(E)$ – остатъчното разнообразие на същностните променливи, законът приема вида (формула 1):

$$V(E) \geq V(D) - V(R) \qquad (1)$$

Смисълът е пряк: за да задържи същностните си променливи в допустими граници, регулаторът трябва да разполага с поне толкова разнообразие от реакции, колкото са различимите състояния на смущението. Допълва го теоремата на Конант – Ешби: всеки добър регулатор на една система трябва да бъде модел на тази система (Conant & Ashby 1970). Регу-

лиране без адекватен вътрешен модел е сляпо – регулаторът не разграничава състоянията, които трябва да управлява.

В тази рамка държавата, обществото и командването се разглеждат като регулатори, а управляемостта – като способността им да поддържат съответствие на разнообразията при нарастваща сложност на средата. Ешби посочва два и само два пътя за възстановяване на това съответствие, преработени приложно от Стафорд Биър (Beer 1979): усилване на разнообразието на регулатора и атенюиране на разнообразието на средата. Този дуализъм е аналитичната ос, по която по-нататък се разполагат както рисковете, така и отговорът.

III. Ефектът Курамото: спонтанна синхронизация на езиковите модели

Ефектът е често представян чрез познат физически експеримент: метрономи с различни начални фази, поставени върху обща подвижна платформа, стартират със случайно зададена начална фаза. Обменяйки малки количества енергия през платформата, след определено време те започват да се синхронизират. Синхронизацията не е програмирана в нито един метроном – тя е емерджентно свойство на свързаната система. Платформата играе ролята на общия обект, точно както пазарът или управляваната система свързват иначе независимите езикови модели (ИИ агенти).

Формално всеки модел се съпоставя на фазов осцилатор с естествена честота, а интензивността на споделяните данни – на силата на свързване. Третирането е обосновано: моделът на Курамото не изисква буквален осцилатор, а само вграден цикличен механизъм, задаващ темп на поведението – редуването на изследване и уточняване в генеративните процеси, балансът exploration–exploitation в обучението с подкрепление, gating-циклите в секвенционните архитектури (Kuramoto 1984; Strogatz 2000). Степента на колективна синхронизация се измерва с комплексния параметър на подреденост (формула 2):

$$r \cdot e^{i\psi} = (1/N) \cdot \Sigma_j \, e^{i\theta_j} \qquad (2)$$

Величината $r \in [0, 1]$ е модулът на средния фазов вектор: при пълна некохерентност $r \approx 0$, при пълна синхронизация $r = 1$. В средно-полевия вид силата на обратната връзка към всеки агент е пропорционална на вече постигнатата подреденост r, откъдето следва лавинообразният, самоусил-

ващ се характер на прехода. Съществува критична стойност на свързването (формула 3):

$$K_c = 2 / (\pi \cdot g(0)) \quad (3)$$

Под K_c единственото устойчиво състояние е некохерентното; над *Kc* некохерентността губи устойчивост и подреденост нараства скокообразно – фазов преход от втори род. За гаусово разпределение на честотите праговата стойност е $K_c \approx 1{,}60$ – стойност, която числените експерименти възпроизвеждат точно. Тук g(ω) е разпределението на естествените честоти: хомогенна екосистема (модели, обучени върху сходни корпуси и настроени сходно) има тясно g(ω), голямо g(0) и следователно нисък праг, т.е. синхронизира се лесно.

3.1. Резултати и системни следствия

Проведените числени експерименти образуват свързана верига: съществува ясно изразен праг; над него настъпва синхронизация във времето и в пространството на фазите; при разнородна популация синхронизацията се разпада на няколко вътрешно съгласувани клъстера при ниска глобална подреденост – количественият подпис на спонтанни „картели“; и, което е практически най-важно, синхронизация възниква дори без пряка връзка между агентите, само през общия управляван обект (в експериментите $r \approx 0{,}85$). Емпирично този режим вече е документиран при алгоритмичното ценообразуване, където самостоятелно обучаващи се агенти достигат колузивни равновесия без комуникация помежду си (Calvano et al. 2020).

Пренесен върху информационната среда, механизмът обяснява как синхронизирани модели могат съгласувано да усилват наративи и внушения в множество платформи. Тъй като все по-голям дял от търсенията и взаимодействията в мрежата се изместват към ИИ системи, синхронизираното им поведение придобива непропорционално влияние върху обществените нагласи – и директно захранва проблематиката на когнитивната война. Едновременно с това концентрацията на пазара около малък брой доставчици и корпуси стеснява g(ω), понижава прага и по този начин технически приближава средата към режим на глобална синхронизация – механизмът, който превръща зависимостта от качествата на доставените от външни организации на моделии, в загуба на цифров суверенитет.

Формалният анализ дава и конструктивен резултат: параметърът на подреденост *r* и езиково-специфичните му аналози (припокриване на теми,

свиване на дисперсията на стила, синхронно във времето реагиране на общи събития) са наблюдаеми отвън, без достъп до вътрешните състояния на моделите. Устойчивото им нарастване предопределя приближаване към критичния праг още преди самата манипулация да е настъпила – изпреварващ, а не закъснял индикатор за ранно предупреждение, приложим и спрямо системи получавани от трети страни.

IV. Емерджентност и възникващи ефекти в свързаните ИИ системи

Под емерджентност се разбира появата на свойство на цялото, което не е налично у частите и не се предвижда тривиално от техните локални правила, но е реално и причинно действено – то поражда ефекти, които обратно ограничават поведението на компонентите (нисходяща причинност). За аналитични цели се разграничават слаба емерджентност (изводима по принцип, но само чрез симулация) и силна (неизводима дори по принцип); за управлението разликата е второстепенна, защото и в двата случая регулаторът среща поведение, което не може да предвиди с наличния ресурс.

Емерджентността е възможно да се разглежда чрез следните разпознаваеми механизми: Първият е самоорганизацията далеч от равновесие: отворени системи, през които преминава постоянен поток от данни, могат спонтанно да породят подредени (дисипативни) структури, а малка флуктуация край точка на бифуркация да преведе цялото в качествено нов режим (Prigogine & Stengers 1984). Вторият е синхронизацията по Курамото – колективен ритъм без централен синхронизиращ компонент. Третият е фазовият преход: при плавно нарастване на един контролен параметър поведението се променя скокообразно; именно този профил се наблюдава при мащабирането на големите модели, където способности се появяват рязко над даден праг. За регулатора фазовият преход е най-неудобната форма на емерджентност, защото унищожава екстраполацията: миналото поведение престава да е надежден модел на бъдещото.

4.1. Отражението в апарата на Ешби

Емерджентността влошава баланса на разнообразията по три начина. Първо, тя увеличава *V(D)*: всеки нов емерджентен слой добавя различими колективни състояния, така че разнообразието на смущенията нараства не адитивно, а комбинаторно. Второ, тя разкъсва модела на Конант – Ешби: емерджентното свойство по дефиниция не се съдържа в модела на компонентите, затова регулатор, чийто модел описва частите, „не вижда“ поведението на цялото и реагира на два различни колективни режима по един и

същ начин. Трето, тя понижава разделителната способност: емерджентните преходи често са невидими за инструменти, калибрирани за нивото на компонентите − номиналното разнообразие на регулатора остава неизползваемо, защото той не разпознава кога да приложи реакциите си (капацитет без вход).

Съвременната ситуация е такава, че самите регулиращи технологии днес се свързват в мрежи и се превръщат в източник на емерджентност, а не само в инструмент за справяне с нея. Показателен случай е алгоритмичната колузия (Calvano et al. 2020): няма заговор в правния смисъл, а емерджентно колективно поведение, чийто резултат е еквивалентен на сговор без комуникация и умисъл. Към него се добавят синхронните информационни каскади, ята от автономни агенти и контурите на обратна връзка, при които обучението на едни модели върху изходите на други самоусилва отклоненията през екосистемата. Съществено е, че този риск е невидим на равнище компонент – всеки агент функционира изправно, а опасността живее в топологията на връзките. Свързаният ИИ измества локуса на риска от способностите на отделния модел към структурата на взаимодействието – измерение, което класическата оценка на единичен модел не улавя. Таблица 1 обобщава произтичащата пренастройка на кибернетичния апарат.

Таблица 1. Пренастройка на кибернетичния апарат от единичната система към емерджентния, свързан случай

Понятие на Ешби	***Единична система***	***Свързани ИИ (емерджентен слой)***
Разнообразие V(D)	Състояния на компонентите	Комбинаторен ръст от колективни режими; синхронизация и каскади
Закон за необходимото разнообразие	$V(R) \geq V(D)$ за пълна регулация	Разривът се разширява скокообразно при фазов преход
Конант – Ешби (модел)	Модел на частите е достатъчен	Нужен е модел на ансамбъла; моделът на частите „не вижда“ цялото
Усилване (Биър)	Повече ресурс/автоматизация	Мета-регулация на правилата на взаимодействие
Атенюиране (Биър)	Опростяване на средата	Триене, прекъсвачи, хетерогенност срещу синхронизация
Същностни променливи	Задържане в граници	Задържане при подвижни, емерджентно менящи се граници

4.2. Новите изисквания към регулатора

Ако свързаните ИИ системи произвеждат емерджентност, регулаторът трябва да отговори на едно ниво по-високо. Усилването вече не се изчерпва с повече ресурс на същото ниво – то трябва да е мета-регулация на правилата на взаимодействието: плътността на връзките, скоростта на разпространение на сигналите, допустимите контури на обратна връзка. Атенюирането на средата означава внасяне на „триене“ и разнообразие – забавяния, прекъсвачи (circuit breakers), хетерогенност на агентите – така че синхронизацията да не достига критичния си праг. А от Конант – Ешби следва най-твърдото изискване: наблюдаемост (observability) на колективните режими – метрики за синхронизация и близост до бифуркация, ранни индикатори за фазов преход. Без такъв модел на ансамбъла регулаторът остава нерелевантен.

V. Кибернетичен прочит на рисковете

Двата ефекта се събират в една и съща кибернетична оценка: разширяване на разрива в разнообразието (variety gap) между средата и регулатора. Оттук произтича и различна картина на рисковете. Синхронизацията е атенюатор на разнообразието – тя свива множеството възможни колективни състояния до един или няколко режима и така отнема на регулатора разнообразието-резерв, което му е нужно, за да поглъща смущения. Същевременно синхронизираната популация се превръща в единна точка на отказ: едно въздействие върху общия сигнал повлича целия клъстер, което прави привидната подреденост системна крехкост. Емерджентността, от своя страна, поражда непредвидимост в информационната среда, която допълнително се усилва от наличие на фазови преходи.

От тази оценка произтича следното съждение: Класическата политика реагира на конкретна заплаха с конкретна забрана; кибернетичната политика проектира капацитет. Забраната атенюира едно измерение на разнообразието, но оставя останалите отворени; капацитетът добавя разнообразие към самия регулатор и му позволява да поглъща цели класове смущения, включително още непоявили се. Оттук следва и, че отговорът на ИИ-усилените заплахи е усилване, а не концентрация. Концентрацията на власт свива броя на решаващите центрове, намалява вътрешното разнообразие на регулатора и възпроизвежда единна точка на отказ, тоест влошава именно параметъра, който трябва да бъде защитен. Усилването включва изграждане на технически и регулаторен капацитет, мета-регула-

ция на взаимодействието, външна наблюдаемост и ранно предупреждение чрез параметъра на подреденост, хетерогенност на екосистемата и поддържане на човешки когнитивен резерв в критичните сектори.

VI. Изводи

Първо. Сигурността в ерата на изкуствения интелект е управляемост и информация, а управляемостта е съответствие между разнообразието на смущенията и разнообразието на регулатора. Правилният обект на оценяване вече не е единичният модел, а ансамбълът от взаимодействащи модели, чиито свойства не се свеждат до свойствата на частите.

Второ. Спонтанната синхронизация на езиковите модели по модела на Курамото е числено демонстрируем атенюатор на разнообразието с остър критичен праг ($K_c \approx 1{,}60$) и възниква дори без пряка връзка, само през общия управляван обект. Пазарната концентрация понижава прага, а параметърът на подреденост r служи като външно наблюдаем, изпреварващ индикатор за ранно предупреждение.

Трето. Емерджентността в мрежите от свързани ИИ системи увеличава комбинаторно разнообразието на средата, разкъсва модела на регулатора по Конант – Ешби и понижава разделителната му способност, като измества локуса на риска към топологията на връзките. Това налага мета-регулация на правилата на взаимодействие и наблюдаемост на емерджентния слой.

Четвърто. Парадигменият отговор е „усилване, а не концентрация“: кибернетичната политика проектира капацитет – технически, регулаторен и когнитивен, вместо да концентрира власт или само да забранява. Това е единственият съвместим с закона на Ешби път за запазване на управляемостта в среда, наситена с изкуствен интелект.

REFERENCES

ASHBY, W.R., 1956. *An Introduction to Cybernetics.* London: Chapman & Hall.

BEER, S., 1979. *The Heart of Enterprise.* Chichester: John Wiley & Sons.

CALVANO, E.; CALZOLARI, G.; DENICOLÒ, V. & PASTORELLO, S., 2020. Artificial Intelligence, Algorithmic Pricing, and Collusion. *American Economic Review,* vol. 110, no. 10, pp. 3267 – 3297. ISSN 0002-8282.

CONANT, R.C. & ASHBY, W.R., 1970. Every Good Regulator of a System Must Be a Model of That System. *International Journal of Systems Science,* vol. 1, no. 2, pp. 89 – 97. ISSN 0020-7721.

KURAMOTO, Y., 1975. Self-entrainment of a population of coupled non-linear oscillators. In: *International Symposium on Mathematical Problems in Theoretical Physics. Lecture Notes in Physics*, vol. 39, pp. 420 – 422. Berlin: Springer.

KURAMOTO, Y., 1984. *Chemical Oscillations, Waves, and Turbulence.* Berlin: Springer-Verlag.

PRIGOGINE, I. & STENGERS, I., 1984. *Order Out of Chaos: Man's New Dialogue with Nature.* New York: Bantam.

STROGATZ, S.H., 2000. From Kuramoto to Crawford: exploring the onset of synchronization in populations of coupled oscillators. *Physica D: Nonlinear Phenomena,* vol. 143, no 1 – 4, pp. 1 – 20.

GOVERNABILITY IN THE AGE OF ARTIFICIAL INTELLIGENCE: A CYBERNETIC READING OF THE RISKS

Abstract. This paper offers a cybernetic reading of governability in the age of artificial intelligence, derived from Ashby's law of requisite variety and the Conant – Ashby theorem. Its central thesis is that security is governability and information, and governability is a match between the variety of disturbances and the variety of the regulator. Two systemic effects that undermine this match are examined: the spontaneous synchronization of populations of language models along the Kuramoto model, producing a phase transition above a critical threshold and clustering of outputs; and emergence in networks of connected AI systems, which raises environmental variety, breaks the regulator's internal model and lowers its resolution. On this basis the risks are reinterpreted as variety attenuation, and the principle of "amplification, not concentration" is derived as the operational maxim of the response.

Keywords: governability; cybernetics; Ashby's law; Kuramoto model; synchronization; emergence; artificial intelligence; cognitive security

Dr. Nikolay Nikolov
ORCID iD: 0000-0002-0627-6951
Sofia, Bulgaria
E-mail: niki2_1974@abv.bg

https://doi.org/10. 66334/annu26_dynaresilisoc

ДИНАМИКА НА РЕЗИЛЕНТНОСТТА НА БЪЛГАРСКОТО ОБЩЕСТВО СРЕЩУ ИНФОРМАЦИОННО ВЪЗДЕЙСТВИЕ И ДЕЗИНФОРМАЦИЯ: СРАВНИТЕЛЕН АНАЛИЗ 2023 – 2025 г.

полковник доц. д.н. Петко Димов
Военна академия „Георги Стойков Раковски“

Абстракт. Настоящото изследване представлява продължение на разработения през 2023 г. композитен индекс за измерване на резилентността на българското общество срещу информационно въздействие и дезинформация. Целта на статията е да провери дали в периода 2024 – 2025 г. е налице подобрение на националната устойчивост спрямо базовата 2023 г., като за целта 15-те наблюдаеми индикатора на модела са актуализирани с данни от същите първични източници. Резултатите показват, че общият индекс на устойчивост е приблизително стабилен с много лек спад през изборната 2024 г. и пълно възстановяване през 2025 г. Зад привидната стабилност на агрегираната стойност се крият разнопосочни процеси – укрепване на културната устойчивост и на институционалното доверие, съчетано с трайна ерозия на информационната устойчивост и рекордно влошаване на възприятието за корупция. Изследването доказва приложимостта на индекса като инструмент за периодичен мониторинг и извежда препоръки за целенасочени политики.

Ключови думи: резилентност; информационно въздействие; дезинформация; национална сигурност; социална кохезия; композитен индекс

I. Въведение

Информационното въздействие и дезинформацията се утвърдиха като основни инструменти на съвременните хибридни конфликти, а способността на обществата да им противостоят се превърна в самостоятелен обект на измерване и стратегическо планиране[1]. В предходно изследване беше разработен и приложен композитен индекс на национална устойчивост, който интегрира информационни, социални, културни, граждански и икономико-екологични компоненти и отчете обща стойност от 45,9 пункта за 2023 г. по набелязаните 15 параметъра за измерване (Dimov 2024). Още тогава беше подчертано, че истинската стойност на подобен инструмент се разкрива едва при периодичното му прилагане, което позволява да се проследи дали предприетите от държавата мерки водят до реално укрепване на обществената резилентност.

Настоящата статия отговаря именно на тази изследователска задача. Основната ѝ теза е, че в периода 2024 – 2025 г. българското общество не е постигнало устойчиво подобрение на резилентността си срещу информационно въздействие, а наблюдаваната стабилност на агрегирания индекс прикрива задълбочаване на структурните уязвимости в информационния и гражданския компонент, компенсирано от изпреварващ ръст на културната устойчивост. Периодът е особено подходящ за подобна проверка, тъй като включва безпрецедентна поредица от предсрочни парламентарни избори през 2024 г. (седми пореден вот за четири години), присъединяването на България към Шенгенското пространство от 1 януари 2025 г., подготовката за въвеждане на еврото и ескалацията на когнитивната война, свързана с агресията на Русия срещу Украйна (Price 2025).

Актуалността на изследването се обуславя и от навлизането на генеративния изкуствен интелект като нов мултипликатор на дезинформацията, което според последното издание на Индекса за медийна грамотност поставя обществата пред качествено нови предизвикателства (Lesenski 2026). В този контекст лонгитюдното проследяване на националната устойчивост престава да бъде академично упражнение и се превръща в елемент от системата за ранно предупреждение на националната сигурност.

II. Методология

Изследването прилага без изменения концептуалния петкомпонентен модел от базовото проучване, включващ информационна устойчивост (ИУ), социална устойчивост (СУ), културна устойчивост (КУ), гражданска

активност (ГА) и икономико-екологична устойчивост (ИЕУ), операционализирани чрез 15 наблюдаеми индикатора (Dimov 2024). Запазването на идентичен набор от индикатори и източници е методологическо изискване за съпоставимост на резултатите между отделните години – основен принцип при конструирането на композитни индекси.

Процесът на актуализация премина през три етапа. Първо, за всеки индикатор бяха извлечени стойностите за 2024 г. и 2025 г. от същите първични източници, използвани в базовото изследване: Националния статистически институт, Централната избирателна комисия, Европейската комисия (доклади за състоянието на Цифровото десетилетие), Евробарометър, Институт „Отворено общество – София“, Transparency International, Allianz Research, Heritage Foundation, Yale Center for Environmental Law & Policy и „Галъп интернешънъл“. Второ, стойностите бяха нормализирани по формулата от базовото изследване, при която позитивните индикатори се преобразуват като I = (x − min)/(max − min), а негативните – като огледална стойност, така че всички измерения да попадат в интервала 0 – 100. За коефициента на Джини като емпирични граници са приети min = 20 и max = 45, отговарящи на наблюдавания диапазон в Европейския съюз.

Наложени са и няколко изрично декларирани ограничения. При индикатори с двугодишна периодичност (Индексът за екологични резултати) или с липсващо годишно издание стойността на последното налично измерване е пренесена напред и е обозначена със звездичка. При индикатора за социална устойчивост на Allianz, чиито национални стойности за 2024 – 2025 г. не са публично оповестени в резюметата на доклада, е използвана регионалната стойност за Нововъзникваща Европа (48,4 пункта) като консервативна апроксимация[2]. Индикаторът „следящи националните новини“ е операционализиран чрез огледалната стойност на дела на гражданите, които системно избягват новините по данни на Reuters Institute, което представлява методологическа замяна и се отчита при интерпретацията. И накрая, както и в базовото изследване, извън обхвата остават военната, политическата, инфраструктурната и технологичната уязвимост, тъй като обект на измерване е готовността на гражданите, а не на държавните институции.

III. Литературен преглед

Теоретичната рамка на изследването стъпва върху еволюцията на концепцията за национална мощ към концепция за национална устойчивост. Класическият алгебричен модел на възприетата мощ (Cline 1975) и

неговите съвременни линейни разширения с културни, социални и научни фактори (Angelov 2020) описват потенциала на държавата, но не и способността на обществото да абсорбира шокове. Комплексният подход на НАТО измества фокуса именно към обществения слой на устойчивостта[3], а глобалната рамка на целите за устойчиво развитие предоставя измерими индикатори за социално-икономическото ѝ измерение[4] (Helliwell et al. 2024). Социалният капитал и междуличностното доверие се разглеждат като фундамент на способността на общностите да устояват на разделящи манипулации (Putnam 2000), културната идентичност – като защитен механизъм срещу подкопаване на ценностите (Soini and Birkeland 2014), а гражданската ангажираност – като поведенческо проявление на готовността за защита на общото благо (Adler and Goggin 2005).

Прегледът на литературата, публикувана след базовото изследване през 2023 г., откроява три нови акцента. Първият е институционализирането на понятието „манипулация на информация и вмешателство от чужди сили“ (FIMI) в стратегическите документи на Европейския съюз и произтичащото от това търсене на измерими показатели за обществена уязвимост. Вторият е ефектът на генеративния изкуствен интелект: деветото издание на Индекса за медийна грамотност изрично отчита, че синтетичното съдържание и автоматизираните кампании повишават изискванията към когнитивната имунизация на обществата и препоръчва образователен, а не рестриктивен подход (Lesenski 2026). Третият акцент е емпиричното потвърждение на връзката между социална резилентност и суверенен риск – според Allianz Research резките спадове в социалната устойчивост предхождат епизоди на суверенен стрес с период от една до две години, което превръща подобни индекси в инструменти за ранно предупреждение[5].

Тези индекси са много подходящи за съпоставяне между държавите. Например индексът за медийна грамотност класира 41 европейски държави, но обхваща само информационно-образователното измерение (Lesenski 2026); Digital News Report проследява доверието в новините, но не го обвързва с отбранителната готовност (Newman et al. 2025); Индексът за възприятие на корупцията измерва институционалното измерение изолирано[6].

Именно в това се състои приносът на настоящия подход – той интегрира разнородните измервания в единна времева редица за конкретната държава и позволява да се идентифицират компонентите на устойчивостта и в коя посока се движат. От този анализ произтича и работната хипотеза на изследването – при съчетание на политическа нестабилност и интен-

зивно информационно въздействие компонентите на устойчивостта ще се движат разнопосочно, като институционално зависимите индикатори ще се влошават по-бързо, отколкото културно-идентичностните, които действат като стабилизатор.

IV. Актуализация на индикаторите за 2024–2025 г.

В областта на информационната устойчивост данните очертават стагнация на ниски равнища. Делът на населението с поне основни дигитални умения остава 35,5% при средно 55,6% за ЕС, което нарежда България на 26-о място от 27 държави членки, а Докладът за цифровото десетилетие от 2025 г. не отчита напредък спрямо предходната година[7]. Индексът за медийна грамотност дори намалява леко от 33 на 31 пункта и България остава последна в ЕС въпреки вложените финансови ресурси в различни европейски проекти, които са работили у нас през този период. Най-тревожна е динамиката на доверието в новините, което по данни на Reuters Institute спада от 32% (2023 г.) на 29% (2024 г.) и 26% (2025 г.), като страната се нарежда на 44-то място от 48 изследвани пазара и регистрира най-високото равнище на избягване на новини в цялата извадка – 63% (Newman et al. 2024; 2025; Price 2025).

При социалната устойчивост картината е смесена. Миграционният баланс остава положителен – през 2024 г. в страната са се заселили 52 189 души при 13 002 изселили се, което формира механичен прираст от +39 187 души, а 34,9% от заселилите се са български граждани[8]. Изчисленото по методиката на базовото изследване съотношение дава стойност от около 40% – близка до отчетените 42,8% за 2023 г., а предварителните данни за 2025 г. потвърждават запазването на положителния баланс[9]. Коефициентът на Джини обаче се влошава от 37,2 (2023 г.) на 38,4 (2024 г.), преди да се подобри частично до 37,7 през 2025 г., като България остава държавата с най-високо подоходно неравенство в ЕС[10]. Глобалният индекс на социална устойчивост на Allianz отчита слабо подобрение в световен мащаб (от 47,4 на 47,9 пункта), но регионът, към който принадлежи България, остава със стойност 48,4 пункта – под равнището, отчетено за страната през 2023 г.[11]

Културната устойчивост е компонентът с най-силна положителна динамика. Посещенията в музеите нарастват от 4 965 хил. през 2023 г. на 5 070 хил. през 2024 г. (+2,1%) и достигат 6 394 хил. през 2025 г. – ръст от 26,1% само за една година, като съотнесени към населението на страната те се равняват на 99,3%[12]. Делът на гражданите, декларирали използване

на български език, остава стабилен по данни от последното преброяване. В противовес, редовното следене на националните новини намалява – изчислено чрез огледалната стойност на избягването на новини, то спада от 55% (2023 г.) до около 37% през 2025 г., което показва, че културното участие и информационното участие се разминават като поведенчески модели (Newman et al. 2025).

Гражданската активност демонстрира вътрешно противоречива динамика. Изборите през юни 2024 г. регистрираха исторически минимум на избирателната активност от 33,8%, частично компенсиран от 38,9% на вота през октомври 2024 г., който освен това беше съпътстван от установени от Конституционния съд изборни нарушения и частично касиране[13] (Price, 2025). Индексът за възприятие на корупцията се срива от 45 пункта (2023 г.) през 43 пункта (2024 г.) до рекордно ниските 40 пункта през 2025 г. – най-лошият резултат на страната от 2012 г. насам, нареждащ я на 84-о място от 182 държави и на последно място в ЕС заедно с Унгария[14,15]. Парадоксално, доверието в правителството се повишава от 16,5% (2023 г.) на 23% през есента на 2024 г. и 27% през пролетта на 2025 г., макар да остава далеч под средното за ЕС от 36%[16]. Декларираната готовност за участие в отбраната се задържа на 30% по данни на „Галъп интернешънъл“, като национално представително проучване сред младежите на възраст 16 – 25 години отчита значително по-висока готовност от 62% при тази възрастова група, съчетана обаче с висока податливост на конспиративно мислене при 40% от анкетираните[17,18].

Икономико-екологичният компонент остава практически непроменен: Индексът на икономическа свобода се движи от 69,4 през 2023 г. към 69,0 пункта (31-во място) през 2024 г. и 68,9 пункта в изданието, обхващащо данни за 2025 г.[19,20], а Индексът за екологични резултати, който се публикува на две години, запазва стойността си от 56,3 пункта от изданието за 2024 г. (Block et al. 2024). Пълната картина на актуализираните индикатори е представена в Таблица 1.

V. Резултати

Резултатите от това проучване ясно показват, че в периода 2023 – 2025 г. резилентността на българското общество срещу информационно въздействие не е отбелязала устойчиво подобрение. Общият индекс е приблизително стабилен, като пада с един пункт през изборната 2024 г. и се възстановява с леко надвишение през 2025 г. Динамиката на компонентните подиндекси е обобщена в Таблица 2 и визуализирана на Фигура 1.

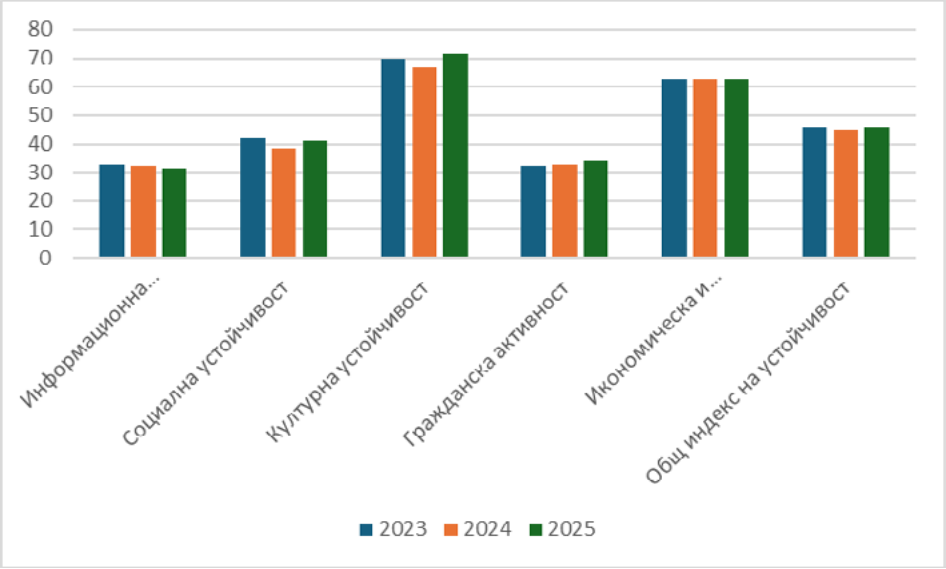
Таблица 1. Стойности на наблюдаемите индикатори за периода 2023 – 2025 г.

Латентна променлива	*Наблюдаем индикатор*	*2023*	*2024*	*2025*	*Източник*
Информационна устойчивост	Основни дигитални умения, % от населението	33	35,5	35,5	European Commission (2024; 2025)
	Индекс на медийна грамотност (точки, 0 – 100)	33	33*	32	Лесенски (2026)
	Доверие в новините, % от населението	32	29	26	Newman et al. (2024; 2025)
Социална устойчивост	Съотношение между напускащи и завръщащи се граждани (нетен прираст, %)	42,8	40,1	45	НСИ (2026)
	Индекс на социална устойчивост (SRI, точки)	53,1	48,4*	48,4*	Allianz Research (2026)
	Коефициент на Джини (нормализиран, обърнат)	29,4	26,4	29,2	Eurostat (2026)
Културна устойчивост	Използване на български език, %	78	78	78	НСИ
	Посещения в музеи, % от населението	77	78,8	99,3	НСИ (2025а; 2026а)
	Редовно следящи националните новини, %	55	43	37	Newman et al. (2025)
Гражданска активност	Избирателна активност, %	40,3	38,9	38,9*	ЦИК (2024)
	Индекс за възприятие на корупцията (точки)	43	43	40	Прозрачност без граници (2025; 2026)
	Доверие в правителството, %	16,5	23	27	Eurobarometer (2024; 2025)
	Готовност за участие в отбраната, %	30	30*	30*	Gallup International (2024)
Икономическа и екологична	Индекс на икономическа свобода (точки)	69,4	69,0	68,9	Heritage Foundation (2024; 2026)
	Индекс за екологични резултати (EPI, точки)	56,3	56,3	56,3*	Block et al. (2024)
Общ индекс на устойчивост:		45,9	44,8	46,1	

** Пренесена последна налична стойност, апроксимация или заместващ индикатор*

Таблица 2. Компонентни подиндекси и общ индекс на устойчивост, 2023–2025 г.

Компонент	*2023*	*2024*	*2025*	*Δ 2025/2023*
Информационна устойчивост	32,7	32,5	31,2	– 1,5
Социална устойчивост	41,8	38,3	40,9	– 0,9
Културна устойчивост	70,0	66,6	71,4	+ 1,4
Гражданска активност	32,5	32,8	34	+ 1,5
Икономическа и екологична устойчивост	62,9	62,7	62,6	– 0,3
Общ индекс на устойчивост	45,9	44,8	46,1	+ 0,2



Фигура 1. Компоненти на индекса на национална устойчивост, 2023 – 2025 г.

Три констатации заслужават специално внимание. Първо, информационната устойчивост е единственият компонент с монотонен спад през целия период (от 32,7 на 31,2 пункта), воден от ерозията на доверието в новините при стагниращи дигитални умения и медийна грамотност. Второ, културната устойчивост не само се възстановява след спада от кризисната 2024 г., но и надхвърля базовото си равнище (71,4 срещу 70,0 пункта), движена от безпрецедентния ръст на музейните посещения. Трето, граждан-

ската активност се подобрява номинално (+ 1,5 пункта) въпреки срива на възприятието за корупция, тъй като повишеното доверие в правителството и стабилизираната избирателна активност компенсират загубата – композиционен ефект, който изисква внимателна интерпретация.

Спадът през 2024 г. съвпада хронологически с двойния предсрочен вот, установените изборни нарушения и пика на неравенството, което подкрепя работната хипотеза, че политическата нестабилност се капитализира най-бързо в институционално зависимите индикатори. Възстановяването през 2025 г. от своя страна се дължи почти изцяло на културния компонент, а не на информационния, т.е. обществото укрепва идентичностните си защити, докато когнитивните продължават да отслабват.

VI. Дискусия

Едно обяснение за разнопосочната динамика на компонентите е, че те реагират на информационното въздействие през различни механизми и с различна инерция. Културната устойчивост се опира на дълбоко вкоренени идентичностни структури – език, историческа памет, културно наследство – които в условия на външен натиск могат дори да се активизират, както подсказва ръстът на музейните посещения и на културния туризъм. Информационната устойчивост, напротив, зависи от бавно натрупващи се компетентности (дигитални умения, критично мислене) и от качеството на медийната среда, което според независимите оценки остава ниско поради политическа намеса, ограничен плурализъм и стратегически дела срещу журналисти (Price 2025).

Второ обяснение е ефектът на „оттегляне от информационното пространство“ – рекордното избягване на новини може да се интерпретира не само като уязвимост, но и като спонтанна защитна реакция срещу токсична информационна среда – реакция, която обаче създава вакуум, запълван от социалните мрежи и инфлуенсърите, където податливостта на манипулация е най-висока (Newman et al. 2025).

Силните страни на изследването са лонгитюдният дизайн с идентичен набор от индикатори и източници, прозрачната процедура по нормализация и агрегиране, както и триангулацията на данни от национална статистика, международни индекси и социологически проучвания. Подходът позволява да се разкрие, че привидно стабилният агрегиран индекс прикрива структурно пренареждане на устойчивостта – констатация, която би останала невидима при еднократно измерване или при използване само на общата стойност.

Изследването има и ограничения, които трябва да се посочат откровено. Равнотегловното агрегиране е опростяване спрямо моделирането със структурни уравнения от базовото изследване и може да подценява или надценява приноса на отделни индикатори. Три индикатора разчитат на пренесени стойности или регионални апроксимации поради периодичността на първичните източници, а замяната на измерителя за следене на новините с огледалната стойност на избягването им внася методологически шев в редицата. Освен това част от индексите (CPI, SRI, Индексът на медийна грамотност) измерват възприятия и моделирани оценки, а не пряко наблюдавано поведение, което внася систематична несигурност. И накрая, тригодишният времеви прозорец е достатъчен за идентифициране на посоки, но не и за статистически надеждни изводи за тенденции, което е и основният аргумент за продължаване на измерването.

На фона на тези ограничения приносът на изследването за науката е троен – то предоставя първата времева редица на композитен индекс за информационна резилентност на българското общество, демонстрира емпирично, че компонентите на националната устойчивост се движат асинхронно в условия на политическа криза и валидира методологическото решение уязвимостта да се измерва през готовността на гражданите, а не през капацитета на институциите. Последиците за политиката са преки – инвестициите следва да се насочат приоритетно към информационния компонент, където спадът е монотонен, а не към културния, който се самоподдържа.

VII. Предложения за подобряване на националната устойчивост

Най-доброто налично решение за монотонния спад на информационната устойчивост е системното интегриране на медийната грамотност в образованието от ранна възраст по финландски модел – подход, изрично препоръчан и в последното издание на Индекса за медийна грамотност (Lesenski 2026). За България това означава ускорено изпълнение на започнатата ревизия на училищните програми с изричен компонент за разпознаване на фалшиво съдържание и манипулация, съчетано с квалификация на учителите.

Срещу ерозията на доверието в новините работещо решение е укрепването на обществените медии, които и през 2025 г. остават най-доверените марки в страната – БНР (56%) и БНТ (55%) – значително над

средното доверие в новините[21] (Price 2025). По отношение на гражданската активност рекордно ниският резултат в Индекса за възприятие на корупцията изисква възобновяване на замразената национална антикорупционна стратегия и изпълнение на препоръките на Европейската комисия[22], а положителният сигнал от готовността на 62% от младежите да защитават страната следва да бъде капитализиран чрез програми за доброволна подготовка и резерв[23]. И накрая, изпреварващият ръст на културното участие трябва да бъде съзнателно обвързан с националния наратив за България като цивилизационна мозайка и мост между Изтока и Запада, така че идентичностният ресурс да подхранва и информационната, и гражданската устойчивост.

VIII. Заключение

Настоящото изследване проследи за първи път в тригодишна времева рамка динамиката на композитния индекс за резилентност на българското общество срещу информационно въздействие и дезинформация. Основните констатации са, че общият индекс се задържа на равнище от около 46 пункта без устойчиво подобрение спрямо 2023 г., че кризисната 2024 г. предизвика слаб спад, концентриран в социалния и културния компонент и че възстановяването през 2025 г. е избирателно – културната устойчивост и институционалното доверие нарастват, докато информационната устойчивост продължава монотонния си спад, а възприятието за корупция достига историческо дъно. Изведените заключения потвърждават хипотезата за асинхронно движение на компонентите и очертават ясен приоритет за държавната политика – когнитивните защити на обществото изостават от идентичностните и именно там е критичната уязвимост към хибридни въздействия.

Направленията за бъдеща работа включват продължаване на годишното измерване с цел натрупване на статистически надеждна редица, преминаване от равнотегловно към емпирично калибрирано претегляне чрез моделиране със структурни уравнения върху разширената редица, включване на поведенчески индикатори за разпространение на дезинформация в социалните мрежи и съпоставително прилагане на индекса към други държави от Югоизточна Европа, които според клъстерния анализ споделят сходен профил на уязвимост (Lesenski 2026). Проучването е важно, защото превръща разпръснати статистически наблюдения в единен, повторяем

и чувствителен към промени инструмент за мониторинг на националната сигурност.

Посочените открития са достойни за отбелязване от научната общност по три причини. Първо, те емпирично документират рядко наблюдаван феномен – разминаване между културната и информационната резилентност в рамките на едно общество под информационен натиск, което поставя под въпрос допускането за хомогенност на националната устойчивост, имплицитно в повечето съществуващи индекси. Второ, те демонстрират, че еднократните класации между държави систематично пропускат вътрешната динамика, която е решаваща за политическото планиране. Трето, предложеният инструментариум е податлив на репликация – всички източници са публични, процедурите по нормализация са изрично декларирани, а ограниченията са прозрачно посочени, което отговаря на съвременните изисквания за отворена наука и позволява независима проверка и надграждане на резултатите.

БЕЛЕЖКИ

1. NATO, 2020. *NATO's Approach to Countering Disinformation: A Focus on COVID-19*. Brussels: NATO Review.

2. ALLIANZ RESEARCH, 2026. *Allianz Social Resilience Index 2025: The Middle-Resilience Trap*. Munich: Allianz SE. https://www.allianz.com/en/economic_research/insights/publications/specials_fmo/260311_Social_Resilience_Index.html

3. NATO, 2020...

4. UNITED NATIONS, 2015. *Transforming Our World: The 2030 Agenda for Sustainable Development. Resolution A/RES/70/1*. New York: United Nations.

5. ALLIANZ RESEARCH, 2026...

6. Прозрачност без граници, 2026. *Индекс за възприятие на корупцията 2025 – анализ за България*. София: Асоциация „Прозрачност без граници". https://transparency.bg/corruption-perception-index-2025/.

7. EUROPEAN COMMISSION, 2025. *State of the Digital Decade 2025 – Country Report Bulgaria*. Brussels: European Commission. https://digital-strategy.ec.europa.eu.

8. НСИ, 2026. *Външна миграция по възраст и гражданство на мигрирали-те лица*. София: Национален статистически институт. Достъпно на: https://www.nsi.bg/bg/content/13036/.

9. НСИ, 2026...

10. EUROSTAT, 2026. *Gini coefficient of equivalised disposable income – EU-SILC survey (ilc_di12)*. Luxembourg: Eurostat. available from: https://ec.europa.eu/eurostat.

11. ALLIANZ RESEARCH, 2026…

12. НСИ, 2026а. *Култура – дейност на музеите през 2025 година*. София: Национален статистически институт.

13. ЦИК, 2024. *Резултати от изборите за народни представители на 9 юни и 27 октомври 2024 г*. София: Централна избирателна комисия. Достъпно на: https://results.cik.bgл

14. Прозрачност без граници, 2025. *Индекс за възприятие на корупцията 2024 – анализ за България*. София: Асоциация „Прозрачност без граници“. Достъпно на: https://transparency.bg/corruption-perception-index-2024/.

15. Прозрачност без граници, 2026. *Индекс за възприятие на корупцията 2025 – анализ за България*. София: Асоциация „Прозрачност без граници“. Достъпно на: https://transparency.bg/corruption-perception-index-2025/.

16. EUROBAROMETER, 2025. *Standard Eurobarometer 103 – Spring 2025*. Brussels: European Commission. Available from: https://europa.eu/eurobarometer.

17. GALLUP INTERNATIONAL, 2024. *Willingness to Fight for Their Country: Global Survey in 45 Countries*. Sofia/Zurich: Gallup International Association. Available from: https://www.gallup-international.com.

18. ЦИД, 2025. *Национално представително проучване сред младежи на възраст 16 – 25 години относно готовността за отбрана и податливостта на дезинформация*. София: Център за изследване на демокрацията.

19. HERITAGE FOUNDATION, 2024. *2024 Index of Economic Freedom: Bulgaria*. Washington, DC: The Heritage Foundation. Available from: https://www.heritage.org/index/pages/country-pages/bulgaria.

20. HERITAGE FOUNDATION, 2026. *2026 Index of Economic Freedom: Bulgaria*. Washington, DC: The Heritage Foundation. Available from: https://www.heritage.org/index/pages/country-pages/bulgaria.

21. БТА, 2026. *Доверието в новините в България спада до 21%, показва доклад на Института „Ройтерс“*. София: Българска телеграфна агенция. Достъпно на: https://www.bta.bg/bg/news/bulgaria.

22. Прозрачност без граници, 2026...

23. ЦИД, 2025...

ЛИТЕРАТУРА

АНГЕЛОВ, Г., 2020. *Държавност и национална сигурност*. София: Военно издателство.

БАХЧЕВАНОВ, Г., 2007. *Система за национална сигурност. Държавни институции и оперативни компоненти*. София: Издателство на Военна академия „Г. С. Раковски“.

ДИМОВ, П., 2024. *Измерване на резилентността на българското общество срещу информационно въздействие и дезинформация*. София: Военна академия „Г. С. Раковски“.

ЛЕСЕНСКИ, М., 2026. *Индекс за медийна грамотност 2026*. София: Институт „Отворено общество – София“. Достъпно на: https://osis.bg/?p=5744.

ADLER, R.P., & GOGGIN, J., 2005. What Do We Mean By "Civic Engagement"? *Journal of Transformative Education*, vol. 3, no. 3, pp. 236 – 253. Available from: https://doi.org/10.1177/1541344605276792.

BLOCK, S.; EMERSON, J.W.; ESTY, D.C., SHERBININ, A.; WENDLING, Z.A., et al., 2024. *2024 Environmental Performance Index*. New Haven, CT: Yale Center for Environmental Law & Policy. Available from: https://epi.yale.edu/measure/2024/EPI.

CLINE, R. S., 1975. *World Power Assessment: A Calculus of Strategic Drift*. Boulder: Westview Press.

HELLIWELL, J.; LAYARD, R.; SACHS, J.D.; DE NEVE, J.-E.; AKNIN, L.B. & WANG, S., 2024. *World Happiness Report 2024*. Oxford: Sustainable Development Solutions Network. ISBN 978-1-7348080-7-0

NEWMAN, N.; FLETCHER, R.; ROBERTSON, C.T.; ARGUEDAS, A.R. & NIELSEN, R.K., 2024. *Reuters Institute Digital News Report 2024*. Oxford: Reuters Institute for the Study of Journalism. Available from: https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024.

NEWMAN, N.; FLETCHER, R.; ROBERTSON, C.T. & NIELSEN, R.K., 2025. *Reuters Institute Digital News Report 2025*. Oxford: Reuters Institute for the Study of Journalism. Available from: https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2025

PRICE, L.T., 2025. Bulgaria. In: *Reuters Institute Digital News Report 2025*. Oxford: Reuters Institute for the Study of Journalism. Available from: https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2025/bulgaria.

PUTNAM, R.D., 2000. *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon and Schuster.

SOINI, K. & BIRKELAND, I., 2014. Exploring the scientific discourse on cultural sustainability. *Geoforum*, vol. 51, pp. 213 – 223. Available from: https://doi.org/10.1016/j.geoforum.2013.12.001

WACKERNAGEL, M.; LIN, D.; EVANS, M.; HANSCOM, L. & RAVEN, P., 2019. Defying the Footprint Oracle: Implications of Country Resource Trends. *Sustainability*, vol. 11, no. 7, 2164. Available from: https://doi.org/10.3390/su11072164.

DYNAMICS OF THE RESILIENCE OF BULGARIAN SOCIETY AGAINST INFORMATION INFLUENCE AND DISINFORMATION: A COMPARATIVE ANALYSIS 2023 – 2025

Abstract. This study is a follow-up to the composite index developed in 2023 for measuring the resilience of Bulgarian society against information influence and disinformation. The aim of the article is to examine whether national resilience improved in 2024–2025 compared to the 2023 baseline, by updating the fifteen observable indicators of the model with data from the same primary sources. Behind the apparent stability of the aggregate

value lie divergent processes: a strengthening of cultural resilience and institutional trust, combined with a persistent erosion of informational resilience and a record deterioration in corruption perception. The study confirms the applicability of the index as a periodic monitoring tool and formulates recommendations for targeted policies.

Keywords: resilience; information influence; disinformation; national security; social cohesion; composite index

Colonel Assoc. Prof. Petko Dimov, DSc.
ORCID iD: 0000-0002-0071-7787;
Department of Distance Learning,
Language Training and Qualification
Rakovski National Defence College
82, Evlogi and Hristo Georgievi Blvd.
1504 Sofia, Bulgaria
E-mail: p.dimov@rndc.bg

https://doi.org/10. 66334/annu26_geopolizm

ГЕОПОЛИТИЧЕСКИТЕ ИЗМЕРЕНИЯ НА ВОЕННОИСТОРИЧЕСКАТА КОМПАРАТИВИСТИКА: МЕТОДОЛОГИЧЕСКИ И ПРИЛОЖНИ АСПЕКТИ

доц. д-р Радослав Бонев
Военна академия „Георги Стойков Раковски“

Абстракт. Разработката изследва геополитическите измерения на военноисторическата компаративистика като методологически подход за сравнително изучаване на войните, военните системи и стратегическите решения в различни исторически и пространствени контексти. Основната теза е, че геополитическият анализ не следва да се използва като външно допълнение към военноисторическото сравнение, а като негов структурен компонент. Анализира се ролята на географското положение, стратегическото пространство, националните интереси, ресурсния потенциал, съюзните отношения и политическите цели. Чрез примери от Наполеоновите войни, Балканските войни, Първата и Втората световни войни се показва как сходни военни явления придобиват различен смисъл в различни геополитически конфигурации. Изведени са методологически ограничения на историческата аналогия и приложната стойност на сравнителния подход за анализа на съвременната стратегическа среда и националната сигурност.

Ключови думи: военно изкуство; военноисторическа компаративистика; геополитика; историческа аналогия; национална сигурност; стратегия

Сравнителният подход е един от устойчивите инструменти на историческото познание. Чрез него отделното събитие се извежда от собствената си уникалност и се поставя в отношение към други събития, процеси и структури. **Във военната история това има особено значение, защото войната винаги се разгръща едновременно във времето и пространството, а военното действие е зависимо от политическата цел, географската среда, ресурсите, съюзите и характера на държавата.** Следователно сравнението на войни, кампании, армии или стратегически решения не може да бъде сведено до съпоставяне на численост, въоръжение и оперативни резултати.

Съвременната сравнителна история подчертава необходимостта сравняваните случаи да бъдат поставяни в собствените им исторически контексти и да се избягва механичното пренасяне на категории между различни епохи (Haupt, Kocka 2009; Kocka 2003). Тази постановка е особено важна за военноисторическата компаративистика. Сходството на формата не означава тъждество на съдържанието, а аналогията не е доказателство за повторяемост на историческия процес.

Целта на настоящия доклад е да обоснове тезата, че геополитическият анализ трябва да бъде структурен компонент на военноисторическата компаративистика. Изследването следва аналитичната връзка: **геополитическо положение → национален интерес → политическа цел → стратегически избор → военно действие**. Тази последователност позволява военното събитие да бъде разглеждано не като изолирана проява на военното изкуство, а като резултат от взаимодействието между пространство, политика, ресурси и историческа ситуация.

Сравнението е познавателна операция, чрез която се установяват сходства и различия между два или повече обекта. В историческото изследване то придобива по-сложен характер, защото сравняваните обекти са времево обусловени и принадлежат към неповторими исторически конфигурации. Затова сравнителната история не търси само формални подобия, а проверява доколко едни и същи категории имат еднакво значение в различни общества и периоди.

Военноисторическата компаративистика може да се разбира като систематично сравнение на военни явления (войни, кампании, операции, стратегически култури, организационни модели, мобилизационни системи и форми на военно изкуство), с цел установяване на закономерности, различия и причинни зависимости. Нейният предмет не е просто „кое е сходно“, а защо при привидно сходни условия възникват различни резултати.

Методологически съществено е разграничението между сравнение и аналогия. Аналогията открива сходство и може да насочи изследователя към хипотеза. Сравнението изисква критерии, контрол върху контекста и аргументация. Когато историческата аналогия се превърне в заместител на анализа, възниква опасност миналото да бъде използвано като готов модел за настоящето. Затова сравнителният подход трябва да съчетава типологизиране и контекстуализация (Krom, Guyatt 2022; Mahoney, Rueschemeyer 2003).

Особено значение има и отношението между сравнителна и свързана история. Държавите, армиите и стратегиите не съществуват като затворени единици. Те взаимстват институции, технологии и доктрини; участват в съюзи; реагират на едни и същи международни промени. Следователно сравнението трябва да отчита не само различията между случаите, но и историческите връзки между тях.

Геополитиката въвежда пространственото измерение в анализа на политическата и стратегическата дейност. Още класическите трудове на Фридрих Ратцел и Алфред Тайър Махан поставят въпроса за отношението между географско положение, политическа мощ и стратегически възможности (Ratzel 1897; Mahan 1890). За военноисторическото изследване географията не е неподвижен фон. Тя представлява система от ограничения и възможности, които получават различна стойност според технологиите, ресурсите и политическите цели.

Първият критерий е географското положение. Континентална, морска, полуостровна или островна държава е изправена пред различни стратегически проблеми. Дължината и характерът на границите, релефът, транспортните направления, достъпът до морета и ресурсни райони влияят върху организацията на отбраната и върху възможността за проекция на сила. Това не означава географски детерминизъм. Едно и също пространство може да има различно военно значение при различни технологични и политически условия.

Вторият критерий е стратегическото пространство. Клаузевиц показва, че войната трябва да се разбира във връзка с политическата цел, а не като автономна техническа дейност (Clausewitz 1984). Пространството придобива стратегическо значение именно чрез политическата цел. Една територия може да бъде важна като комуникационен възел, ресурсна база, буфер, плацдарм или символен обект. Следователно военноисторическото сравнение трябва да пита не само къде се води войната, но защо точно това пространство е политически и стратегически значимо.

Третият критерий е националният интерес. Той свързва геополитическото положение с политическата цел. При сравнението на две държави не е достатъчно да се установи, че те действат в сходна географска среда. Необходимо е да се изясни как техните политически елити разбират сигурността, границите, съюзите, ресурсите и желаното място в международната система.

Четвъртият критерий е икономическият и ресурсният потенциал. Продължителността на войната, мобилизационната способност и устойчивостта на армията зависят от демография, индустриална база, транспорт, финанси и достъп до суровини. В този смисъл геополитическото пространство включва не само територия, но и инфраструктурата, която превръща пространството във военно използваем ресурс.

Петият критерий е съюзната конфигурация. Международната система променя стойността на географското положение. Държава, която самостоятелно е периферна, може чрез съюз да придобие централно стратегическо значение. Обратно, неблагоприятна съюзна структура може да превърне иначе силна държава в стратегически уязвима. Поради това съюзите трябва да се анализират не като външна добавка, а като част от геополитическата конфигурация.

Наполеоновите войни (1799 – 1815) показват значението на пространството, ресурсите и политическата устойчивост. Кампанията от 1812 г. не може да бъде разбрана единствено чрез тактическите характеристики на френската и руската армии. Огромното пространство, комуникациите, снабдяването, руската способност за отстъпление и запазване на военния потенциал превръщат географията в действащ стратегически фактор. Сравнението с други кампании е продуктивно само ако тези особености бъдат запазени, а не редуцирани до **формулата „дълбочина срещу настъпление“**.

Балканските войни (1912 – 1913) предлагат друг тип сравнителна ситуация. На относително ограничено пространство действат държави с различни национални цели, мобилизационни възможности и взаимно противоречащи си териториални програми. Военният успех през 1912 г. не премахва политическите противоречия между съюзниците. Тъкмо обратното – **промяната на военното положение променя и политическите очаквания. Така връзката между национален интерес, съюзна конфигурация и военно действие става особено видима.**

Първата световна война (1914 – 1918) показва как индустриалната мощ, комуникационните системи и съюзните структури могат да трансформират класическите географски фактори. Пространството продъл-

жава да има значение, но то вече се измерва и чрез железопътна мрежа, производствен капацитет, морска блокада и способност за продължителна мобилизация. Сравняването на фронтовете изисква да се отчита различната плътност на инфраструктурата, тактическата и оперативната емкост на основни направления в хода на военните действия, различният оперативен простор и различната политическа цена на териториалните загуби.

Втората световна война (1939 – 1945) още по-ясно демонстрира взаимодействието между география, технология и ресурси. Механизацията увеличава оперативната подвижност, но едновременно с това засилва зависимостта от гориво, транспорт и логистика. Морските и въздушните комуникации придобиват ново значение. **Стратегическата дълбочина** остава фактор, но нейният ефект зависи от индустриалния потенциал и способността за възстановяване на силите. Така една и съща географска категория придобива различно съдържание в различните технологически епохи.

Тези примери показват, че военноисторическата компаративистика е най-продуктивна, когато не сравнява отделни битки като самостоятелни технически феномени, а цели геополитически конфигурации. Тогава могат да бъдат съпоставяни отношенията между политическа цел, пространство, ресурс, съюз и военен инструмент.

Историческата аналогия е привлекателна, защото прави сложната реалност разбираема чрез познат пример. Но тя носи и риск. Назоваването на дадена съвременна ситуация като „нов Мюнхен“, „нов Виетнам“ или „нова 1914 година“ може да има реторична сила, без да притежава достатъчна аналитична стойност. Подобни формули често избират едно сходство и пренебрегват множество структурни различия.

За да бъде научно продуктивна, аналогията трябва да бъде подложена на проверка. Необходимо е да се определят сравняваните единици, времевият хоризонт, критериите и причинните механизми. Трябва да се проверят не само сходствата, но и различията. Именно различията често показват защо очакваното повторение не настъпва.

Следователно миналото не трябва да се използва като каталог от готови решения. Неговата стойност е в разширяването на аналитичния хоризонт. Военната история може да покаже диапазона от възможни взаимодействия между политика, пространство и военна сила, но не освобождава стратега от необходимостта да анализира конкретната съвременна среда.

Приложната стойност на военноисторическата компаративистика се проявява най-вече в способността ѝ да дисциплинира стратегическото мислене. Тя учи изследователя да различава структурно сходство от повърх-

ностна прилика и да проверява дали механизмите, действали в миналото, съществуват и в настоящето. В този смисъл историческото знание не предсказва автоматично бъдещето, а подобрява качеството на въпросите, които поставяме към него.

За националната сигурност особено полезно е сравнението на модели на стратегическа уязвимост и устойчивост: зависимост от външни комуникации, ресурсни ограничения, съюзна надеждност, демографски потенциал, институционална способност и стратегическа дълбочина. Тези категории позволяват историческите случаи да бъдат използвани като аналитични лаборатории, без да бъдат превръщани в рецепти.

Геополитическият компонент е необходим и защото националната сигурност е пространствено обусловена. Държавите имат различни граници, съседства, комуникационни направления и стратегически зависимости. Същевременно съвременните технологии променят значението на пространството, без да го премахват. Киберпространството, космическите системи, далекобойните средства и информационните мрежи разширяват географията на сигурността, но материалната инфраструктура и територията запазват своето значение.

За военното образование сравнителният подход има и педагогическа стойност. Той позволява обучаемият да бъде изведен отвъд запаметяването на факти и да бъде поставен пред необходимостта да обяснява различията. Защо една стратегия работи в един контекст и се проваля в друг? Кои фактори са структурни и кои случайни? Как политическата цел изменя стойността на военния успех? Тези въпроси изграждат военноисторическа култура, която е непосредствено свързана със стратегическото мислене.

Изследването позволява да бъдат формулирани няколко основни извода. Първо, военноисторическото сравнение е методологически непълно, ако географската среда се третира само като фон на военните действия. Второ, геополитическото положение придобива стратегическо значение чрез националния интерес и политическата цел. Трето, ресурсите, инфраструктурата и съюзите посредничат между пространството и реалната военна способност. Четвърто, историческата аналогия е полезна само когато е контролирана чрез ясни критерии и чрез анализ на различията.

Оттук следва, че обект на сравнение трябва да бъде не само военният резултат, а цялата причинна последователност: **геополитическо положение → национален интерес → политическа цел → стратегически избор → военно действие.** Така сравнителният метод се превръща от описателен инструмент в средство за причинно обяснение.

Военноисторическата компаративистика придобива по-голяма обяснителна сила, когато разглежда историческите случаи едновременно като уникални събития и като елементи на различни геополитически конфигурации. Географията не определя механично политиката, но очертава полето на възможностите; политиката превръща тези възможности в цели; стратегията свързва целите с наличните средства; военното действие проверява тази връзка в конкретна историческа среда.

Поради това геополитическият анализ не е външна добавка към военноисторическото сравнение. Той е един от неговите структурни елементи. Съчетаването на сравнителна история, военна история и геополитически анализ позволява по-прецизно да се разберат както решенията на миналото, така и ограниченията при използването на историческия опит за осмисляне на съвременната стратегическа среда.

Благодарности. Авторът изказва благодарност на колегите, чиито професионални дискусии допринесоха за формулирането на част от поставените методологически въпроси.

БЕЛЕЖКИ

1. Под „военноисторическа компаративистика“ в текста се разбира систематично сравнително изследване на военни явления в техния политически, социален, технологичен и пространствен контекст.

2. Използваната аналитична верига има евристичен характер и не предполага еднопосочен детерминизъм между география, политика и военно действие.

3. ECHEVARRIA II, A. J., 2007. *Clausewitz and Contemporary War*. Oxford: Oxford University Press.

4. GRAY, C. S., 1999. *Modern Strategy*. Oxford: Oxford University Press.

5. MEARSHEIMER, J. J., 2001. The Tragedy of Great Power Politics. New York: W. W. Norton. *CSSPlatform* [online]. Available from: https://cssplatformbytha.com/wp-content/uploads/2024/10/John_J._Mearsheimer_-_The_Tragedy_of_Great_Power_Politics_2001_W._W._Norton__Company1.pdf [01.09.2026].

REFERENCES

CLAUSEWITZ, C. von, 1984. *On War.* M. Howard and P. Paret (ed. and translated). Princeton, NJ: Princeton University Press.

HAUPT, H.-G.; KOCKA, J., 2009. *Comparative and Transnational History: Central European Approaches and New Perspectives.* New York: Berghahn Books.

KOCKA, J., 2003. *Comparison and Beyond. History and Theory*, vol. 42, no. 1, pp. 39-44. *Internet Archive* [online]. Available from: https://archive.org/details/comparativetrans0000unse_y9v4 [29.08.2026].

KROM, M.; GUYATT, N., 2022. *An Introduction to Historical Comparison*. Cambridge: Cambridge University Press. Available from: https://api.pageplace.de/

preview/DT0400.9781350123335_A40755969/preview-9781350123335_A40755969.pdf [30.08.2026].

MAHAN, A. T., 1890. *The Influence of Sea Power upon History, 1660–1783*. Boston: Little, Brown and Company. Available from: https://dn790003.ca.archive.org/0/items/seanpowerinf00maha/seanpowerinf00maha.pdf [30.08.2026].

MAHONEY, J.; RUESCHEMEYER, D. (eds.), 2003. Comparative Historical Analysis in the Social Sciences. Cambridge: Cambridge University Press. *GoogleBooks* [online]. Available from: https://books.google.bg/books?id=oT86uvC8KBEC&lpg=PR9&dq=MAHONEY%2C%20J.%20%26%20RUESCHEMEYER%2C%20D.%20(eds.)%2C%202003&lr&pg=PR9#v=onepage&q&f=false [01.09.2026].

RATZEL, F., 1897. Politische Geographie. München und Leipzig: R. Oldenbourg. *Internet Archive* [online]. Available from: https://archive.org/details/bub_gb_PXZJAAAAYAAJ/page/n19/mode/2up [01.09.2026].

THE GEOPOLITICAL DIMENSIONS OF MILITARY-HISTORICAL COMPARATIVISTICS: METHODOLOGICAL AND APPLIED ASPECTS

Abstract. The paper examines the geopolitical dimensions of military-historical comparativistics as a methodological approach to the comparative study of wars, military systems and strategic decisions in different historical and spatial contexts. Its central thesis is that geopolitical analysis should not be treated as an external supplement to military-historical comparison, but as one of its structural components. The study focuses on geographical position, strategic space, national interests, resource potential, alliance configurations and political objectives. Examples from the Napoleonic Wars, the Balkan Wars, the First World War and the Second World War demonstrate how apparently similar military phenomena acquire different meanings within different geopolitical configurations. The paper also identifies methodological limits of historical analogy and outlines the practical value of comparative analysis for contemporary strategic studies and national security.

Keywords: geopolitics; historical analogy; military art; military-historical comparativistics; national security; strategy

Dr. Radoslav Bonev, Assoc. Prof.
ORCID iD: 0009-0009-2774-2235
Department of National and International Security
Faculty of National Security and Defence
Rakovski National Defence College
82, Evlogi and Hristo Georgievi Blvd.
Sofia, Bulgaria
E-mail: r.bonev@rndc.bg

https://doi.org/10. 66334/annu26_prepofilo

ПРЕПОДАВАНЕТО НА ФИЛОСОФИЯ ВЪВ ВОЕННАТА АКАДЕМИЯ: ДИДАКТИЧЕСКИ ПРЕДИЗВИКАТЕЛСТВА И ПЕРСПЕКТИВИ

доц. д-р Радослав Бонев
Военна академия „Георги Стойков Раковски“

Абстракт. Настоящият доклад анализира дидактическите аспекти на обучението по философия във Военната академия в контекста на динамично променящата се среда за сигурност и нарастващите изисквания към подготовката на бъдещите офицери. Разглеждат се мястото и ролята на философските дисциплини при формирането на критическо и стратегическо мислене, нравствена отговорност, лидерски качества и умения за аргументирано вземане на решения. Особено внимание се отделя на съвременните дидактически подходи – проблемно-ориентираното обучение, анализа на казуси, дискусионните методи и интердисциплинарната интеграция на философията с военната история, политическите науки и науките за сигурността. Обосновава се тезата, че философското образование има съществен принос за развитието на професионалните компетентности на бъдещите офицери, като подпомага изграждането на аналитична култура, ценностна ориентация и способност за адекватно поведение в условията на сложни и неопределени ситуации. В заключение се очертават перспективи за усъвършенстване на методиката на преподаване по философия във висшето военно образова-

ние чрез прилагане на иновативни образователни практики и компетентностно ориентиран подход.

Ключови думи: философия; висше военно образование; дидактика; критическо мислене; военно лидерство; национална сигурност

Военното образование традиционно е насочено към усвояването на специализирани знания, практически умения и професионални компетентности, необходими за изпълнение на задачите на въоръжените сили. Съвременната среда за сигурност поставя обучаемите – бъдещи военни и цивилни експерти по национална сигурност и отбрана, пред ситуации, в които техническата подготовка сама по себе си не е достатъчна. Неопределеността, информационното пренасищане, ценностните конфликти, ускорените технологични промени и необходимостта от решения с висока степен на отговорност изискват способност за самостоятелна преценка, аргументация и критическа рефлексия. Именно тук философското образование придобива непосредствено професионално значение.

Философията във висшето военно образование не следва да бъде разглеждана като периферна общообразователна дисциплина, нито като исторически преглед на философски учения. Нейната дидактическа стойност се проявява тогава, когато обучаемият бъде поставен пред проблем, понятие, аргумент или ценностна дилема и бъде насърчен да изгради собствено, рационално защитимо становище. В този смисъл преподаването на философия е обучение в мислене, а не само предаване на сведения за историята на идеите.

Целта на настоящия доклад е да анализира основните дидактически предизвикателства пред преподаването на философия във Военна академия „Г. С. Раковски“ и да очертае възможности за неговото усъвършенстване. Основната теза е, че философската подготовка допринася за професионалното формиране на бъдещия офицер и цивилен експерт по национална сигурност и отбрана чрез развитие на критическо и стратегическо мислене, нравствена отговорност, аргументационна култура и способност за действие в сложни ситуации.

Спецификата на философията като учебна дисциплина произтича от нейния особен предмет (Aristotle 1998; Kant 1996). Тя не предоставя единствено готови отговори, а проблематизира основанията на знанието, действието и ценностите. Във военна образователна среда това означава да се поставят въпроси за човека, свободата, отговорността, властта, държава-

та, войната, мира, справедливостта и границите на допустимото действие. Подобни въпроси не са външни спрямо професията на офицера и цивилния експерт; те присъстват в самата логика на командването и в отношенията между военна необходимост, право и морал.

Първата функция на философското обучение е познавателна. То изгражда способност за разграничаване на понятия, предпоставки, факти, оценки и аргументи. Офицерът работи в среда, в която едно и също събитие може да бъде представено чрез различни интерпретации. Затова умението да се проверява логическата структура на твърденията и да се различава доказателство от внушение има значение за академичната подготовка и за професионалната дейност.

Втората функция е ценностно-нормативна. Военната професия е свързана с дълг, чест, дисциплина, лоялност, отговорност и законност. Философската етика позволява тези категории да бъдат осмислени не само като правила, а като принципи, между които понякога възниква напрежение. Третата функция се отнася към светогледа – философията поставя отделното професионално действие в по-широк контекст на обществото, държавата и човешкото съществуване. Оттук следва, че мястото на философията във военното образование се определя не толкова от количеството философско съдържание, колкото от качеството на интелектуалните операции, които обучаемият усвоява – дефиниране, анализ, сравнение, аргументиране, критика, оценка на алтернативи и рефлексия върху собствените предпоставки.

Първото предизвикателство е различният предварителен опит на обучаемите. Философският текст използва абстрактни понятия и често изисква работа с аргументи, които не могат да бъдат усвоени чрез механично запаметяване. За част от курсантите, слушателите и студентите това поражда усещане за дистанция между философията и практическите потребности на военната професия. Задачата на преподавателя е да преодолее тази дистанция, без да опростява дисциплината до набор от житейски примери.

Второто предизвикателство е ограниченото учебно време. Историята на философията обхваща повече от две хилядолетия, а тематичният спектър включва онтология, теория на познанието, етика, социална и политическа философия, философия на историята и философска антропология. При ограничен хорариум преподавателят е принуден да избира. **Дидактически по-продуктивно е подборът да се организира около проблемни ядра, а не около стремеж към енциклопедична изчерпателност.**

Третото предизвикателство е съотношението между авторитет и дискусия. Военната организация по необходимост е йерархична, докато

философското обучение изисква пространство за въпрос, несъгласие и аргументиран спор. Това не е противоречие, ако се разграничат институционалната дисциплина и интелектуалната самостоятелност. Академичната дискусия не отменя авторитета на преподавателя, тя го преобразува от източник на готови истини в организатор и коректив на рационалното изследване.

Четвъртото предизвикателство е влиянието на дигиталната информационна среда. Обучаемият има бърз достъп до огромно количество текстове, резюмета и автоматично генерирано съдържание. Това увеличава достъпа до информация, но не гарантира разбиране. Следователно преподаването трябва да премести акцента от възпроизвеждането към проверката на аргументи, надеждността на източници, разпознаването на логически грешки и защитата на собствена позиция.

Критическото мислене може да бъде определено като способност за съзнателна оценка на твърдения, основания и изводи (Dewey 1933; Paul & Elder 2014; Brookfield 2012). Във философската аудитория то се развива чрез въпроси от типа какво точно означава понятието, какви предпоставки съдържа тезата, какви доказателства я подкрепят, възможно ли е алтернативно обяснение и какви последици следват, ако приемем дадено твърдение. Подобна структура на мислене има пряко отношение към анализа на сложна оперативна и стратегическа информация.

Стратегическото мислене не е тъждествено на философското, но между тях съществува методологическа близост (Clausewitz 1984). И двете изискват работа с цели, средства, ограничения, последици и алтернативи. **Философията добавя способността да се поставят под въпрос самите основания на избраните цели и категории. Така обучаемият се учи не само да пита „как да постигнем целта“, но и „как е формулирана целта“, „какви ценности предполага“ и „какви непредвидени последици може да произведе“.**

Особено важно е да се избягва превръщането на критическото мислене в синоним на отрицание. Критиката във философски смисъл е проверка на основанията. Тя може да потвърди дадена теза, да я ограничи или да я отхвърли. За бъдещия офицер това означава интелектуална дисциплина – способност да различава лично предпочитание от професионална оценка и увереност от достатъчно основание.

Проблемно-ориентираното обучение е особено подходящо за философията, защото започва не от готовата теория, а от въпрос, противоречие или ситуация (Dewey 1933; Freire 2000). Вместо лекцията да представя последо-

вателно учението на Хобс например, тя може да започне с проблема за сигурността и политическия ред – какво оправдава ограничаването на индивидуалната свобода в името на общата сигурност (Hobbes 1996). След това класическият текст се въвежда като концептуален инструмент за анализ.

Казусът е мост между абстрактното понятие и конкретното решение. Във военното образование той може да бъде исторически, етически, организационен или стратегически. Важното е казусът да не бъде използван само за илюстрация на предварително известен „правилен отговор". Неговата дидактическа стойност се състои в необходимостта обучаемият да разпознае принципи в конфликт, да формулира алтернативи и да защити решение.

Историческите казуси предоставят особено богата среда за подобна работа. Решенията на командири и държавници могат да бъдат анализирани през категории като дълг, отговорност, легитимност, риск и съотношение между цел и средство. Така военната история престава да бъде само източник на факти, а се превръща в пространство за философска рефлексия. Същевременно философията получава конкретност, без да губи своята концептуална строгост.

Дискусията е естествен метод на философското обучение, но нейното качество зависи от ясни правила. Свободният разговор сам по себе си не е философски диалог. Необходими са дефиниране на тезата, разграничаване на аргумент от пример, уважение към опонента и готовност за корекция на собствената позиция. Преподавателят трябва да създаде среда, в която несъгласието е допустимо, но произволното твърдение не е достатъчно.

Сократическият тип въпрос има особена стойност – той не съобщава отговора, а разкрива противоречията в предпоставките (Brookfield 2012). В съвременната аудитория това може да се реализира чрез кратки структурирани дебати, защита на противоположни позиции, анализ на грешки при аргументацията и писмени миниатюри, в които обучаемият трябва да формулира теза и две основания в нейна подкрепа.

За военното лидерство културата на аргументиране има практическо измерение. Командирът трябва да може да обяснява замисъл, да оценява доклади, да изслушва експертни становища и да различава съществено възражение от риторичния натиск. Философската дискусия упражнява именно тази способност за организирано отношение към различието.

Една от най-перспективните посоки е интегрирането на философията с военната история, политическите науки и науките за сигурността. Подобна интеграция не означава размиване на предметните

граници. Напротив, всяка дисциплина запазва своя метод, но общият проблем се разглежда от различни равнища. Войната например може да бъде изследвана исторически като събитие, политологически като инструмент на политиката и философски като проблем на насилието, отговорността и човешката свобода.

Социалната философия позволява да се анализират институциите, властта, легитимността и обществениият ред, политическата философия – основанията на държавата и справедливостта, етиката – нормите на професионалното действие, философията на историята – смисълът и границите на историческата аналогия. Така философското обучение може да се превърне в интегративно поле, което свързва знанията, получени в различни дисциплини.

За обучаемия тази интеграция има и мотивационен ефект. Абстрактното понятие се разбира по-лесно, когато неговата аналитична стойност бъде показана върху познат професионален материал. Но преподавателят трябва да пази баланс – военният пример не бива да замества философския проблем, а да го прави видим.

Военното лидерство съдържа неизбежно нравствено измерение (Kant 1996). Правомощието да се вземат решения за други хора предполага отговорност, която не може да бъде сведена до административна процедура. Философската етика предоставя език за анализ на дълга, последствията, добродетелите, справедливостта и личната отговорност. Тя не замества правните норми и професионалните регламенти, а позволява да се разберат техните основания и граници.

В обучението е важно етическите проблеми да не се представят като абстрактни морализаторски поучения. По-продуктивно е те да бъдат формулирани като дилеми, в които различни ценности могат да влязат в напрежение – лоялност и истина, изпълнение и лична отговорност, ефективност и допустимост на средствата, сигурност и свобода. Целта не е да се релативизират нормите, а да се изгради способност за съзнателно нравствено решение.

Това има значение и за авторитета на лидера. Устойчивият авторитет не се основава единствено на формалната позиция. Той включва доверие, последователност и разбираемо основание на решенията. Философската подготовка подпомага именно способността на офицера да свързва професионалната компетентност с нравствена отговорност.

Компетентностно ориентираният подход променя въпроса от „какво съдържание е преподадено“ към „какво може да прави обучаемият със

знанието“ (Bloom 1956). При философията това означава да се оценяват не само възпроизведени определения и имена, а умения за анализ на текст, формулиране на проблем, изграждане на аргумент, сравняване на позиции и прилагане на понятия към нова ситуация.

Тестовото изпитване има своето място, особено при проверка на основни понятия и историко-философска ориентация, но не може да бъде единствен инструмент. Подходящо е съчетаването му с кратък аргументиран отговор, анализ на казус, устна дискусия или есе. Така оценяването става продължение на учебните цели, а не отделна административна процедура.

Критериите трябва да бъдат прозрачни – яснота на тезата, релевантност на аргументите, логическа последователност, коректна употреба на понятия, способност за разглеждане на възражение (Paul & Elder 2014). Това насочва обучаемия към качеството на мисленето и намалява зависимостта от механичното възпроизвеждане.

Дигиталните технологии създават нови възможности за достъп до първични текстове, електронни библиотеки, интерактивни материали и сравнителни ресурси. Те могат да подпомогнат подготовката и да освободят време за дискусия и анализ. Същевременно лесното генериране на готов текст поставя ново дидактическо предизвикателство – как да се оцени действителното разбиране на обучаемия.

Отговорът не е непременно в забраната на технологиите, а в промяната на задачите. Ако задачата изисква лично аргументиране, защита пред аудитория, сравнение с конкретен източник или последващо устно обяснение, механичното предаване на готов текст губи стойност. Така технологичната среда може да бъде използвана и като повод за обучение по интелектуална честност, проверка на източници и отговорно използване на помощни инструменти.

За философията това е особено значимо, защото дисциплината по самата си природа поставя въпроса за основанията на знанието. Дигиталната грамотност следователно трябва да бъде свързана с епистемологична грамотност – кой твърди, на какво основание, как може да бъде проверено и каква е границата между информация и знание.

Първата перспектива е по-ясното обвързване на философското съдържание с компетентностите, необходими на офицера, без философията да се превръща в обслужваща дисциплина. Това предполага учебни цели, формулирани едновременно в познавателен и професионален план – разбиране на концепция, умение за аргументация, оценка на дилема, критичен анализ на предпоставка.

Втората перспектива е разширяването на активните методи – казуси, дебати, проблемни задачи, анализ на кратки първични текстове и междудисциплинарни семинари.

Третата перспектива е създаването на устойчив набор от военноисторически и стратегически казуси, чрез които философските категории да се прилагат към реални проблеми, без да се губи историческият контекст.

Четвъртата перспектива е разумното използване на дигитални инструменти за предварителна подготовка, визуализация и самопроверка, съчетано с форми на оценяване, които изискват лично разбиране.

Петата перспектива е по-тясното взаимодействие между преподавателите по философия, военна история, лидерство, политически науки и сигурност при разработването на общи проблемни модули.

В крайна сметка иновацията в преподаването не трябва да се измерва с количеството използвани технологии. Истинската дидактическа иновация е тази, която прави обучаемия по-самостоятелен, по-точен и по-отговорен в мисленето си.

Анализът показва, че философското образование във Военната академия има потенциал да изпълнява едновременно общообразователна и професионално формираща функция. **Неговият принос се проявява в развитието на критическо мислене, аргументационна култура, ценностна ориентация и способност за работа с неопределеност.**

Дидактическият ефект се увеличава, когато преподаването се организира около проблеми и казуси, а класическите философски идеи се използват като инструменти за анализ. Дискусионните методи и интердисциплинарната интеграция позволяват на обучаемия да свърже философското понятие с военната история, политиката, сигурността и лидерството.

Едновременно с това съществуват ограничения – различна входна подготовка, ограничен хорариум, риск от прекомерна абстрактност и нови трудности, породени от дигиталното генериране на съдържание. Тези ограничения изискват не намаляване на философската сложност, а по-прецизен подбор на съдържание, ясни учебни цели и разнообразни форми на оценяване.

Преподаването на философия във висшето военно образование има смисъл тогава, когато съчетава академична строгост с професионална релевантност. Бъдещият офицер и цивилен експерт по национална сигурност и отбрана се нуждае не само от знания за философски системи, но и от навик да пита за основанията на решенията, да разпознава ценностни кон-

фликти, да оценява аргументи и да поема интелектуална и нравствена отговорност за собствената си позиция.

В динамична среда за сигурност тези способности не са допълнение към професионалната компетентност, а част от нея. Философското образование не предлага алгоритъм за всяка ситуация. Неговата сила е друга – то подготвя човека да мисли, когато алгоритъмът е недостатъчен, информацията е непълна, а решението не може да бъде отложено. Именно в това се състои една от най-съществените перспективи пред философията във Военната академия.

БЕЛЕЖКИ

1. Под „компетентностно ориентиран подход“ се разбира организация на обучението, при която усвоеното знание се свързва с наблюдаеми способности за анализ, аргументация и приложение.

REFERENCES

ARISTOTLE, 1998. *Politics.* [Translated by C.D.C. Reeve]. Indianapolis: Hackett Publishing.

BLOOM, B.S. (ed.), 1956. Taxonomy of Educational Objectives: The Classification of Educational Goals. Handbook I: Cognitive Domain. New York: Longmans, Green. *Internet archive*. [online]. Available from: https://archive.org/details/taxonomyofeducat0000bloo_o9o7/page/n211/mode/2up. [viewed: 16.08.2026].

BROOKFIELD, S.D., 2012. *Teaching for Critical Thinking.* San Francisco: Jossey-Bass. Springer. [online]. Available from: https://link.springer.com/chapter/10.1057/9781137378057_31. [viewed: 17.08.2026].

CLAUSEWITZ, C., 1984. *On War. Edited and translated by M. Howard and P. Paret*. Princeton, NJ: Princeton University Press. Available from: https://www.usmcu.edu/Portals/218/EWS%20On%20War%20Reading%20Book%201%20Ch%201%20Ch%202.pdf. [viewed: 18.08.2026].

DEWEY, J., 1933. *How We Think*. Boston: D.C. Heath. Available from: https://bef632.wordpress.com/wp-content/uploads/2015/09/dewey-how-we-think.pdf. [viewed: 19.08.2026].

FREIRE, P., 2000. *Pedagogy of the Oppressed. 30th anniversary ed.* New York: Continuum. Available from: https://files.libcom.org/files/Paulo%20Freire,%20Myra%20Bergman%20Ramos,%20Donaldo%20Macedo%20-%20Pedagogy%20of%20the%20Oppressed,%2030th%20Anniversary%20Edition%20(2000,%20Bloomsbury%20Academic).pdf. [viewed: 20.08.2026].

HOBBES, T., 1996. *Leviathan. Edited by R. Tuck.* Cambridge: Cambridge University Press. Available from: https://iranacademia.com/wp-content/uploads/2023/12/Thomas-Hobbes-Leviathan-1996.pdf. [viewed: 20.08.2026].

KANT, I., 1996. *Practical Philosophy.* [Edited and translated by M. J. Gregor]. Cambridge: Cambridge University Press. Available from: https://mavidano.wordpress.com/wp-content/uploads/2021/02/critique-of-practical-reason-kant-1.pdf. [viewed: 21.08.2026].

PAUL, R. & ELDER, L., 2014. *Critical Thinking: Tools for Taking Charge of Your Professional and Personal Life. 2nd ed.* Upper Saddle River, NJ: Pearson. Available from: https://ptgmedia.pearsoncmg.com/images/9780133115284/samplepages/0133115283.pdf. [viewed: 22.08.2026].

WEBER, M., 1978. *Economy and Society: an Outline of Interpretive Sociology.* Berkeley: University of California Press. [Internet archive. Online]. Available from: https://archive.org/details/MaxWeberEconomyAndSociety. [viewed: 21.08.2026].

TEACHING PHILOSOPHY AT THE MILITARY ACADEMY: DIDACTIC CHALLENGES AND PERSPECTIVES

Abstract. The paper analyses the didactic aspects of teaching philosophy at the Military Academy in the context of a dynamically changing security environment and increasing requirements for the education of future officers. It examines the role of philosophical disciplines in developing critical and strategic thinking, moral responsibility, leadership qualities and reasoned decision-making. Particular attention is paid to problem-based learning, case analysis, discussion methods and interdisciplinary integration with military history, political science and security studies. The paper argues that philosophical education contributes substantially to the professional competences of future officers by fostering analytical culture, value orientation and the ability to act adequately under complex and uncertain conditions. It concludes by outlining perspectives for improving philosophy teaching in higher military education through innovative educational practices and a competence-oriented approach.

Keywords: philosophy; higher military education; didactics; critical thinking; military leadership; national security

Dr. Radoslav Bonev, Assoc. Prof.
ORCID iD: 0009-0009-2774-2235
Department of National and International Security
Faculty of National Security and Defence
Rakovski National Defence College
82, Evlogi i Hristo Georgievi Blvd.
E-mail: r.bonev@rndc.bg

https://doi.org/10. 66334/annu26_prograpaosi

ПРОГРАМНО И АПАРАТНО ОСИГУРЯВАНЕ НА АВТОНОМНИ БЕЗПИЛОТНИ ЛЕТАТЕЛНИ СИСТЕМИ

Севдалин Стойков[1], Венелин Рашков[2], Александър Колев[3], Иван Иванов[3]
[1)] Военна академия „Георги Стойков Раковски“
[2)] Министерство на отбраната
[3)] Институт по отбрана „Професор Цветан Лазаров“

Абстракт. Безпилотните летателни системи (Unmanned Aerial Systems – UAS) заемат значително място във военното дело и се представят като важен фактор при завоюване на военно превъзходство. В зависимост от решаваните задачи UAS подлежат на разширена класификация, отразяваща основните им способности. В настоящия материал авторите правят опит да изяснят различните подходи на приложение по линия на дистанционно управлявани апарати или автономно функциониращи такива. Отделено е внимание на програмното и апаратно осигуряване на UAS за функциониране в автономен режим. Приведени са резултати от проведени експерименти.

Ключови думи: автономни; безпилотни; летателни; системи

I. Увод

Безпилотните летателни системи представляват „система от системи“, като основните такива са наземна контролна станция (*Ground Control Station – GCS*) и безпилотен летателен апарат (*Unmanned Aerial Vehicle – UAV*). Приложението на *UAS* може да бъде разглеждано в светлината на два основни подхода – дистанционно управляеми дронове, известни още като *First Person View (FPV)*, или автономни с различна степен на автоматизация в отделните фази на изпълняваната мисия.

Системите тип *FPV* се отличават с пряка ангажираност на пилота по време на полета, всички действия с управляващите органи се изпълняват незабавно от апарата и контролът на полета се основава на визуална връзка през специално поддържана видеосистема. Тук *GCS* се представя в минимална конфигурация от дистанционно управление (*Remote Control – RC*) и видеомонитор (*FPV glasses*).

Автономните системи от своя страна могат да се разглеждат като следващо, по-високо ниво на развитие на управляваните дронове. В това приложение *GCS* е организирана като компютъризирано работно място, оборудвано със специфичен софтуер и хардуер. Въздушната компонента на автономната система е дрон с разширена функционалност, която включва усъвършенствана навигационна система. Автономните системи също така предполагат висока степен на автоматизация по отношение на обмена на оперативно-тактически данни към армейски системи за командване и управление (C4I).

В настоящия материал, част от разширено научно изследване, авторите изследват възможностите за конфигуриране на дрон тип квадрокоптер с повишена автономност и представят числени данни от проведените полеви експерименти.

II. Програмно осигуряване

2.1. Програмно осигуряване на GCS

Софтуерният компонент на *GCS* поддържа процеса на първоначално конфигуриране на *UAS*, наземно тестване на винто-моторните групи, навигационната и комуникационна подсистема, задаване на правила за безопасност по време на полета и създаване на полетни планове за автономно изпълнение.

Типична последователност на провеждане на автономна мисия след зареждане на полетен план в полетния контролер е: активиране на апара-

та (на англ. *Arming*); подаване на команда за излитане (на англ. *TakeOff*); преминаване на полета в автоматичен режим. Изпълнението на мисията се проследява през телеметрична обратна връзка и се визуализира с подвижна икона на апарата върху електронна географска карта. Автономната мисия при необходимост може да бъде поставена на пауза, операторът, подобно на *FPV* системата, да извърши полагащите се действия, след което изпълнението на автономната мисия да бъде продължено. Всяка автономна мисия обикновена завършва с команда за автоматично завръщане към мястото на излитане и след това автоматично приземяване (на англ. *ReturnToLand – RTL*).

Известни и широко използвани *open-source* програмни продукти (извън тясно специализираните с чисто военно предназначение), които поддържат автономност при *UGS*, са *Mission Planner*, *QGroundControl*, *iNav* и др.

2.2. Програмно осигуряване на UAV

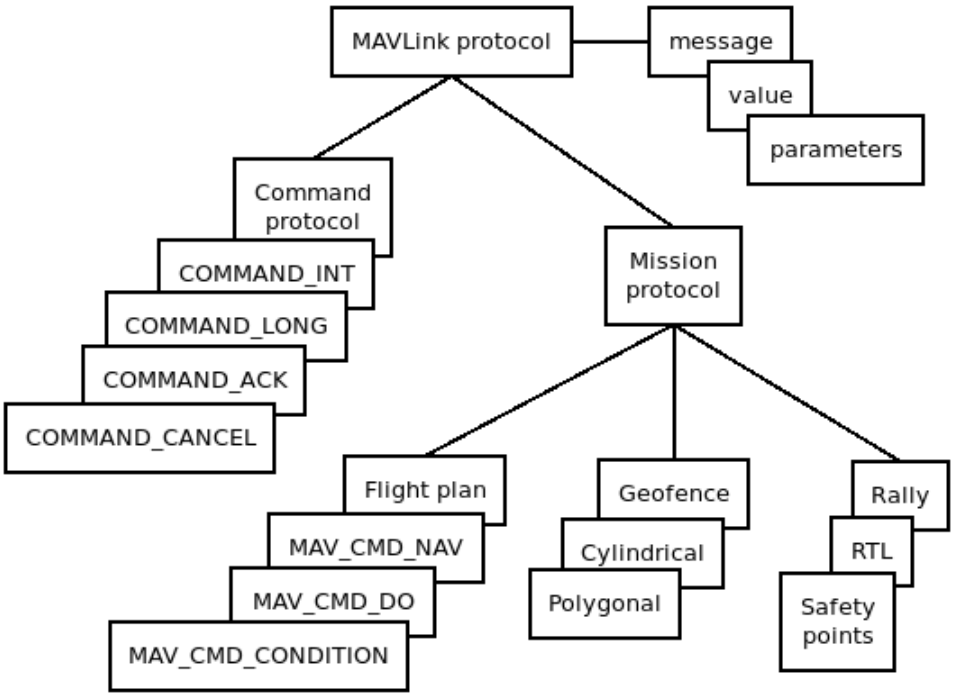
За основно програмно осигуряване на *UAV* може да се определи бинарният код (на англ. *firmware*), който се зарежда еднократно в полетния контролер на дрона и свойствата му подлежат на конфигуриране. Възможностите на полетния контролер – включително и тези за осигуряване на автономност, зависят на първо място от използвания централен процесор (на англ. *Central Processing Unut – CPU*). Докато при апаратите от тип *FPV*, е достатъчно *CPU* да е от серията *STM32F4*, то за автономно приложение се прилагат *CPU* с повишена производителност, например от серията *STM32H7*. Често използвани *open-source firmware*, съвместими със софтуера *Mission Planner* и *QGorundControl*, са *Ardupilot* и *PX4-Autopilot*. Пълен преглед на разширената функционалност на полетния контролер в зависимост от приложеното *CPU* може да се достъпи на страницата *ArduPilot Custom Build*.

Вторична, поддържаща софтуерна подсистема на борда на *UAV* може да се организира чрез включване на допълнителен компютър (на англ. *Companion Computer – CC*). Системата на CC се прилага в случаите, когато специфична функционалност не е предвидено да работи на полетния контролер и затова се прилага допълнително компютърно устройство от типа *SingleBoardComputer (SBC)* или *SystemOnChip (SoC)*. Типични представител на използваните *SBC* е *Raspberry Pi*, а на *SoC* са устройства от серията *ESP32*. Вписването на CC в общата логика на функциониране на автономния апарат е чрез информационен обмен, от една страна, към по-

летния контролер, от друга страна – към допълнителен бордови хардуер и изпълнителни устройства. В изследваните от авторите конфигурации информационният обмен между бордовите модули на автономния апарат, както и към *GCS* се осъществява с прилагане на протокола *MAVLink*.

2.3. Протокол MAVLink

Един наложил се протокол за работа на *UAS* е *Micro Air Vehicle Link (MAVLink)*.[1] Предназначен е за комуникация с *UAV*, полетния контролер, компонентите на бордовата апаратура, допълнителен компютър *CC* и *GCS*. Протоколът е разработен като *open-source* проект, първоначално насочен към малки безпилотни апарати. През годините се издават нови версии на протокола, също така се появяват по-специализирани клонове, насочени към самолетен и мулти-пропелерен тип въздушни, наземни и подводни безпилотни апарати. На фигура 1 е показана обобщената структура на протокола.



Фигура 1. Обобщена структура на протокол *MAVLink*

Основен компонент в протокола е съобщението *message*. Съобщението е бинарно кодирано и се състои от числови стойности. Стойността *value* е цифровият код на изпълняваната команда, *parameters* са седем на брой числови стойности с различно значение в зависимост от изпълняваната команда.

Отличават се две групи протоколни функции – *Command* и *Mission*. Функционалната група *Command* описва вида на подаваните за изпълнение команди. Типовете *COMMAND_INT* и *COMMAND_LONG* са подлежащите на изпълнение команди. Различават се по възможността за задаване на прецизни или не толкова стойности на свързаните с командата параметри. При командите тип *LONG* всички числени параметри са от тип *float*, което позволява прецизно задаване на стойности, например координати. При командите *INT* за повечето параметри се очакват стойности от тип *integer.*

С подаване на *COMMAND_ACK* се предизвиква връщане на информация за резултата от изпълнението на предишна команда. *COMMAND_CANCEL* прекъсва изпълнението на текуща зададена команда.

Функционалната група *Mission* поддържа автономната функционалност на *UAS*. Групата *Flight plan* съдържа навигационни команди *MAV_CMD_NAV*, команди за непосредствено изпълнение *MAV_CMD_DO* и команди, които следва да се изпълнят при наличие на достигнато условие – *MAV_CMD_CONDITION*. Групата *Geofence* е част от системата за сигурност при провеждане на автономни мисии. Пространствените информационни структури *Cylindrical* и *Polygonal* дефинират зоните, в които на безпилотния апарат е разрешено да оперира. Групата от команди *Rally* също е част от системата за осигуряване на безпроблемен полет. *Return to Land (RTL)* поддържа координатите на позицията, от която *UAV* излита, така, че при необходимост апаратът самостоятелно да се върне и приземи в началната точка на полетния план. *Safety points* са предварително дефинирани сигурни позиции, към които *UAV* може да се придвижи при изпълнение на полетния план или при команда от оператора.

III. Апаратно осигуряване

3.1. Осигуряване на базова летателна годност

Разглеждан от авторите е случаят, когато *UAS* не е придобита като цялостно завършена система, а *UAV* е частично или напълно конструиран апарат със собствени якостни, механични и други конструктивни особености. Визирани са разработки на Института по отбрана на ново констру-

иран квадрокоптерен микродрон от типоразмер 2.5 inch и извършена конверсия чрез замяна на полетния контролер от *FPV* към автономен дрон от типоразмер 10 inch.

Особено важно е първият полет да протече без конфликтни ситуации, апаратът да е в състояние да излети, да се задържи до минута във въздуха и плавно да се приземи. Софтуерът *Mission Planner* подготвя подходящи стойности за избрани параметри от менюто *Setup Initial Tune Parameters*. За входни данни се въвеждат характеристиките на дрона „Размер на витлото“, „Тип батерия“, брой на последователно свързаните клетки на батерията, волтаж на напълно заредена клетка и допустим волтаж на разредена клетка.

В таблица 1 са показани определените стойности на съответните значими параметри за двата изследвани апарата. Критично за възможността за излитане е запазване на стойността на параметъра *INS_GYRO_FILTER*. При големи разлики спрямо показаните в таблицата за двата апарата, дронът пада веднага и не може да се задържи във въздуха.

Таблица 1. Стойности за базова летателна годност

Параметър	***Дрон 2.5 inch***	***Дрон 10 inch***
ATC_ACCEL_P_MAX	200200	116700
ATC_ACCEL_R_MAX	200200	116700
ATC_ACCEL_Y_MAX	33800	27000
ATC_RAT_PIT_FLTD	67	21
ATC_RAT_PIT_FLTT	67	21
ATC_RAT_RLL_FLTD	67	21
ATC_RAT_RLL_FLTT	67	21
ATC_RAT_YAW_FLTT	67	21
BATT_ARM_VOLT	6.7	20.3
BATT_CRT_VOLT	6.4	19.2
BATT_LOW_VOLT	6.6	19.8
INS_GYRO_FILTER	134	42
MOT_BAT_VOLT_MAX	8.4	25.2
MOT_BAT_VOLT_MIN	6	18
MOT_THST_EXPO	0.38	0.6
MOT_THST_HOVER	0.2	0.2

3.2. Постигане на оптимална полетна конфигурация

След като е постигната базова летателна годност, следва да се извършат проверки и при необходимост прецизиране на параметрите, които

отговарят за нивото на вибрации в конструкцията, осцилации по време на полет и наличие на електромагнитна интерференция.

3.2.1 Определяне на нивото на вибрации в конструкцията на дрона

Един от чувствителните компоненти в полетния контролер на дрона е инерциалният сензор (на англ. *Inertial Measurement Unit – IMU*), който пряко отговаря за ориентацията на дрона в пространството по време на полет. Този високо чувствителен прибор силно се влияе от вибрациите в конструкцията, наличието на които може да доведе до неправилни показания и оттам до катастрофално прекъсване на полета. Емпирично е определено, че нивото на вибрации, най-силно по време на излитане, не бива да превишава повече от 30 m/s^2 по всяка една от трите пространствени оси.

Определянето на нивото на вибрациите в програмата *Mission Planner* се определя от менюто *Setup Compass/Motor Calibration*. Предложената методика е плавно повишаване на подаваната към двигателите мощност и отчитане на получените вибрации. В таблица 2 са показани вибрационните стойности по трите оси за експерименталния 10 inch дрон.

Таблица 2. Ниво на вибрация при излитане

По ос X	***По ос Y***	***По ос Z***
17,45 m/s^2	6,60 m/s^2	21,92 m/s^2

Получените експериментални стойности показват, че нивото на вибрация за дрона 10 inch е в допустимите граници.

3.2.2 Наличие на осцилации при полет

Ефектът „осцилиране“ на дрона по време на полет се изразява в периодично паразитно движение на апарата в хоризонтална плоскост или по вертикалната ос. Това паразитно движение може да е зрително доловимо или да се наблюдава като специфична периодична промяна в звука на двигателите. Според материала *Ardupilot Initial Tunning Flight* не трябва да се провеждат полети при наличие на осцилации, докато последните не се отстранят. Предложената методика за отстраняване на осцилациите е да се извърши серия от пробни полети и след всеки от тези полети да се коригират стойностите на параметрите, отговарящи за работата на *PID* регулатора на полетния контролер.

При първия полет на 10 inch дрона е наблюдавана осцилация с отчетливо звуково изражение. Методиката за отстраняване на осцилации е приложена при серия от тестови полети. Съответните параметри на *PID* регулатора са показани в таблици 3 и 4.

Таблица 3. *PID* параметри в равнина XY

Параметър	*Начална стойност*	*Крайна стойност*
ATC_RAT_PIT_P	0.135	0.0169
ATC_RAT_PIT_I	0.135	0.0169
ATC_RAT_PIT_D	0.0036	0.0004
ATC_RAT_RLL_P	0.135	0.0169
ATC_RAT_RLL_I	0.135	0.0169
ATC_RAT_RLL_D	0.0036	0.0004

Таблица 4. PID параметри по ос Z

Параметър	*Начална стойност*	*Крайна стойност*
PSC_ACCZ_I	1	0.25
PSC_ACCZ_P	0.5	0.25
PSC_VELZ_P	5	5
PSC_POSZ_P	1	1

Получените крайни стойности на съответните параметри водят до отстраняване на нежеланото явление „осцилации“ по време на полет на дрона.

3.2.3 Компенсация на електромагнитната интерференция

В състава на навигационната подсистема на автономния *UAV* е включен електронен магнитен компас (на англ. *Electro-Magnetic Compass – EMC*). Нарушения в работата на *EMC* са крайно нежелателни при провеждане на автономни полети, защото при ниска хоризонтална скорост може да рефлектират в неправилно определяне на азимута, под който се движи дронът, и да се затрудни достигането на следващ *waypoint*. Статично калибриране на *EMC* се извършва при първоначалната подготовка за полети, но влиянието на електромагнитната интерференция при променливо натоварване на електродвигателите не трябва да се пренебрегва. В наблюдавани експериментални условия разликата в определяне на азимута в статично положение спрямо положение с натоварени електродвигатели може да достигне до десетки градуси. За компенсация на електромагнитната интерференция в софтуерния пакет на *Ardupilot* е предвиден онлайн инструмент *MAGFit in flight compass calibration*.

Входни данни за определяне на стойностите на параметрите, отговорни за компенсиране на електромагнитната интерференция, се съдържат в т.нар. *log* файл. Основно изискване за пълноценно прилагане на *log* файла е този файл да бъде записан по време на продължителен полет на дрона,

при който полет дронът да се движи под различен азимут и при променливо натоварване на двигателите. В таблица 5 са показани стойностите на параметрите, които участват в определяне на азимута на движение на дрона при изпълнение на автономна мисия.

Таблица 5. Компенсация на електромагнитната интерференция

Параметър	***Статично калибриране***	***Калибриране In Flight***
COMPASS_OFS_X	-640.1586475989176	-513.7130652226815
COMPASS_OFS_Y	-151.721410952064	-134.87008333581937
COMPASS_OFS_Z	-200.41756009216573	-121.9991969731816
COMPASS_DIA_X	1	0.9708358311140457
COMPASS_DIA_Y	1	0.9906909871255121
COMPASS_DIA_Z	1	1.0384731817604427
COMPASS_ODI_X	0	-0.028130090677974853
COMPASS_ODI_Y	0	-0.06260911151318414
COMPASS_ODI_Z	0	-0.0020571481533834227
COMPASS_MOT_X	0	-12.276848893010298
COMPASS_MOT_Y	0	-1.3516194568406061
COMPASS_MOT_Z	0	-11.684859334592922
COMPASS_SCALE	1	1.0188026344715733

IV. Заключение

В материала е извършено изследване на възможностите за конфигуриране на *UAV* от квадрокоптерен тип в състава на високотехнологична *UAS* така, че да придобие свойства за автономно изпълнение на летателни мисии. Последователно са разгледани програмната и апаратната страна в процеса на конфигуриране. Изследвани са възлови положения за осигуряване на базова летателна годност и са експериментирани средствата за последваща оптимизация на избрана полетна конфигурация. Посочените числени резултати са получени вследствие на продължителна експериментална работа и извършване на многобройни тестови полети на територията на войскови полигони в разположение на Българската армия.

Получените положителни резултати дават увереност в способностите на авторския екип за конструиране на пълноценни автономни *UAV*, също е пример за успешна конверсия на *FPV* дрон към такъв с автономна функционалност. Проведените дотук изследвания се разглеждат като една успешна стъпка в посока придобиване на по-голяма автономна функционалност, включваща елементи на използване на *Artificial Intelligence (AI).*

Acknowledgements. This work was supported by the NSP DS program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

БЕЛЕЖКИ

1. ArduPilot, 2024. Mission Planner Advanced Installation. *ArduPilot* [online] [last viewed 2026-09-22]. Available from: https://ardupilot.org/planner/docs/mission-planner-advanced-installation.html; QGroundControl, 2019. Homepage. *QGroundControl* [online] [last viewed 22.09.2026]. Available from: https://qgroundcontrol.com; iNav Configurator, 2026. Homepage. *iNav Configurator* [online] [last viewed 22.09.2026]. Available from: https://inavconfigurator.com

2. ArduPilot, N/A. ArduPilot Firmware builds. *ArduPilot* [online] [last viewed 22.09.2026]. Available from: https://firmware.ardupilot.org

3. GitHub, 2026. PX4-Autopilot. *GitHub* [online] [last viewed 22.09.2026]. Available from: https://github.com/px4/px4-autopilot

4. ArduPilot, N/A. ArduPilot CustomBuild. *ArduPilot* [online] [last viewed 22.09.2026]. Available from: https://custom.ardupilot.org

5. ArduPilot, N/A. ArduPilot CustomBuild. *ArduPilot* [online] [last viewed 22.09.2026]. Available from: https://custom.ardupilot.org

6. MAVLink, 2026. MAVLink XML File Schema/Format. *MAVLink* [online] [last viewed 22.09.2026]. Available from: https://mavlink.io/en/guide/xml_schema.html

7. MAVLink, 2026. Command Protocol. *MAVLink* [online] [last viewed 22.09.2026]. Available from: https://mavlink.io/en/services/command.html

8. MAVLink, 2026. Command Protocol. *MAVLink* [online] [last viewed 22.09.2026]. Available from: https://mavlink.io/en/services/command.html

9. MAVLink, 2026. Mission (Plan) Protocol. *MAVLink* [online] [last viewed 22.09.2026]. Available from: https://mavlink.io/en/services/mission.html

10. ArduPilot, N/A. ArduPilot MAGFit in flight compass calibration. *ArduPilot* [online] [last viewed 22.09.2026]. Available from: https://firmware.ardupilot.org/Tools/WebTools/MAGFit

11. ArduPilot, N/A. ArduPilot MAGFit in flight compass calibration. *ArduPilot* [online] [last viewed 22.09.2026]. Available from: https://firmware.ardupilot.org/Tools/WebTools/MAGFit

12. Ardupilot, 2024. Ardupilot Initial Tunning Flight. *Ardupilot* [online] [last viewed 22.09.2026]. Available from: https://ardupilot.org/copter/docs/initial-tuning-flight.html

SOFTWARE AND HARDWARE PROVISION FOR AUTONOMOUS UNMANNED AERIAL SYSTEMS

Abstract. Unmanned Aerial Systems (UAS) play a vital role in military operations and are a key factor in achieving military superiority. Depending on the tasks performed, UAS are subject

to a broad classification reflecting their primary capabilities. In this article, the authors examine various operational approaches, distinguishing between remotely piloted aircraft and those that operate autonomously. Special attention is paid to the software and hardware required for UAS operation in autonomous mode. Results from conducted experiments are presented.

Keywords: autonomous; unmanned; aerial; systems

Dr. Sevdalin Stoykov
ORCID iD: 0000-0001-7861-9039
Defence Advanced Research Institute
Rakovski National Defence College
82, Evlogi and Hristo Georgievi Blvd.
Sofia, Bulgaria
E-mail: s.stoykov@rndc.bg

Colonel Venelin Rashkov, PhD student
ORCID iD: 0009-0001-5414-9113
Communication and Information Systems Department
Ministry of Defense
3, Dyakon Ignatiy St.
Sofia, Bulgaria
E-mail: v.rashkov@mod.bg

Dr. Alexander Kolev, Assoc. Prof.
ORCID iD: 0000-0002-9211-2717
Development of C4I Systems Directorate
Bulgarian Defense Institute "Professor Tsvetan Lazarov"
2, Professor Tzvetan Lazarov Blvd.
Sofia, Bulgaria
E-mail: a.kolev@di.mod.bg

Dr. Ivan Ivanov, Assoc. Prof.
ORCID iD: 0009-0002-1304-1306
Development of C4I Systems Directorate
Bulgarian Defense Institute "Professor Tsvetan Lazarov"
2, Professor Tzvetan Lazarov Blvd.
Sofia, Bulgaria
E-mail: i.p.ivanov@di.mod.bg

https://doi.org/10. 66334/annu26_sustotnstrat

ОТ СЪСТОЯНИЕ КЪМ ОТНОШЕНИЕ: СТРАТЕГИЗАЦИЯТА НА ИКОНОМИЧЕСКАТА СИГУРНОСТ ПРИ СТРАТЕГИЧЕСКА ВЗАИМОЗАВИСИМОСТ

д-р Станимир Станев
Шуменски университет „Епископ Константин Преславски“

Абстракт. Литературата за международната взаимозависимост и геоикономическата мощ показва, че икономическите връзки могат едновременно да създават взаимни ползи и да пораждат асиметрични зависимости, стратегически уязвимости и възможности за принуда. По-слабо теоретизиран остава въпросът как промяната от безличен системен риск към риск, зависещ от избора и поведението на конкретни външни участници, изменя логиката на институционалната защита. Настоящата статия използва понятието „стратегизация на икономическата сигурност“ за процеса, при който институции, организирани преимуществено около общи правила, започват системно да диференцират решенията си според идентичността, способностите и очакваното поведение на конкретни външни участници. Докладът предлага теоретичен модел, който разграничава стратегизацията от секюритизацията, геополитизацията и използването на икономически инструменти за постигане на стратегически цели, и обяснява условията за възникване на стратегическа заплаха, институционалната адаптация в рамките на запазена взаимозависимост и разпределението на стратегическата преценка.

Ключови думи: геоикономика; икономическа сигурност; институционална адаптация; стратегизация; стратегическа взаимозависимост; стратегическа преценка

I. Увод

Следвоенната международна икономическа архитектура се развива върху разбирането, че ползите и рисковете на трансграничната взаимозависимост могат да бъдат управлявани чрез общи правила и институции (Ruggie 1982; Keohane 1984). Тази традиция не изключва властта, като Hirschman (1945) показва как асиметричната търговска зависимост се преобразува в политическо влияние, Strange (1988) развива понятието за структурна мощ, Baldwin (1985) систематизира използването на икономически инструменти за постигане на стратегически цели, а Kirshner (1995) анализира паричната принуда. Съвременните глобални производствени, финансови, технологични и информационни мрежи задълбочават тази логика – те едновременно създават икономически способности и разпределят неравномерно контрола върху тях (Farrell, Newman 2019).

Оттук възниква специфичен проблем за икономическата сигурност. Държавата трябва да запази достъпа до трансгранични структури, от които зависят значими икономически способности, и едновременно да се защити от възможността зависимостта от същите структури да бъде използвана за ограничаване на нейната свобода на действие. Прекъсването или съществеността ограничаване на взаимозависимостта може да отслаби именно способностите, които политиката за сигурност се стреми да защити, запазването на съществуващата взаимозависимост без допълнителни защитни механизми, от друга страна, може да остави стратегически уязвимости неуправлявани. Това оформя тезата, че основният институционален проблем не е изборът между интеграция и отделяне, а как защитата да бъде реорганизирана вътре в система, която едновременно произвежда икономическа способност и стратегическа уязвимост.

Съвременната литература описва различни страни на тази трансформация. Farrell и Newman (2019) показват как контролът върху централни мрежови възли създава способности за наблюдение и ограничаване на достъпа. Изследванията върху ЕС проследяват геополитизирането на търговската и инвестиционната политика, геоикономическия обрат на единния пазар и възникването на нови защитни инструменти (Meunier, Nicolaïdis 2019; Herranz-Surrallés, Damro, Eckert 2024; Haroche 2024; Bauerle Danzman, Meunier 2024). По-слабо разработен остава въпросът как институционалната защита се променя, когато рискът системно зависи от способностите и вероятното поведение на конкретен стратегически участник.

Докладът обозначава тази промяна в логиката на институционалната защита с понятието „стратегизация на икономическата сигурност“ и изследва условията, при които тя възниква. Подобна конструкция изисква обаче предварително разграничение между икономически проблем и проблем на сигурността. Ако всяка неблагоприятна икономическа последица бъде квалифицирана като заплаха за сигурността, понятието за стратегизация би загубило аналитичната си стойност. Baldwin (1997) развива тази постановка в систематична аналитична схема, според която всяко съдържателно твърдение за сигурност трябва да уточнява чия сигурност се защитава, кои ценности са предмет на защита, каква степен на сигурност се търси, срещу какви заплахи, с какви средства, при каква цена и в какъв времеви хоризонт.

Тази логика е особено важна за икономическата сигурност. Ако всяка инфлация, безработица, бюджетен дефицит, зависимост от внос или банков риск бъде обозначен като „заплаха за сигурността“, границата между икономическа политика и политика на сигурност се размива. Baldwin (1997) предлага дисциплиниращ критерий: трябва да бъдат уточнени референтният обект, защитаваните ценности, заплахата, средствата, степента, цената и времевият хоризонт на сигурността. Стратегизацията не означава просто разширяване на кръга от икономически проблеми, а промяна в характера на заплахата и вследствие на това в логиката на институционалната защита.

Настоящото изследване свързва две измерения – икономическата сигурност като защитено състояние и сигурността като релационно взаимодействие. Стратегизацията обозначава промяна в начина, по който желаното състояние се осигурява, когато заплахата започне да зависи от способностите, избора и очакваната реакция на конкретен стратегически участник. Приносът не е твърдението, че икономическата взаимозависимост може да бъде стратегически използвана – това е установено в литературата, нито претенцията за новост на самата дума „стратегизация“, която вече се среща в по-нови геоикономически изследвания (Babić 2025; Friedrich, Oers, Miorner, Fuenfschilling 2026). Промяната настъпва, когато защитата започне да отчита възможността друг участник целенасочено да използва, ограничи или преобразува съществуващото икономическо отношение и когато неговият бъдещ избор се превърне в релевантна променлива за оценката на риска.

II. Икономическата сигурност между състояние и релационно взаимодействие

Значителна част от литературата концептуализира икономическата сигурност като състояние на защитеност на националната икономика и на

способностите, които тя осигурява. В българската литература Велкова разглежда икономическата сигурност като материална основа на националната сигурност (Velkova 2022, pp. 9-10), Маринов (Marinov 2014, p. 92) акцентира върху устойчивостта на икономическата система, а Петев (Petev 2021) и Йоцов (Yotsev 2025a; Yotsev 2025b) развиват рискови и приложни измерения. Предимството на тази перспектива е, че ясно определя какво трябва да бъде защитено и кои качества на системата следва да бъдат съхранени.

Ограничението на перспективата, която разглежда сигурността преди всичко като състояние на защитеност, не е, че тя непременно изключва противник, а че определението на желаното състояние само по себе си не разграничава достатъчно причинните механизми, чрез които то може да бъде нарушено. Прекъсване на критична доставка вследствие на природно бедствие, технологична авария или пазарен фалит и прекъсване вследствие на целенасочено решение на друга държава могат да произведат сходен непосредствен икономически резултат, но представляват различни проблеми на сигурността. В първия случай централният проблем е устойчивостта на системата към шок, във втория рискът зависи и от избора на друг участник и придобива релационно и стратегическо измерение.

Релационното разбиране има дълбоки основания в литературата. Слатински (Slatinski 2000, p. 4) свързва сигурността с конфликт, интереси и сила. Hirschman (1945) показва политическите последствия на асиметричната зависимост, Keohane и Nye (1977) разграничават чувствителност и уязвимост според цената на адаптацията, а Farrell и Newman (2019) добавят мрежовото измерение. Уязвимостта придобива характер на релационна стратегическа заплаха, когато неблагоприятният резултат зависи не само от системните характеристики, а и от контрола, способностите и избора на конкретен участник.

Полезно разграничение между опасност и заплаха се съдържа и в българската литература по сигурността. Коджахристов (Kodzhahristov 2025, pp. 92-94) отделя неумишлената вътрешна опасност от умишлената вътрешна заплаха и свързва последната с достъп, способност и мотивация на конкретен участник. Подобна постановка се среща и в по-ранно изследване на автора, където заплахата е определена като конкретно-адресна и персонифицирана, а опасността като хипотетична и неадресирана (Stanev 2015, pp. 63-64). Настоящият доклад развива тази линия, без да приема доказаното намерение за необходимо условие: достатъчни са контролът върху зависимостта, способността тя да бъде използвана и значима последица за защитаван интерес. Луански (Lulanski 2024, p. 108) също подчертава

значението на изпреварващи действия, способни да предотвратят блокиране на националните икономически интереси.

Това разграничение предотвратява механичното секюритизиране на икономическата политика. Копенхагенската школа обяснява как даден въпрос се конструира като въпрос на сигурността (Buzan, Wæver, Wilde 1998), но това не обяснява как той се управлява институционално. Изследванията на ЕС вече показват геоикономическа адаптация чрез нови инструменти, наслояване на компетентности и секюритизация на икономическото управление (Couvreur 2025; Heldt, Meunier 2026). По-слабо разработен остава механизмът, чрез който икономическата експозиция се интерпретира като риск, който зависи от поведението и възможностите на конкретен външен участник, и тази интерпретация се превръща в устойчива институционална компетентност.

Разбирането на икономическата сигурност като защитено състояние и анализът на заплахата, като отношение между конкретни участници не са алтернативни подходи, а взаимно допълващи се равнища на анализа. Първото позволява да се определи какво трябва да бъде защитено, а второто – спрямо кого, в рамките на каква зависимост и чрез какъв механизъм може да възникне стратегически релевантна заплаха. Стратегизацията свързва двете: тя започва, когато защитата на желаното икономическо състояние изисква системна оценка на конкретната зависимост, участника, който може да я контролира, и вероятното му поведение. От тази точка следващият раздел преминава към трите звена на предложения механизъм – структурна експозиция, стратегическа интерпретация на риска и институционализиране на стратегическата преценка.

III. Понятието стратегизация на икономическата сигурност

Стратегизация на икономическата сигурност е процесът, при който институционалната защита на национално значими икономически способности започва да се организира спрямо риск, чиито вероятност и последици зависят от стратегическия избор на друг участник, така че ефектът на защитната мярка трябва да бъде оценяван и спрямо очакваната реакция на този участник. Стратегизацията има наблюдаемо институционално проявление, когато оценката на идентичността, способностите, интересите и вероятното поведение на конкретен външен участник бъде формално включена в правила, компетентности, процедури или организационни механизми за управление на икономически отношения, значими за защитаваните национални интереси.

Предложеният механизъм съдържа три аналитично различими звена. Първото е структурната експозиция: между участниците съществува икономическо отношение, чието прекъсване, ограничаване, манипулиране или преобразуване може съществено да засегне защитавана национална способност. Структурната експозиция е материално условие за стратегизацията, но сама по себе си не е достатъчна – взаимозависимостта може да създава уязвимост, без тя да бъде интерпретирана като резултат от стратегическо действие.

Второто звено е стратегическата интерпретация на риска. Защитаващият се участник започва да оценява вероятността или тежестта на неблагоприятния резултат като зависещи не само от пазарна динамика, технологичен отказ или друг безличен процес, а и от избора, способностите, и вероятното поведение на друг участник. Именно тук обикновеният риск от взаимозависимостта придобива стратегическо измерение.

Третото звено е институционализирането на стратегическата преценка. Стратегическата интерпретация престава да бъде единична политическа реакция и се превежда в устойчиви правила, компетентности, процедури, информационни изисквания или организационни структури. Тази стъпка отделя стратегизацията като институционално явление, както от самото наличие на международно сътрудничество, така и от еднократното използване на икономически инструмент по политически причини.

Разграничението между трите звена има и методологична функция. Структурната експозиция и стратегическата интерпретация на риска трябва да бъдат установени независимо от институционалната мярка, чието възникване теорията се стреми да обясни. В противен случай би възникнало кръгово доказване: наличието на защитна мярка би служило едновременно като доказателство за съществуването на стратегическа заплаха и като доказателство, че същата заплаха е причинила институционалната промяна.

Самото управление на уязвимостта не е достатъчно, за да се говори за стратегизация, ако институционалната оценка не отчита кой конкретен участник може да използва тази уязвимост, по какъв начин и с какви последици.

IV. Теоретична рамка: от понятието към институционалната форма

Стратегизацията насочва анализа на икономическата сигурност към конкретните отношения на зависимост между участниците и към възможността тези отношения да бъдат използвани за стратегическо въздействие. Поради това националната икономика, разглеждана само като агрегирано

състояние, вече не е достатъчна единица на анализ. Необходимо е да се проследи конкретната връзка между защитаваната национална способност, икономическата зависимост, външния участник и институционалния механизъм за защита. Необходимо е да бъде проследено конкретното отношение между защитавана национална способност, икономическа зависимост, външен участник и институционален механизъм на защита. Една и съща степен на икономическа зависимост може да има различно значение за сигурността в зависимост от това кой контролира съответните ресурс или инфраструктура, какви способности притежава и какви възможности има защитаващият се участник за заместване, адаптация или ответно действие.

Стратегизацията поражда втори институционален проблем: Кой извършва стратегическата преценка? Стратегическата преценка обаче може да изисква оценка на бъдещо поведение, класифицирана или непълна информация и избор при висока несигурност. Затова въпросът е не само дали компетентността се делегира, а на кое равнище, на кой орган и при какъв баланс между експертна оценка и политическа отговорност. Зародиш на този проблем присъства в Станев (Stanev 2015, pp. 139-140), където са разграничени защитата на критичния финансов обект и установяването кой, как и кога може да създаде заплаха.

Този проблем е особено отчетлив при малките държави, включени в по-големи интеграционни системи. Колективното равнище може да им предостави пазарен мащаб, регулаторен капацитет, информационни ресурси и способност за ответно действие, които те трудно могат да произведат самостоятелно. Колективизирането на защитните способности обаче поставя отделен въпрос: Доколко и на кое равнище се споделя преценката кога определена икономическа експозиция преминава прага на стратегическа заплаха? Следователно дилемата не се свежда до „повече“ или „по-малко“ интеграция. Тя засяга разпределението на стратегическата преценка между националното и колективното равнище.

Формата на институционалната адаптация зависи и от структурната позиция на защитаващия се участник. Юрисдикционният контрол върху централен мрежов възел разширява набора от достъпни стратегически действия, като предоставя възможности за наблюдение и ограничаване на достъпа, които участниците без подобен контрол не притежават (Farrell, Newman 2019). Мащабът на интегрирания пазар и регулаторният контрол могат да бъдат преобразувани във външно влияние (Damro 2012). Обратно, държавите с по-ограничен собствен контрол върху ключови инфраструк-

тури разполагат с по-тесен набор от защитни възможности и в по-голяма степен разчитат на диверсификация, резерви и колективни механизми. При риск от ограничаване или загуба на достъп до съществуваща инфраструктура се засилва стимулът за създаване на заместители и алтернативни технологични, финансови или логистични канали (Drezner, Farrell, Newman 2021; McDowell 2023).

Следвайки тази логика може да се твърди, че стратегизацията няма единна институционална форма. Структурната позиция определя различни пространства на възможното действие, а разпределението на стратегическата преценка определя кой избира между наличните защитни стратегии. Оттук следва теоретичното очакване, че еднаква по характер външна заплаха може да произведе различни институционални реакции в зависимост от позицията на защитаващия се участник и от равнището, на което е разположена компетентността за стратегическа оценка и действие.

V. Емпирична илюстрация и граници на рамката

Европейският съюз представлява особено подходящ случай за проверка на този механизъм. Неговата икономическа архитектура е изградена върху единен пазар, трансгранична мобилност и общи правни режими, докато компетентностите, свързани със защитата на икономически интереси и националната сигурност, са разпределени между Съюза и държавите членки. Това превръща ЕС в система, в която икономическата способност в значителна степен се произвежда колективно, но стратегическата оценка на отделни рискове не е автоматично централизирана на същото равнище. Националната сигурност остава отговорност на държавите членки по чл. 4, пар. 2 от Договора за Европейския съюз.[1]

Европейската стратегия за икономическа сигурност от 20 юни 2023 г. е показателна илюстрация. Тя групира рисковете в четири категории: устойчивост на веригите за доставки; физическа и киберсигурност на критичната инфраструктура; технологична сигурност и изтичане на технологии; използване на икономически зависимости за въздействие или принуда. Важното е, че преоценката на риска не води до отказ от интеграция: подходът съчетава икономическа база и конкурентоспособност, защита срещу конкретни рискове и партньорства. В рамките на предложения модел това е селективна адаптация на отворения интеграционен ред.[2]

Регламент (ЕС) 2023/2675 дава по-ясна илюстрация. Икономическа принуда е налице не просто при неблагоприятен икономически ефект, а

когато мярка, засягаща търговията или инвестициите, се използва или заплашва да бъде използвана за повлияване на легитимен суверенен избор. Следователно оценката обхваща не само последствията, а и стратегическата функция на поведението. Комисията извършва проверката и събира информацията, а Съветът правно определя наличието на икономическа принуда по предложение на Комисията – пряка институционализация на стратегическата преценка (Регламент (ЕС) 2023/2675, чл. 2, 4–5).

Препоръка (ЕС) 2025/63 показва друго измерение. Тя не създава режим за контрол върху изходящите инвестиции, а обща рамка за преглед и оценка на риска при инвестиции в усъвършенствани полупроводници, изкуствен интелект и квантови технологии. Прегледът е формално неутрален спрямо държавата получател, но държавите членки могат да приоритизират дейностите си според рисковия профил и, когато е релевантно, предходното поведение на отделни държави. Така стратегическата диференциация възниква още на равнището на оценката, преди конкретен ограничителен инструмент.[3]

Тези примери не представляват самостоятелен емпиричен тест на предложения причинен механизъм, но показват неговата емпирична правдоподобност, доколкото основните му елементи намират наблюдаем институционален израз в практиката на Европейския съюз. Интегрирана система може да запази базовата си ориентация към икономическа отвореност и едновременно да институционализира процедури, при които оценката на определени икономически отношения зависи от характера на контрагента, неговите способности, предходното му поведение и предполагаемите последствия за защитаваните интереси.

Рамката на Baldwin (1997) позволява допълнително ограничаване на понятието. Референтни обекти са държавата и обществото, защитават се съществени икономически функции и способности, от които зависи свободата на действие, релевантни са заплахи, зависещи от стратегическия избор на участник в общи трансгранични структури. Средствата включват наблюдение, диференцирана оценка, намаляване на експозицията, възпиране и при необходимост ограничаване или ответно действие. Целта е достатъчна защита без непропорционално разрушаване на ползите от интеграцията, при отчитане на икономическата цена, политическата дискреция и разпределителните последствия.

VI. Заключение

Настоящият доклад изследва как се променя институционалната организация на икономическата сигурност, когато рискът започне да зависи

и от стратегическия избор на участник, включен в същите трансгранични структури, от които зависят защитаваните национални способности.

Предложеният модел локализира стратегизацията между икономическата зависимост и стратегическото взаимодействие. Самата структурна експозиция и общото възприятие за съперничество не са достатъчни. Решаващият момент настъпва, когато рискът се интерпретира като зависещ от избора и вероятната реакция на конкретен участник и тази преценка се институционализира в устойчиви критерии, компетентности и процедури. Именно институционализирането отличава стратегизацията от еднократната политическа реакция.

Дълбоката интеграция не изисква непременно прекъсване на взаимозависимостта. Пазарите, мрежите и институциите продължават да създават способности и ползи, а стратегическите механизми могат да бъдат добавяни чрез наслояване, преобразуване и селективна адаптация (Mahoney, Thelen 2010; Couvreur 2025). Получава се хибридна конфигурация: общите правила се запазват, но определени зависимости и потоци се подлагат на стратегически диференцирана оценка.

Вторият централен проблем е разпределението на стратегическата преценка: кой определя кога експозицията представлява стратегическа заплаха, на каква информация се основава оценката и кой избира ответната мярка. Тази функция може да бъде национална, споделена или делегирана на колективно равнище. По-голямото споделяне е по-вероятно при сходни оценки на заплахата и съвместими експозиции; при различаващи се рискове и разпределителни последствия преценката остава по-фрагментирана.

Трансформацията следователно не може да бъде описана достатъчно точно чрез оста „отвореност – затваряне“. По-точно е да се разглежда като селективно управление на взаимозависимостта – запазване на отношенията, които създават значими способности и институционално диференциране на зависимостите, оценени като стратегически релевантни. Икономическата отвореност и стратегизацията следователно представляват различни аналитични измерения: една икономическа система може да остане високо интегрирана и едновременно с това да прилага стратегически диференциран подход към определени зависимости.

Основната промяна е институционализирането на въпросите кой контролира конкретната зависимост, как може да я използва, как вероятно ще реагира на защитната мярка и кой има компетентността да извърши тази преценка. Когато тези въпроси се превърнат от извънредна политическа реакция в устойчиви критерии, компетентности и процедури вътре в

икономическите институции, е налице процесът, който настоящата статия определя като стратегизация на икономическата сигурност.

БЕЛЕЖКИ

1. Договор за Европейския съюз (консолидирана версия), 2016. *Официален вестник на Европейския съюз*, C 202, 7.6.2016, с. 13 – 45. CELEX: 12016M

2. Европейска комисия; Върховен представител на Съюза по въпросите на външните работи и политиката на сигурност, 2023. Съвместно съобщение до Европейския парламент, Европейския съвет и Съвета относно Европейска стратегия за икономическа сигурност. JOIN(2023) 20 final. Брюксел, 20.06.2023. CELEX: 52023JC0020

3. ЕВРОПЕЙСКА КОМИСИЯ, 2025. Препоръка (ЕС) 2025/63 на Комисията от 15 януари 2025 година за преглеждане на изходящите инвестиции в технологични области от възлово значение за икономическата сигурност на Съюза. *Официален вестник на Европейския съюз*, L 2025/63, 15.01.2025. CELEX: 32025H0063, съобр. 11 – 16 и т. 1

4. MAJONE, G., 2001. Two Logics of Delegation: Agency and Fiduciary Relations in EU Governance. *European Union Politics*, vol. 2, no 1, pp. 103-122. DOI: 10.1177/1465116501002001005

5. WOLFERS, A., 1952. “National Security” as an Ambiguous Symbol. *Political Science Quarterly*, vol. 67, no 4, pp. 481-502. DOI: 10.2307/2145138

ЛИТЕРАТУРА

ВЕЛКОВА, Л., 2022. Икономическата сигурност – фундамент на националната сигурност. *Сигурност и отбрана*, № 2, с. 7 – 19. DOI: 10.70265/SDLY7619.

ЙОЦОВ, И., 2025a. *Икономическа сигурност: Теоретични аспекти*. Варна: ВВМУ „Никола Й. Вапцаров“. 198 с. ISBN 978-619-7752-06-9 (печат); ISBN 978-619-7752-07-6 (електронно издание).

ЙОЦОВ, И., 2025b. *Икономическа сигурност: Приложни и хуманитарни аспекти*. Варна: ВВМУ „Никола Й. Вапцаров“. 138 с. ISBN 978-619-7752-10-6 (електронно издание).

КОДЖАХРИСТОВ, П., 2025. Теоретични основи на вътрешните заплахи в гражданската авиация. *Сигурност и отбрана*, № 1, с. 86 – 103. DOI: 10.70265/OMXR7058.

ЛУЛАНСКИ, В., 2024. Практически аспекти на икономическата сигурност. В: *Годишник на Висше училище по сигурност и икономика*, т. XXI, с. 104 – 120.

МАРИНОВ, А., 2014. Примерен модел на стратегия за икономическа сигурност на Република България. *Управление и устойчиво развитие*, № 1 (44), с. 91 – 96.

ПЕТЕВ, Б., 2021. Икономическата сигурност, фактор за национална сигурност. *Бизнес посоки*, № 1, с. 69 – 73.

СЛАТИНСКИ, Н., 2000. *Измерения на сигурността*. София: Парадигма. 367 с. ISBN 954-9536-30-0.

СТАНЕВ, С. С., 2015. *Механизъм за гарантиране на финансовата сигурност на Република България при валутен борд* [Дисертационен труд]. София: Университет по библиотекознание и информационни технологии, Институт за научни изследвания и обучение на докторанти.

BABIĆ, M., 2025. *Geoökonomie: Anatomie der neuen Weltordnung*. Berlin: Suhrkamp Verlag. 236 p. ISBN 978-3-518-12833-6.

BALDWIN, D.A., 1985. *Economic Statecraft*. Princeton, NJ: Princeton University Press.

BALDWIN, D.A., 1997. The Concept of Security. *Review of International Studies*, vol. 23, no 1, pp. 5-26. DOI: 10.1017/S0260210597000053.

BAUERLE DANZMAN, S.; MEUNIER, S., 2024. The EU's Geoeconomic Turn: From Policy Laggard to Institutional Innovator. *JCMS: Journal of Common Market Studies*, vol. 62, no 4, pp. 1097-1115. DOI: 10.1111/jcms.13599.

BUZAN, B.; WÆVER, O.; WILDE, J. de, 1998. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers.

COUVREUR, S., 2025. Inside the European Union's Trade Machinery: Institutional Changes in an Age of Geoeconomics. *JCMS: Journal of Common Market Studies*, vol. 63, no 1, pp. 284-301. DOI: 10.1111/jcms.13625.

DAMRO, C., 2012. Market Power Europe. *Journal of European Public Policy*, vol. 19, no 5, pp. 682-699. DOI: 10.1080/13501763.2011.646779.

DREZNER, D. W.; FARRELL, H.; NEWMAN, A.L. (eds.), 2021. *The Uses and Abuses of Weaponized Interdependence*. Washington, DC: Brookings Institution Press. 351 p. ISBN 978-0-8157-3837-4.

FARRELL, H.; NEWMAN, A.L., 2019. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, vol. 44, no 1, pp. 42-79. DOI: 10.1162/isec_a_00351.

FRIEDRICH, J.; OERS, L. van; MIORNER, J.; FUENFSCHILLING, L., 2026. The Geo-economization of Sustainability Transitions: Spatial Dynamics and Trade-offs between Sovereignty and Sustainability. *Environmental Innovation and Societal Transitions*, vol. 60, article 101118. DOI: 10.1016/j.eist.2026.101118.

HAROCHE, P., 2024. Geoeconomic Power Europe: When Global Power Competition Drives EU Integration. *JCMS: Journal of Common Market Studies*, vol. 62, no 4, pp. 938-954. DOI: 10.1111/jcms.13596.

HELDT, E. C.; MEUNIER, S., 2026. How EU Industrial Policy Got Its Groove Back: Securitisation and Governance Shifts in the Geoeconomic Era. *Journal of European Public Policy*. DOI: 10.1080/13501763.2026.2627350.

HERRANZ-SURRALLÉS, A.; DAMRO, C.; ECKERT, S., 2024. The Geoeconomic Turn of the Single European Market? Conceptual Challenges and Empirical Trends. *JCMS: Journal of Common Market Studies*, vol. 62, no 4, pp. 919-937. DOI: 10.1111/jcms.13591.

HIRSCHMAN, A. O., 1945. *National Power and the Structure of Foreign Trade*. Berkeley: University of California Press.

KEOHANE, R. O., 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton, NJ: Princeton University Press.

KEOHANE, R.O.; NYE, J.S., 1977. *Power and Interdependence: World Politics in Transition*. Boston: Little, Brown.

KIRSHNER, J., 1995. *Currency and Coercion: The Political Economy of International Monetary Power*. Princeton, NJ: Princeton University Press.

MAHONEY, J.; THELEN, K. (eds.), 2010. *Explaining Institutional Change: Ambiguity, Agency, and Power*. Cambridge: Cambridge University Press.

MCDOWELL, D., 2023. *Bucking the Buck: US Financial Sanctions and the International Backlash against the Dollar*. New York: Oxford University Press. DOI: 10.1093/oso/9780197679876.001.0001. ISBN 978-0-19-767987-6.

MEUNIER, S.; NICOLAÏDIS, K., 2019. The Geopoliticization of European Trade and Investment Policy. *JCMS: Journal of Common Market Studies*, vol. 57, no S1, pp. 103-113. DOI: 10.1111/jcms.12932.

RUGGIE, J.G., 1982. International Regimes, Transactions, and Change: Embedded Liberalism in the Postwar Economic Order. *International Organization*, vol. 36, no 2, pp. 379-415. DOI: 10.1017/S0020818300018993.

STRANGE, S., 1988. *States and Markets*. London: Pinter.

REFERENCES

BABIĆ, M., 2025. *Geoökonomie: Anatomie der neuen Weltordnung*. Berlin: Suhrkamp Verlag. ISBN 978-3-518-12833-6.

BALDWIN, D.A., 1985. *Economic Statecraft*. Princeton, NJ: Princeton University Press.

BALDWIN, D.A., 1997. The Concept of Security. *Review of International Studies*, vol. 23, no 1, pp. 5-26. DOI: 10.1017/S0260210597000053.

BAUERLE DANZMAN, S.; MEUNIER, S., 2024. The EU's Geoeconomic Turn: From Policy Laggard to Institutional Innovator. *JCMS: Journal of Common Market Studies*, vol. 62, no 4, pp. 1097-1115. DOI: 10.1111/jcms.13599.

BUZAN, B.; WÆVER, O.; WILDE, J. de, 1998. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers.

COUVREUR, S., 2025. Inside the European Union's Trade Machinery: Institutional Changes in an Age of Geoeconomics. *JCMS: Journal of Common Market Studies*, vol. 63, no 1, pp. 284-301. DOI: 10.1111/jcms.13625.

DAMRO, C., 2012. Market Power Europe. *Journal of European Public Policy*, vol. 19, no 5, pp. 682-699. DOI: 10.1080/13501763.2011.646779.

DREZNER, D.W.; FARRELL, H.; NEWMAN, A.L. (eds.), 2021. *The Uses and Abuses of Weaponized Interdependence*. Washington, DC: Brookings Institution Press. ISBN 978-0-8157-3837-4.

FARRELL, H.; NEWMAN, A.L., 2019. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, vol. 44, no 1, pp. 42-79. DOI: 10.1162/isec_a_00351.

FRIEDRICH, J.; OERS, L. van; MIORNER, J.; FUENFSCHILLING, L., 2026. The Geo-economization of Sustainability Transitions: Spatial Dynamics and Trade-offs between Sovereignty and Sustainability. *Environmental Innovation and Societal Transitions*, vol. 60, article 101118. DOI: 10.1016/j.eist.2026.101118.

HAROCHE, P., 2024. Geoeconomic Power Europe: When Global Power Competition Drives EU Integration. *JCMS: Journal of Common Market Studies*, vol. 62, no 4, pp. 938-954. DOI: 10.1111/jcms.13596.

HELDT, E. C.; MEUNIER, S., 2026. How EU Industrial Policy Got Its Groove Back: Securitisation and Governance Shifts in the Geoeconomic Era. *Journal of European Public Policy*. DOI: 10.1080/13501763.2026.2627350.

HERRANZ-SURRALLÉS, A.; DAMRO, C.; ECKERT, S., 2024. The Geoeconomic Turn of the Single European Market? Conceptual Challenges and Empirical Trends. *JCMS: Journal of Common Market Studies*, vol. 62, no 4, pp. 919-937. DOI: 10.1111/jcms.13591.

HIRSCHMAN, A.O., 1945. *National Power and the Structure of Foreign Trade*. Berkeley: University of California Press.

KEOHANE, R.O., 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton, NJ: Princeton University Press.

KEOHANE, R.O.; NYE, J.S., 1977. *Power and Interdependence: World Politics in Transition*. Boston: Little, Brown.

KIRSHNER, J., 1995. *Currency and Coercion: The Political Economy of International Monetary Power*. Princeton, NJ: Princeton University Press.

KODZHAHRISTOV, P., 2025. Teoritichni osnovi na vatreshnite zaplahi v grazhdanskata aviatsia. *Sigurnost i otbrana*, no 1, pp. 86 – 103. DOI: 10.70265/OMXR7058 [in Bulgarian].

LULANSKI, V., 2024. Prakticheski aspekti na ikonomicheskata sigurnost. In: *Godishnik na Visshe uchilishte po sigurnost i ikonomika*, vol. XXI, pp. 104 – 120 [in Bulgarian].

MAHONEY, J.; THELEN, K. (eds.), 2010. *Explaining Institutional Change: Ambiguity, Agency, and Power*. Cambridge: Cambridge University Press.

MARINOV, A., 2014. Primeren model na strategia za ikonomicheska sigurnost na Republika Bulgaria. *Upravlenie i ustoychivo razvitie*, no 1 (44), pp. 91 – 96 [in Bulgarian].

MCDOWELL, D., 2023. *Bucking the Buck: US Financial Sanctions and the International Backlash against the Dollar*. New York: Oxford University Press. DOI: 10.1093/oso/9780197679876.001.0001. ISBN 978-0-19-767987-6.

MEUNIER, S.; NICOLAÏDIS, K., 2019. The Geopoliticization of European Trade and Investment Policy. *JCMS: Journal of Common Market Studies*, vol. 57, no S1, pp. 103-113. DOI: 10.1111/jcms.12932.

PETEV, B., 2021. Ikonomicheskata sigurnost, faktor za natsionalna sigurnost. *Biznes posoki*, no 1, pp. 69 – 73 [in Bulgarian].

RUGGIE, J. G., 1982. International Regimes, Transactions, and Change: Embedded Liberalism in the Postwar Economic Order. *International Organization*, vol. 36, no 2, pp. 379-415. DOI: 10.1017/S0020818300018993.

SLATINSKI, N., 2000. *Izmerenia na sigurnostta*. Sofia: Paradigma. ISBN 954-9536-30-0 [in Bulgarian].

STANEV, S.S., 2015. *Mehanizam za garantirane na finansovata sigurnost na Republika Bulgaria pri valuten bord* [Disertatsionen trud]. Sofia: Universitet po

bibliotekoznanie i informatsionni tehnologii, Institut za nauchni izsledvania i obuchenie na doktoranti [in Bulgarian].

STRANGE, S., 1988. *States and Markets*. London: Pinter.

VELKOVA, L., 2022. Ikonomicheskata sigurnost – fundament na natsionalnata sigurnost. *Sigurnost i otbrana,* no 2, pp. 7 – 19. DOI: 10.70265/SDLY7619 [in Bulgarian].

YOTSOV, I., 2025a. *Ikonomicheska sigurnost: Teoretichni aspekti*. Varna: VVMU „Nikola Y. Vaptsarov“. ISBN 978-619-7752-06-9 (pechat); ISBN 978-619-7752-07-6 (elektronno izdanie) [in Bulgarian].

YOTSOV, I., 2025b. *Ikonomicheska sigurnost: Prilozhni i humanitarni aspekti*. Varna: VVMU „Nikola Y. Vaptsarov“. ISBN 978-619-7752-10-6 (elektronno izdanie) [in Bulgarian].

FROM STATE TO RELATION: THE STRATEGIZATION OF ECONOMIC SECURITY UNDER STRATEGIC INTERDEPENDENCE

Abstract. The literature on international interdependence and geoeconomic power shows that economic ties can simultaneously generate efficiency and mutual gains, asymmetric power, coercion and strategic vulnerability. Less theorized is how the shift from impersonal systemic risk to risk contingent on the choices and behaviour of specific external actors changes the logic of institutional protection. This conference paper uses the concept of “strategization of economic security” to describe a process in which institutions organized primarily around general rules begin systematically differentiating decisions according to the identity, capabilities and expected behaviour of specific external actors. It develops a theoretical model distinguishing strategization from securitization, geopoliticization and economic statecraft and explains three connected outcomes: the emergence of strategic threats, institutional adaptation within continuing interdependence, and the distribution of strategic judgement across institutional levels.

Keywords: economic security; European Union; institutional adaptation; interdependence; relational security; strategization

Dr. Stanimir Stanev
Konstantin Preslavsky University of Shumen
Shumen, Bulgaria
E-mail: stanimirststanev@abv.bg

https://doi.org/10. 66334/annu26_liderorgapod

ЛИДЕРСТВО И ОРГАНИЗАЦИОННИ ПОДХОДИ В УПРАВЛЕНИЕТО НА ОБРАЗОВАТЕЛНИЯ ПРОЦЕС В ЕРАТА НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ

полковник Стоян Червеняков
Военна академия „Георги Стойков Раковски

Абстракт. Съвременните образователни продукти и особено този на военнообразователната система са генерирани в сложна международна среда и на фона на сериозна геополитическа тектоника, характеризираща се с голяма динамика на процесите. На този фон се налагат нови подходи, свързани с необходимостта от развиване у обучаемите от всички категории на компетентности, осигуряващи възможности за образование през целия живот (*Lifelong learning)* и способности за създаване на съдържание. Изкуственият интелект е мощен инструмент за покриване на тези необходимости, но той съдържа определени слаби страни и рискове, не е универсално решение и не може да замени ролята на преподавателя, лидера и командира.

Ключови думи: вземане на решения; военно образование; изкуствен интелект; лидерство; обработка на информация; управление на образованието

1. Увод

Съвременната среда за сигурност се характеризира с бързо навлизане на информационни технологии и неимоверно нарастване на обема, скоростта и разнообразието на информацията, което увеличава възможностите за събиране и обработка на данни, но едновременно с това създават риск от информационно претоварване и натрупване на големи масиви от недостоверна информация (Puyvelde, Tabárez Rienzi 2025). Технологиите не отменят необходимостта от лидерството, те само променят начина, по който лидерът формулира проблеми, организира експертната работа и използва информацията. Затова и в настоящото изследване ИИ се разглежда като инструмент за подпомагане на информационни и аналитични функции, а не като заместител на човешката преценка.

Предложен е двукомпонентен итеративен модел за управление на информацията и вземане на решения, приложим в различни организации, включително образователна среда и адаптируем към военното образование. Основната теза е, че ефективността на ИИ зависи не само от технологията, а от качеството на информационните източници, организацията на процеса, експертната оценка и най-важното – уменията на командирите, началниците и изобщо лидерите на различните нива в организациите да анализират факторите на средата и да вземат информирани и аргументирани решения. Този подход е базиран и съответства на човекоцентричните принципи за използване на генеративен ИИ в образованието (Miao, Holmes 2023). В тази връзка и в съответствие с актуални тенденции в развитието на информационните технологии са формулирани и обект, предмет, цел и изследователски въпрос на изследването, посочени конкретно в следващите точки:

2. Обект

Образователната среда и някои възможни организационни подходи в съвременните образователни институции.

3. Предмет

Лидерски стил, управленска стратегия и възможности за подобрен организационен подход и интегриране на изкуствения интелект в управлението на образователния процес.

4. Изследователски въпрос

Какви нови лидерски компетентности и организационни модели са необходими за ефективното управление на образователния процес в навлизащата ера на изкуствения интелект?

5. Теоретична основа

5.1. Образователният процес като организационна система

В рамките на изследването образователният процес се разглежда като организирана система за обмен, създаване, структуриране и прилагане на знания, която включва цели, съдържание, ресурси, участници и механизми за оценка на дадена дигитална среда. По този начин се променя ролята на обучаемия от реципиент към активен участник в създаването и трансформирането на съдържание, а това от своя страна води до увеличаване ефективността на процеса (Miao, Holmes 2023) и педагогическата валидация на информацията.

5.2. Информацията като ресурс за управление

Управленската дейност може да се разглежда в определен контекст и като последователност от идентифициране на предизвикателства, събиране и обработка на информация, анализ, избор, изпълнение и оценка. OSINT практиката показва, че големият обем публична информация не означава автоматично качествено знание и висока добавена стойност – за да е изпълнено това очакване, необходими са селективност, проверки и експертен анализ (Puyvelde, Tabárez Rienzi 2025). При цифрови открити източници са важни идентифицирането, събирането, съхраняването, анализът и представянето на информацията[1], като следва да се има предвид постоянно нарастващата сложност.

5.3. Еволюция на средствата за обработка на информация

За целите на модела е представена авторска работна периодизация: предмикропроцесорен период, период на предписмени и писмени източници, микропроцесорен период, съвременен период на цифрови мрежи и специализирани бази данни, развиващ се период на интеграция между ИИ, сензорни системи и интернет на нещата, период, където се очаква основно комуникация между „машини“, разгледано в най-общ план. Периодизацията тук няма претенция за всеобхватност и универсалност, а има по-скоро методологична функция. В този порядък е предложена и следната класификация в табличен вид (таблица 1).

Таблица 1. Класификация на методите и средствата в исторически, функционален и ресурсен план

Категория/ Времеви периоди	***ФУНКЦИОНАЛНА***	***РЕСУРСНА***
Периоди преди възникване на микропроцесорната техника	Исторически методи	– От източници, създадени с използване на хора (исторически анализи на HUMINT); – Писмени източници от различни епохи, създадени на различни носители (пергаметно писмо, скални надписи и др.)
Период на възникване и развитие на микропроцесорната техника (от средата на 50-те години на XX век до днес)	Съвременни методи и средства;	– От специализирани издания; – От справочни издания; – От официални издания; – От научни публикации; – От карти, планове и сателитни (GPS) снимки; – От интернет.
Бъдещи периоди от време	Методи, средства и инструменти, които ще възникнат в бъдещето	Вероятни решения, базирани на изкуствен интелект, интернет на нещата и др.

* Забележка: Таблица 1 е отразява авторско концепция и предложение за нова контекстуално свързана класификация от гледна точка на времевите исторически периоди на възникването и развитието на някои методи и средства за обработка на информация. Въпреки че е разработена на основата на други източници и подходи, цитирани в литературата на настоящата разработка, възможни са определени терминологични различия с вече съществуващи такива, като това е част от замисъла за принос в тази посока.

6. Методология на изследването и разработване на модела

Изследването е концептуално-приложно, тъй като дадено управленско решение се разглежда като процес, а не като еднократен акт, поради

което моделът е изграден като итеративен цикъл, или по-скоро може да се итерира, в зависимост от входните данни на казуса и получените резултати. Информационната му основа включва организационно управление, анализ на цифрови и отворени източници, експертна оценка и елементи от ИИ, който може да подпомага търсенето и класифицирането на информация, обобщаването, откриването на взаимовръзки, сравнението на варианти и подготовката на таблици и визуализации. Той не е самостоятелен етап или субект на управленското решение, а елемент от цялостна система. Човешкият контрол е структурен принцип: машинно генерираният резултат се проверява, контекстуализира и оценява от компетентен човек. Това е особено важно и понякога критично при решения със значими организационни или военни последици (Bode, Chandler 2026).

Моделът има два компонента: I. организационно-информационен – етапи 1 – 3; II. организационно-административен/команден – етапи 4 – 10. Приложимостта му зависи от времето, персонала, ресурсите, достъпа до информация и характера на задачата. В контекста на променящата се среда, научните новости и необходимостта от допълване на вече съществуващи подобни цикли, настоящият модел е насочен към обединяването на човешкия ресурс и изчислителната мощ на съвременните компютри за едно по-пълно и рационално взаимодействие на ангажираните елементи. Част от съществуващите организационни модели не непременно включват подходи за интелектуално предизвикателство и стимули за генериране на нови идеи, какъвто е „Брейнсторминг“, а също така и обикновено липсва елемент или звено за *прогностична* дейност. Отделните му фази, осигурени с възможностите на ИИ и потенциала за многобройни итеративни цикли до получаване на работещ резултат, разгръщат нов оперативен хоризонт и размах пред лидерите от различните нива на управление.

7. Двукомпонентен итеративен модел за управление и вземане на решения

Моделът е представен на фигура 1, където първият компонент обхваща иницииране и дефиниране на случая, планиране и търсене/обработка на информация. Вторият включва експертна работа, решение, изпълнение, анализ, извличане на поуки и актуализиране на стандартната оперативна процедура. Отделните действия в него в следващата фигура са наречени за удобство „стъпки“, като могат да се или да не се препокриват с определени

етапи в обработката на информация в зависимост от казуса и характера на информацията, която бива обработвана.



Фигура 1. Двукомпонентен итеративен модел за управление и вземане на решения в условията на изкуствения интелект

Стъпка 1. Иницииране и дефиниране на случая. Ръководителят определя проблема и информационната среда, включително наличието на непълна, противоречива или манипулирана информация.

Стъпка 2. Планиране. Определят се екипът, задачите, сроковете, ресурсите и контролът.

Стъпка 3. Търсене и подготовка. Използват се специализирани търсачки, бази данни и ИИ за търсене, класификация и предварително структуриране на информацията.

Стъпка 4. Експертна работа. Информацията се анализира от експерти; при недостиг на време и персонал работата се концентрира около ръководителя и непосредствените му заместници.

Стъпка 5. Решение. Компетентният ръководител избира вариант след оценка на алтернативите.

Стъпка 6. Изпълнение и контрол.

Стъпка 7. Анализ на резултатите.

Стъпка 8. Извличане на поуки.

Стъпка 9. Корекция на процедурите.

Стъпка 10. Актуализирана стандартна оперативна процедура, съхранена в организационната информационна среда.

Последните стъпки/етапи превръщат опита в организационно знание и осигуряват обратна връзка към следващ цикъл.

Забележка: Предложеният модел е логическа рамка с директни възможности за прилагане в широк спектър от организационни необходимости. Важно е да се има предвид, че в практиката резултатите от някои стъпки, като „Прилагане на решението“ и „Анализ на резултатите“, биха могли да имат различна продължителност във времето в зависимост от конкретиката на средата и характера на проблема/казуса.

8. Възможности за практическо приложение на модела

Като илюстративен казус моделът може да се използва при актуализиране на учебен модул за обработка на информация и ИИ във военнообразователна среда. Казусът не представлява емпирична проверка, като ръководителят дефинира необходимостта, планира екипа и ресурсите, а ИИ подпомага предварителното структуриране на научни, нормативни и методически източници. Експертната група (в състава на която могат да влязат различни специалисти с необходимата експертиза, от организацията или привлечени външни такива) оценява резултатите, формулира варианти и

предлага актуализация, а след внедряването се анализират резултатите, извличат се поуки и се актуализира учебната процедура.

Таблица 2. Етапи, роля на ИИ и човешки контрол

Етап	*Основна дейност*	*Роля на ИИ*	*Човешки контрол*
1 – 2	Дефиниране и планиране	подпомагане	определяне на целите
3	Търсене и обработка	търсене, класификация, обобщаване	проверка
4 – 5	Експертна работа и решение	сравнение на варианти	експертна оценка и избор
6 – 8	Изпълнение, анализ, поуки	мониторинг и анализ	интерпретация
9 – 10	Корекция и SOP	структуриране	валидиране и одобрение

9. Резултати и обсъждане

Основният резултат е структуриране на информационния и управленския процес в единен итеративен цикъл. Моделът не доказва статистически по-висока ефективност спрямо всички алтернативи, а предлага проверима организационна рамка. Разширеният информационен поток е възможно да бъде представен по различни начини. Основно той проследява движението от източниците през предварителното търсене и структуриране, инструментите и ИИ, експертната работа и управленското решение до изпълнението и обратната връзка.

Очакваните ефекти са намаляване на времето за рутинно търсене и структуриране, по-добра проследимост на информационния поток, повторно използване на организационно знание, по-структурирана експертна работа и по-бърза актуализация на процедурите. Те следва да бъдат емпирично проверени, като ИИ не гарантира автоматично по-добро решение. Резултатът ще зависи от качеството на данните, формулирането на задачата, използвания инструмент и коригиращата намеса на човека във всеки конкретен случай. Рисковете могат да включват неточни резултати, пристрастия, проблеми с поверителността и прекомерна зависимост от машинно генерирана информация (Miao, Holmes 2023).

При използване на локални или автономни средства може да се намали експозицията към определени мрежово базирани киберрискове, но офлайн режимът не е абсолютна защита.

Моделът е приложим и към сложни системи с отношение към националната сигурност. Стратегическите обекти и дейности в България са определени с Постановление № 181 на Министерския съвет от 20.07.2009 г. с последващите изменения и допълнения.[63] Тази нормативна рамка е релевантна към по-широкия контекст на управлението на информационни и технологични ресурси в националната сигурност (Tabakov 2025), а емпирична проверка може да използва показатели като време за обработка, брой и качество на източниците, открити грешки, време до решение и качество на последващия анализ.

10. Имплементация на модела

Практическата стойност на подобни модели се определя не само от техните характеристики, но и от условията на средата и обстановката, при които те могат да бъдат внедрени в конкретната действаща организация. В настоящата разработка са разгледани възможностите на двукомпонентния модел, неговите качествени и експлоатационни предимства, потенциалното му значение за системата за национална сигурност, в частност във военнообразователната система, както и работното определение за информация, върху което е изградена архитектурата на модела. Той може да бъде внедряван и като допълнение към специфично контекстуални други аналитични, планиращи и прогностични инструменти, използвани в дадена структура или институция, като очакваното бъдещо развитие на изкуствения интелект само би разширил неговите възможности и потенциални ползи.

11. Лидерство и военно образование в условията на изкуствения интелект

Военното лидерство се формира чрез продължаващо учене, професионален опит и различни форми на образование (Díez, Martínez-Morán and Aurrekoetxea-Casaus 2023). Изследванията върху начинаещи военни лидери също подчертават значението на практиката и лидерското учене (Siew, Koh 2023), а професионалното военно образование трябва да развива не само знания, но и способност за мислене, вземане на решения, планиране и лидерство (Czarnecki 2018). Военният преподавател не е само източник на информация, а организатор на процеса на учене, модел за професионално поведение, валидатор на информацията и подобно на командирите и началниците от всички степени и човек облечен в отговорности, поради което и

академичната подготовка в професионалното военно образование трябва да се разглежда и в контекста на променящите се професионални изисквания (Powell, Townley 2025).

Интуитивното решение не следва да се противопоставя механично на рационалния анализ, като то може и трябва да бъде свързано с професионален опит и разпознаване на ситуации при непълна информация. В това отношение моделът не дава предимство нито на интуицията, нито на алгоритмичния анализ. Те трябва и се очаква да са се развивали в дългата житейска и професионална практика на ръководителите и лидерите на високи позиции в организациите. ИИ може да подпомага симулации, сценарии, казуси и ролеви рефлексии, като най-съвременни изследвания върху *Human–AI collaboration* в *Professional Military Education* разглеждат организацията на взаимодействието между човека и ИИ при подготовката на бъдещи лидери (Combes 2025). Технологичната компетентност следва да се развива заедно с професионалната преценка и човешката отговорност.

12. Педагогически и лидерски аспекти

Дейността и професионалната рефлексия на лидерите и ръководителите в общ план, а в частност в сферата на образованието и още по-конкретно във военно-образователната система могат и трябва да се развиват в следните основни насоки:

– **Лидерство** – задаване на ясна посока за развитие и внедряване на високи стандарти. Личен пример и визионерство, които да приобщават личния състав към мисията, функциите и задачите;

– **Организационна дейност** – планиране, провеждане, контрол и анализ на всички процеси, свързани с вътрешната динамика и междуорганизационното взаимодействие с други структури на организацията/институцията;

– **Методическа и обучителна дейност** – познаване на теоретичните основи в науката, прилагане на утвърдени методики и внедряване на нови подходи;

– **Личностна харизма, интуитивни и иновативни подходи** – не съществуват конкретни формули за тези области на професионалната същност на лидерите; въпреки това, дали тези неща могат да бъдат „тренирани“ и в някаква степен упражнявани, е истински важен въпрос, който се нуждае от по-подробно разглеждане в други, по-обемни и фокусирани изследвания;

– Консултиране и подкрепа на подчинените – проява на емпатия, продължителна грижа и подпомагане усилията за справяне, личностно развитие и лично и организационно благополучие.

13. Критерии за надеждност, сигурност и допустимо използване на ИИ при чувствителна информация

Използването на ИИ трябва да се осъществява в пълно съответствие с всички национални и вътрешноинституционални нормативни документи и добри практики, при спазване на закритостта, нобходимостта да се знае и реда за работа с информация. По-конкретно, моделът не изисква споделяне и „качване“ на вътрешноведомствена информация в публичното пространство. Той по-скоро е пасивен реципиент на вече налична такава в интернет и публично достъпни източници. За максимална сигурност подходите в модела предвиждат и работа в напълно автономен, *„offline* режим, при съответни оперативни условия на средата. Важно е да се отбележи, че той не е прилаган досега в реална обстановка на войсковата динамика, но при спазване на обикновената предпазливост и процедури, характерни за всяка друга рутинна войскова динамика, **не се очакват** проблеми със сигурността в различните ѝ измерения.

14. Заключение

Предложеният двукомпонентен итеративен модел свързва информационното търсене, експертния анализ, управленското решение, изпълнението и организационното учене в единен цикъл, като ИИ е позициониран като подпомагащ инструмент, а не като източник на знание/информация. Основният принос е възможността натрупаният опит да се превръща в мултиплициран ефект върху едно желано и очаквано структурирано организационно знание чрез поуки и актуализирани процедури. Моделът е адаптируем към образователни, военни и граждански организационни системи, но изисква емпирична проверка при конкретни условия, като не е завършен и краен продукт, а следва да бъде допълнително развиван и допълван във времето. В ерата на ИИ лидерството не се свежда до технологично използване. То включва определяне на цели, оценка на контекста, контрол върху информацията и поемане на отговорност за решенията, а ефективното взаимодействие между човешката същност и технологичната обработка на информация е основно организационен въпрос, който заслужава по-сериозно внимание в бъдеще.

БЕЛЕЖКИ

1. United Nations Office of the High Commissioner for Human Rights; University of California, Berkeley, 2022. *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law*. New York; Geneva: United Nations.

2. Министерски съвет на Република България, 2009. *Постановление № 181 от 20.07.2009 г. за определяне на стратегическите обекти и дейности, които са от значение за националната сигурност на Република България, с последващите изменения и допълнения*.

3. Периодизацията на средствата за обработка на информация е авторска работна класификация и има методологична, а не строго историографска функция.

4. Представеният практически казус е илюстративен и не представлява емпирично доказателство за ефективността на модела.

5. Терминът „изкуствен интелект“ включва алгоритмични и генеративни системи, използвани за подпомагане на търсене, класификация, обобщаване, анализ, прогнозиране и представяне на информация.

ЛИТЕРАТУРА

ТАБАКОВ, Илия, 2025. *Изкуственият интелект в националната сигурност: Новите технологии в системата за управление на кризи*. Плевен: Нима. – 261 с. ISBN 978-619-280-019-2.

BODE, I.; CHANDLER, K., 2026. Re-thinking human–machine interaction and the governance of AI in the military domain. *Nature Machine Intelligence*, vol. 8, pp. 663-669. DOI: 10.1038/s42256-026-01231-x.

COMBES, W., 2025. Educating Tomorrow's Leaders: Human-AI Collaboration Patterns for Professional Military Education. *Journal on Baltic Security*, vol. 11, no 2, pp. 172-218. DOI: 10.57767/jobs_2025_012.

CZARNECKI, J.E., 2018. What our professional military leaders need to know: Enhancing the professional military educational structure. *Journal of Military Learning*.

DÍEZ, F; MARTÍNEZ-MORÁN, P.C.; AURREKOETXEA-CASAUS, M., 2023. The learning process to become a military leader: born, background and lifelong learning. *Frontiers in Education*, vol. 8. DOI: 10.3389/feduc.2023.1140905.

MIAO, F.; HOLMES, W., 2023. *Guidance for Generative AI in Education and Research*. Paris: UNESCO. ISBN 978-92-3-100612-8.

POWELL, M.; TOWNLEY, D., 2025. The challenges and opportunities for academics in professional military education. *Defence Studies,* pp. 644-661. DOI: 10.1080/14702436.2025.2467746.

PUYVELDE, D.; TABÁREZ RIENZI, F., 2025. The rise of open-source intelligence. *European Journal of International Security,* vol. 10, no 4, pp. 530-544. DOI: 10.1017/eis.2024.61.

SIEW, D.H.K.; KOH, J.H.L., 2023. Being and becoming beginning military leaders: Implications for leadership learning. *Military Psychology*, vol. 35, no 2, pp. 142-156. DOI: 10.1080/08995605.2022.2088986.

REFERENCES

BODE, I.; CHANDLER, K., 2026. Re-thinking human–machine interaction and the governance of AI in the military domain. *Nature Machine Intelligence*, vol. 8, pp. 663-669. DOI: 10.1038/s42256-026-01231-x.

COMBES, W., 2025. Educating Tomorrow's Leaders: Human-AI Collaboration Patterns for Professional Military Education. *Journal on Baltic Security*, vol. 11, no 2, pp. 172-218. DOI: 10.57767/jobs_2025_012.

CZARNECKI, J.E., 2018. What our professional military leaders need to know: Enhancing the professional military educational structure. *Journal of Military Learning.*

DÍEZ, F; MARTÍNEZ-MORÁN, P.C.; AURREKOETXEA-CASAUS, M., 2023. The learning process to become a military leader: born, background and lifelong learning. *Frontiers in Education*, vol. 8. DOI: 10.3389/feduc.2023.1140905.

MIAO, F.; HOLMES, W., 2023. *Guidance for Generative AI in Education and Research*. Paris: UNESCO. ISBN 978-92-3-100612-8.

POWELL, M.; TOWNLEY, D., 2025. The challenges and opportunities for academics in professional military education. *Defence Studies,* pp. 644-661. DOI: 10.1080/14702436.2025.2467746.

PUYVELDE, D.; TABÁREZ RIENZI, F., 2025. The rise of open-source intelligence. *European Journal of International Security,* vol. 10, no 4, pp. 530-544. DOI: 10.1017/eis.2024.61.

SIEW, D.H.K.; KOH, J.H.L., 2023. Being and becoming beginning military leaders: Implications for leadership learning. *Military Psychology*, vol. 35, no 2, pp. 142-156. DOI: 10.1080/08995605.2022.2088986.

TABAKOV, I., 2025. *Izkustveniyat intelekt v natsionalnata sigurnost: Novite tehnologii v sistemata za upravlenie na krizi*. Pleven: Nima. ISBN 978-619-280-019-2 [in Bulgarian].

LEADERSHIP AND ORGANIZATIONAL APPROACHES TO THE MANAGEMENT OF THE EDUCATIONAL PROCESS IN THE ERA OF ARTIFICIAL INTELLIGENCE

Abstract. Modern educational products, and particularly those of the military educational system, are generated in a complex international environment against the backdrop of serious geopolitical tectonics characterized by high process dynamics. Against this background, new approaches are required, driven by the need to develop competencies in learners of all categories that enable lifelong learning opportunities and content creation capabilities. Artificial intelligence is a powerful tool for addressing these needs, but it contains certain weaknesses and risks, is not a universal solution, and cannot replace the role of the educator, leader, and commander!

Keywords: artificial intelligence; decision-making; educational management; information processing; leadership; military education

Colonel Stoyan Chervenyakov
ORCID iD: 0009-0002-0703-3246
Logistic Department
Rakovski National Defense College
82, Evlogi I Hristo Georgievi Boulevard
Sofia, Bulgaria
E-mail: s.chervenyakov@rndc.bg

https://doi.org/10. 66334/annu26_rasrazinfo

РАЗСЕКРЕТЯВАНЕ НА РАЗУЗНАВАТЕЛНА ИНФОРМАЦИЯ КАТО ИНСТРУМЕНТ НА СТРАТЕГИЧЕСКИТЕ КОМУНИКАЦИИ

Теменуга Хасекиева
Военна академия „Георги Стойков Раковски“

Абстракт. Разсекретяването на разузнавателна информация може да се превърне в инструмент на стратегическите комуникации, чрез който висшето държавно ръководство предупреждава, възпира, противодейства на дезинформацията и координира публичните си послания със съюзниците. Изследването разглежда разсекретяването като управляем процес на трансформирането на част от защитената информация в публично доказателство, без да се компрометират източници, методи и текущи оперативни способности. Анализирани са националната правна рамка и европейските изисквания, както и публични случаи от практиката на САЩ и Великобритания през 2022 г. На тази основа е предложен аналитичен модел за вземане на решение, включващ стратегическа цел, минимално необходим обем информация, оценка на риска, проверка, избор на времева рамка и комуникационен способ и последваща оценка на ефекта. Изводът е, че ефективността зависи не от максималното количество разсекретена информация, а от съотношението между доказателствена стойност, времеви ефект и защита на чувствителните елементи.

Ключови думи: разузнавателна информация; разсекретяване; стратегически комуникации; информационно противоборство; стратегическо предупреждение; национална сигурност

I. Увод

Съвременният въоръжен конфликт се развива едновременно във физическото, информационното и цифровото пространство. В тази среда разузнавателната информация има двойствено предназначение. От една страна, тя е защитен ресурс, необходим за вземане на решения и за осигуряване на оперативно предимство. От друга, част от нея може да придобие самостоятелна стратегическа стойност, когато бъде представена публично в подходящ момент. Така информацията престава да бъде единствено основа за национално управленско решение и се превръща в средство за въздействие върху поведението на съюзници, противници, международни организации и обществеността.[1,2]

Практиката преди и в началото на войната в Украйна през 2022 г. даде особено отчетливи примери за този подход. На 22 януари 2022 г. британското правителство публично заяви, че разполага с информация за руски план за установяване на проруски лидер в Киев. Три дни по-късно министър-председателят на Обединеното кралство посочи, че вече е била разсекретена разузнавателна информация относно намеренията на Руската федерация и че Лондон възнамерява да продължи с публичното оповестяване на информация за кибератаки, операции под чужд флаг и дезинформация.[3,4]

Тези действия поставят основния изследователски въпрос при какви условия публичното разкриване на разузнавателна информация повишава стратегическия ефект без да понижава разузнавателната стойност на източника или да дискредитира оперативните способи. Въпросът е едновременно правен, оперативен и стратегически. Той изисква разграничаване между информацията, която може да бъде публикувана, и информацията, която трябва да остане защитена, между легитимната стратегическа комуникация и политическото използване на разузнаването, както и между своевременността на публичното оповестяване и необходимостта от надеждна проверка.

Целта на настоящия доклад е да систематизира основните предпоставки за разсекретяване на разузнавателна информация във въоръжен конфликт и да предложи приложим аналитичен модел за контролирано вземане на решение. Изследването се основава на нормативен анализ, сравнителен анализ на публично документирани случаи и функционален анализ на връзката между разузнаването и стратегическите комуникации. Понятието „контролирано разсекретяване“ се из-

ползва като аналитично понятие в рамките на изследването, а не като самостоятелен термин.

II. Разузнавателната информация в стратегическите комуникации

2.1. *Разузнавателната информация като стратегически ресурс*

Класическата логика на разузнаването предполага ограничен достъп. Стойността на получената информация е свързана с това противникът да не знае какво е известно, как е получено и какви допълнителни способности стоят зад източника. Публичното разсекретяване променя тази логика. Част от информационната стойност се „жертва“ в полза на придобиването на способност за публично доказване, предупреждение или въздействие.[5] В рамката на НАТО стратегическите комуникации са свързани с координираното използване на комуникационни способности в подкрепа на политиките и операциите, като информацията и комуникацията се интегрират в процеса на планиране и изпълнение.[6]

Следователно решението за разсекретяване не трябва да се разглежда като противоположност на разузнавателната дейност. То е управленско решение относно жизнения цикъл на конкретна информация. Основният критерий е дали загубата на секретност е оправдана от стратегическия ефект. Този ефект може да бъде възпиращ, дипломатически, информационен, правоприлагащ или свързан с изграждането на съюзническо доверие.

2.2. *От секретност към контролирана публичност*

В условията на хибридна среда разузнавателната информация може да бъде използвана за предварително разобличаване на подготвяна дезинформация. В настоящото изследване този подход се означава като „превантивно разобличаване“ (pre-bunking). Той предполага публичното изнасяне на проверима част от информацията преди или в началото на очаквано информационно действие на противника, така че бъдещото му послание да бъде посрещнато с вече създадена рамка за оценка.[7] Европейската служба за външна дейност разглежда стратегическите комуникации и противодействието на FIMI като част от по-широкия инструментариум за устойчивост и реакция при хибридни заплахи.[8]

При този подход времето е съществен компонент. Информацията, публикувана твърде рано, може да загуби актуалност, а твърде късно – да не изпълни възпиращата или предупредителната си функция. Затова вре-

мевата стойност на разузнавателната информация следва да се разглежда заедно с надеждността, чувствителността и потенциалния ефект.[9,10]

III. Правна и институционална рамка

3.1. *Национална правна рамка*

В Република България изходната правна рамка се определя от Закона за защита на класифицираната информация (ЗЗКИ), който урежда основанията, нивата и сроковете за защита, както и периодичния преглед на необходимостта от запазване на класификацията. Особено значение за процеса имат правилата относно основанията за защита и прегледа на необходимостта от запазване на класификацията, както и периодичният преглед на основанията за защита, защото показва, че класификацията не следва да се възприема като неизменен статут на информацията.[11]

За разузнавателната сфера значение имат и Законът за военното разузнаване и Законът за Държавна агенция „Разузнаване“. Според разгледаната правна рамка стратегическото военно разузнаване включва добиване и анализ на стратегическа разузнавателна информация, информационно осигуряване на държавните институции и ранно откриване и предупреждение за рискове и заплахи.[12,13]

Тези функции са съществени за разглеждания проблем, защото показват, че разузнавателната информация има предназначение да подпомага държавното управление, но не определят сами по себе си кога и как тя може да бъде направена публична. Публичното оповестяване изисква отделна оценка на правните основания, класификационния статут, защитата на източниците и способите, както и на потенциалните последици за националната сигурност.[14]

3.2. Европейска рамка и защита на журналистическите източници

Европейската правна среда поставя допълнителни изисквания към баланса между сигурността и свободата на информацията. Регламент (ЕС) 2024/1083 относно общата рамка за медийните услуги установява защита на журналистическите източници и поверителните комуникации. Член 4 предвижда, че държавите членки трябва да гарантират ефективна защита, като ограниченията са допустими при определени условия, включително законово основание, преобладаващ обществен интерес, пропорционалност и предварително разрешение от съдебен или независим и безпристрастен орган в предвидените случаи.

За процеса на разсекретяване това има значение по две линии. Първо, публичното оповестяване не трябва да създава непряка възможност за идентифициране на защитени журналистически източници или поверителни комуникации. Второ, при работа с медиите трябва да се разграничават официално разсекретените данни от информация, която журналистът е получил по независим канал. Въвеждането на допълнителни гаранции за източниците увеличава изискването за прецизност при формулирането на публичното послание.[15]

3.3. *Международноправен и съдебен контекст*

Правото на достъп до информация и защитата на националната сигурност се намират в постоянно противоборство. За целите на доклада бяха анализирани решения на Конституционния съд и Европейския съд по правата на човека, както и тълкувателна практика на Висшия касационен съд и Висшия административен съд, които показват, че основен принцип е необходимостта ограниченията на публичността да бъдат обосновани и пропорционални. Тази линия на аргументация е особено важна при разузнавателна информация, защото самото позоваване на национална сигурност не освобождава държавата от необходимостта да обоснове конкретното ограничение.[16] В практиката на Европейския съд по правата на човека защитата на журналистическите материали и източници е свързана с гаранциите по член 10 от Конвенцията.[17]

В същото време въоръжените конфликти създават ситуации, при които своевременното публично оповестяване има значение за предотвратяване на заблуждение и за координация със съюзниците. Следователно правният анализ следва да се извършва едновременно с оценката на оперативния риск, а не след нейното приключване.[18,19]

IV. Емпиричен анализ на публичното разсекретяване

4.1. *Великобритания: предупреждение преди началото на войната*

Първият показателен случай е британското публично оповестяване от 22 януари 2022 г. на информация за предполагаем руски план за установяване на проруски лидер в Киев. В официалното съобщение на правителството на Обединеното кралство се посочват и връзки между руски разузнавателни служби и бивши украински политици. Съобщението не публикува разузнавателните способи или първичните източници, а представя аналитичната оценка и част от съдържанието, достатъчни за публичното предупреждение.[20]

На 25 януари министър-председател на Великобритания заявява пред парламента, че страната вече е разсекретила убедителна разузнавателна информация относно намерението за установяване на марионетен режим в Киев и ще продължи да оповестява информация за кибератаки, операции под чужд флаг и дезинформация. Така публичното разсекретяване е представено като част от възпираща стратегия, а не като еднократен комуникационен акт.[21]

4.2. *Публично посочване на киберактивност*

Втора група случаи е свързана с публичното посочване на отговорност за кибератаки. На 18 февруари 2022 г. британският National Cyber Security Centre публикува оценка за руско участие в кибератаки срещу украински банкови институции. Публичната оценка се основава на технически анализ и има различна функция от предупреждението за политически план – тя цели да установи публична позиция относно отговорността за конкретна кибердейност. В този тип случаи рискът се измества към доказателствената стойност и защитата на методите за техническо посочване на отговорността.

На 10 май 2022 г. правителството съобщава, че Великобритания, САЩ и съюзници са посочили като отговорна Руската федерация за кибератака срещу Viasat, започнала около час преди пълномащабното нахлуване на Русия в Украйна. Публичното съобщение представя оценката за отговорността, но не разкрива пълния разузнавателен набор, на който тя се основава. Това илюстрира принципа на минимално необходимо разкриване – публичният продукт трябва да е достатъчен за заявената цел, без да предава целия аналитичен и оперативен контекст.[22,23]

4.3. *САЩ и съюзниците: разузнавателно предупреждение и координация*

Публичните изявления на американски представители след началото на войната показват, че разузнавателните служби са използвали синтезирана и разсекретена информация за руските намерения, включително за концентрацията на войски и подготвяни операции под чужд флаг. В реч от 25 ноември 2024 г. директорът на националното разузнаване на САЩ Аврил Хейнс описва координацията със съюзниците от НАТО и публичното представяне на информацията като средство за усложняване на руските планове и за ограничаване на възможността отговорността за последващи действия да бъде прехвърлена.

Този случай показва, че разсекретяването може да има колективен характер. Информацията се превръща в основа за обща позиция на съюзници, а не само в инструмент на националната комуникация. Това обаче увеличава изискванията към съгласуването на оценките, времето на публикуване и формулировките.[24]

Таблица 1. Сравнителни характеристики на публично документирани случаи

Случай	*Тип информация*	*Публична цел*	*Защитен елемент*	*Основен риск*
22.01.2022, UK	Оценка за политически план	Предупреждение и възпиране	Източници и способи	Непълна доказуемост
18.02.2022, UK/NCSC	Техническа оценка	Публично приписване	Методи за атрибуция	Компрометиране на способности
10.05.2022, UK/съюзници	Оценка за кибератака	Международна атрибуция	Разузнавателен набор	Разкриване на аналитични възможности
Преди 24.02.2022, US/NATO	Синтезирана стратегическа оценка	Възпиране и съюзническа координация	Източници и методи	Политизиране на оценката

V. Модел за контролирано разсекретяване. Разсекретяването като инструмент на стратегическите комуникации

На основата на разгледаната нормативна и емпирична рамка може да бъде предложен модел за вземане на решение, който не заменя законовите процедури, а ги допълва с аналитични критерии. Моделът се състои от шест последователни етапа:

● Формулиране на стратегическата цел. Преди да се обсъжда какво да бъде публикувано, трябва да бъде формулирано какво трябва да бъде постигнато. Възможните цели включват предупреждение, възпиране, опровергаване на дезинформация, мобилизиране на съюзническа подкрепа или обосноваване на публична държавна позиция и др. Една и съща разузнавателна информация може да бъде подходяща за една цел и неподходяща за друга.

● Определяне на минимален информационен обем. Следва да се определи минималният информационен обем, който позволява целта да бъде постигната. Това предполага разделяне на информацията на елементи: факт или оценка; произход на информацията; време на получаване; способ на добиване; надеждност; допълнителни индикатори. Публичният продукт по правило не трябва да съдържа повече елементи, отколкото са необходими за доказване на тезата.

● Оценка на риска от компрометиране. Този етап е критичен. Необходимо е да се оцени дали комбинацията от публикувани детайли може да позволи на противника да идентифицира източник, способ, партньорски обмен или аналитичен процес и др. Рискът не се определя само от отделния факт. Съществен може да бъде и ефектът от съпоставянето му с вече публични данни.[25]

● Аналитична и правна проверка. Публичната оценка трябва да бъде проверена от аналитична и правна гледна точка. Проверява се надеждността, актуалността, възможността за независимо потвърждение, класификационният статут и съответствието с приложимите процедури. Когато публичното оповестяване засяга права или защитени категории информация, необходимостта от независим контрол се увеличава.[26,27]

● Избор на времеви момент и канал за комуникация. Времето на публикуване е част от съдържанието на стратегическото решение. Един и същ факт може да има различна стойност 24 часа преди, в началото или след дадено действие на противника. Каналът също има значение – официално изявление, технически анализ, парламентарна позиция или координирано съобщение със съюзници създават различни комуникационни ефекти.

● Последваща оценка на ефекта. Последният етап е оценката на резултата. Тя следва да отчете дали е постигната първоначалната цел, дали противникът е променил поведението или информационната си линия, дали са възникнали неочаквани последици и дали е настъпило компрометиране на разузнавателна способност. Натрупаният опит следва да се използва в следващите решения за публично оповестяване.

VI. Рискове и ограничения

Първият риск е политизирането на разузнавателната оценка. Когато разузнавателна информация се използва за подкрепа на предварително формирана политическа теза, се увеличава опасността от селективен под-

бор на факти. Разузнавателната оценка трябва да запази разграничението между факт, вероятностна оценка и политическо решение.[28]

Вторият риск е ерозията на доверието. Ако публично представена оценка се окаже неточна, прекалено категорична или неподкрепена от последващи факти, бъдещите предупреждения могат да бъдат приемани с по-голяма предпазливост. Поради това степента на увереност и естеството на доказателствата трябва да бъдат отразявани прецизно.[29,30]

Третият риск е компрометирането на източници и способи чрез комбиниране на малки детайли. В настоящата информационна среда публичното пространство позволява бързо съпоставяне на данни от различни държави, медии, социални мрежи и технически платформи. Следователно оценката на риска трябва да бъде кумулативна, а не да се ограничава до въпроса дали отделният факт сам по себе си е секретен.[31]

Четвъртият риск е свързан с отношенията с медиите. Разсекретяването може да подпомогне обществения контрол и информираността, но държавата не трябва да превръща медиите в инструмент за непряко разкриване на защитени източници. Новата европейска рамка за свободата на медиите засилва значението на тази граница.[32]

VII. Основни резултати

Анализът позволява да бъдат формулирани четири основни резултата:

– разсекретяването следва да се разглежда като самостоятелно стратегическо решение в жизнения цикъл на разузнавателната информация;

– публичната стойност на информацията зависи от нейното съдържание, времето и комуникационния контекст, а не от количеството разкрити данни;

– практиката от 2022 г. показва, че разузнавателните оценки могат да бъдат използвани предварително за предупреждение и възпиране, както и след извършване на действие за публично посочване на отговорност;

– правната и оперативната защита на източници и способи трябва да бъде включена в самия процес на подготовка на публичния продукт, а не да се разглежда като последваща проверка.

В този смисъл разсекретяването следва да се разбира не като комуникация сама по себе си, а като вход в стратегически комуникационен процес, в който съдържанието, моментът и координацията определят публичния ефект. Предложеният шестетапен модел дава възможност тези из-

исквания да бъдат превърнати в последователна процедура за анализ: цел – минимален обем – риск – проверка – времеви момент и комуникационен канал – оценка на ефекта. Неговото практическо предимство е, че разделя въпроса дали може информацията да бъде публикувана от въпроса каква част от нея е необходима за постигане на конкретната цел.

VIII. Заключение

Разсекретяването на разузнавателна информация във въоръжен конфликт и не само е сложен баланс между секретност и публичност. Неговата стратегическа стойност произтича от възможността защитена информация да бъде превърната в публично доказателство в момент, когато доказателството може да промени поведението на противника, да укрепи коалиционната позиция или да ограничи въздействието на дезинформацията. Публично документираните действия на Великобритания и САЩ през 2022 г. показват, че успешното разсекретяване не означава публикуване на целия разузнавателен продукт. По-скоро се публикува минималният достатъчен набор от проверима информация, който изпълнява конкретна стратегическа функция. Именно това позволява да се съчетаят комуникационният ефект и защитата на разузнавателните способности.

В български условия този подход следва да се реализира в рамките на Закона за защита на класифицираната информация и специалното законодателство за разузнавателната дейност, при съобразяване с принципите на пропорционалност, независим контрол и защита на основните права. Европейският акт за свободата на медиите допълнително подчертава необходимостта границата между публичната информация и защитените източници да бъде ясно очертана. В този смисъл контролираното разсекретяване не е отслабване на режима за защита, а управление на времевия момент, обема и формата на публичното оповестяване.

БЕЛЕЖКИ

1. UK GOVERNMENT, 2022a. *Kremlin plan to install pro-Russian leadership in Ukraine exposed*. 22 January 2022. [online] Available from: https://www.gov.uk/government/news/kremlin-plan-to-install-pro-russian-leadership-in-ukraine-exposed.

2. GCHQ, 2022. *Director GCHQ's speech on global security amid war in Ukraine*. 31 March 2022. Available from: https://www.gchq.gov.uk/speech/director-gchq-global-security-amid-russia-invasion-of-ukraine.

3. UK GOVERNMENT, 2022a…

4. UK GOVERNMENT, 2022b. *PM statement on Ukraine: 25 January 2022*. [online] Available from: https://www.gov.uk/government/speeches/pm-statement-on-ukraine-25-january-2022.

5. GCHQ, 2022...

6. NATO, 2015. *NATO Strategic Communications Policy*, pp. 20 –21.

7. COUNCIL OF THE EUROPEAN UNION, 2022. *Strengthened EU Code of Practice on Disinformation*. Available from: https://www.consilium.europa.eu/.

8. EUROPEAN EXTERNAL ACTION SERVICE, 2026. *Materials on strategic communication and FIMI.*

9. UK GOVERNMENT, 2022b…

10. GCHQ, 2022…

11. РЕПУБЛИКА БЪЛГАРИЯ, 2002. *Закон за защита на класифицираната информация*.

12. РЕПУБЛИКА БЪЛГАРИЯ, 2015a. *Закон за военното разузнаване.*

13. РЕПУБЛИКА БЪЛГАРИЯ, 2015b. *Закон за Държавна агенция „Разузнаване“*.

14. РЕПУБЛИКА БЪЛГАРИЯ, 2002. *Закон за защита на класифицираната информация*; РЕПУБЛИКА БЪЛГАРИЯ, 2015. *Закон за военното разузнаване*; РЕПУБЛИКА БЪЛГАРИЯ, 2015. *Закон за Държавна агенция „Разузнаване“*.

15. EUROPEAN PARLIAMENT AND COUNCIL, 2024. Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act). *Official Journal of the European Union*, L 2024/1083. [online] Available from: https://eur-lex.europa.eu/eli/reg/2024/1083/oj.

16. EUROPEAN COURT OF HUMAN RIGHTS, 2015. *Saure v. Germany, Application no. 8819/16*.

17. EUROPEAN COURT OF HUMAN RIGHTS, 2021. *Big Brother Watch and Others v. the United Kingdom, Applications nos. 58170/13, 62322/14 and 24960/15.*

18. GCHQ, 2022…

19. ODNI, 2024. *DNI Haines Receives NATO Award*. 25 November 2024. Office of the Director of National Intelligence. [online] Available from: https://www.dni.gov/index.php/newsroom/speeches-interviews/speeches-interviews-2024/4032-dni-haines-receives-nato-award-20241125.

20. UK GOVERNMENT, 2022a…

21. UK GOVERNMENT, 2022b…

22. UK GOVERNMENT, 2022c. *Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion*. 10 May 2022. Available from: https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion.

23. NCSC, 2022. *UK assesses Russian involvement in cyber attacks on Ukraine*. 18 February 2022. Available from: https://www.ncsc.gov.uk/news/russia-ddos-involvement-in-ukraine.

24. ODNI, 2024…

25. РЕПУБЛИКА БЪЛГАРИЯ, 2002. *Закон за защита на класифицираната информация*.

26. РЕПУБЛИКА БЪЛГАРИЯ, 2002. *Закон за защита на класифицираната информация*.

27. EUROPEAN PARLIAMENT AND COUNCIL, 2024. *Regulation (EU) 2024/1083*, Art. 4.

28. EUROPEAN COURT OF HUMAN RIGHTS, 2021. *Big Brother Watch...*

29. UK GOVERNMENT, 2022b. *PM statement on Ukraine*: 25 January 2022. 25 January 2022.;

30. ODNI, 2024. *DNI Haines Receives NATO Award*. 25 November 2024.

31. РЕПУБЛИКА БЪЛГАРИЯ, 2002. *Закон за защита на класифицираната информация*.

32. EUROPEAN PARLIAMENT AND COUNCIL, 2024. *Regulation (EU) 2024/1083, Art. 4*.

33. В текста „контролирано разсекретяване“ е използвано като аналитично понятие за процеса на подбор, правна проверка, оценка на риска и определяне на времевия момент и формата на публично оповестяване. То не се представя като самостоятелен законов термин.

34. Публичните случаи, разгледани в емпиричната част, са основани само на официално публикувани материали. В статията не се използва и не се възпроизвежда класифицирана информация.

3. Изследването разглежда само публично достъпни данни за действия на държавни институции през 2022 г.; не се прави оценка на непубличните разузнавателни процеси, стоящи зад публикуваните оценки.

DECLASSIFICATION OF INTELLIGENCE INFORMATION AS AN INSTRUMENT OF STRATEGIC COMMUNICATIONS

Abstract. The declassification of intelligence information can function as an instrument of strategic communications by enabling states to warn, deter, counter foreign information manipulation and interference, and coordinate public messages with allies. The study examines declassification as a managed process in which a limited part of intelligence is selected for public release while preserving the value of sources, methods and capabilities. It combines analysis of the Bulgarian legal framework with publicly documented cases from the United Kingdom and the United States related to the war in Ukraine. On this basis, a six-stage analytical model is proposed: defining the strategic objective; determining the minimum necessary disclosure; assessing risks to sources and

methods; legal and analytical review; selecting timing and channel; and evaluating effects.

Keywords: intelligence information; declassification; strategic communications; information confrontation; strategic warning; national security

Temenuga Hasekieva
Rakovski National Defence College
82, Evlogi i Hristo Georgievi Blvd.
Sofia, Bulgaria
E-mail: t.hasekieva@rndc.bg

https://doi.org/10. 66334/annu26_secpovclim

СИГУРНОСТ, БЕДНОСТ, КЛИМАТ: ЗАЩО ХОРАТА МИГРИРАТ

Христо Маруков

Абстракт. Миграцията е сложен процес, който се влияе от различни политически, икономически, социални и екологични фактори. Хората напускат родните си страни поради войни, преследване, нарушаване на човешките права, безработица, ниски доходи и неблагоприятни климатични условия. Същевременно възможностите за по-добър живот, образование и професионално развитие в други държави също насърчават преместването им.

Европейският съюз прилага различни мерки за управление на миграционните процеси. Сред тях са законните възможности за работа и пребиваване, предоставянето на международна закрила и сътрудничеството между държавите членки. Важна стъпка в тази посока е Новият пакт за миграцията и убежището, който цели да подобри общите процедури и да осигури по-справедливо разпределение на отговорностите между страните от ЕС.

Анализът показва, че миграцията не може да се обясни само с една причина, тъй като често няколко фактора действат едновременно. Въпреки че разглежданият текст предоставя полезна информация по темата, някои статистически данни и правни сведения се нуждаят от актуализация. Необходимо е също да се прави ясно разграничение между мигранти, търсещи убежище, и бежанци.

Миграцията е явление с важно обществено значение, което изисква балансиран подход. Ефективното ѝ управление

предполага защита на човешките права, създаване на законни възможности за миграция и координирани действия между европейските държави.

Ключови думи: миграция; Европейски съюз; международна закрила; миграционна политика; икономически и екологични фактори; човешки права

Увод

Миграцията е важен обществен процес, който оказва влияние върху развитието на държавите, икономиката и живота на хората. През последните години темата придобива все по-голямо значение за Европейския съюз поради различните причини, които принуждават или мотивират хората да напускат родните си страни. Сред тях са военните конфликти, политическата нестабилност, бедността, безработицата, нарушаването на човешките права и климатичните промени. Наред с тези обстоятелства, стремежът към по-добри условия на живот, образование и професионална реализация също играе съществена роля при вземането на решение за миграция (EP 2020).

Управлението на миграционните процеси представлява предизвикателство за Европейския съюз, тъй като изисква съчетаване на сигурността на външните граници със спазването на основните човешки права и предоставянето на международна закрила на нуждаещите се. В тази връзка европейските институции разработват общи правила и механизми, насочени към регулиране на миграцията, създаване на законни възможности за пребиваване и работа и укрепване на сътрудничеството между държавите членки (CEU 2024).

Целта на настоящата статия е да разгледа основните причини за миграцията към Европейския съюз, да представи възможностите за законна миграция и международна закрила и да анализира мерките, предприемани за управление на миграционните потоци. Особено внимание се отделя на взаимовръзката между икономическите, политическите и екологичните фактори, както и на необходимостта от ефективна и справедлива европейска миграционна политика.

1. Основна тема и предмет на анализа

Основната тема е миграцията към Европейския съюз, разгледана чрез причините за преместването на хора, видовете миграция и мерките,

предприемани от ЕС за регулиране на миграционните процеси. Текстът обхваща три основни направления:

– причини за миграцията – социалнополитически, демографски, икономически и екологични фактори (EP 2020);

– правни и институционални механизми – международна закрила, легални възможности за работа и пребиваване (CEU 2024);

– обща европейска политика – управление на миграционните потоци, охрана на външните граници и Нов пакт за миграцията и убежището (CEU 2024).

Предмет на анализа е начинът, по който са обяснени причините за миграцията и са представени мерките на Европейския съюз за нейното управление.

2. Основна теза

Основната теза на текста е, че миграцията е многоизмерен процес, обусловен от съчетанието на различни фактори, и че нейното управление изисква правни възможности за законно пребиваване и трудова заетост и механизми за международна закрила и координация между държавите членки.

Текстът не разглежда миграцията единствено като икономически процес или като проблем на граничната сигурност. Той представя едновременно причините, поради които хората напускат държавите си, и условията, привличащи мигрантите към Европа. Така се формира причинно-следствена логика: фактори в страната на произход → решение за миграция → избор на държава на местоназначение → правен статут и интеграция → мерки за управление на миграцията. Тази логика е подходяща за систематично изследване, тъй като свързва индивидуалните мотиви за миграция с икономическите условия и институционалната политика.

3. Структура и логическа последователност

Текстът е организиран тематично и преминава от общото определение за миграция към причините за нея, а след това към политиките на ЕС.

Раздел	***Основно съдържание***	***Функция***
Въведение	Данни за мигрантите в ЕС	Представя мащаба на явлението
Определение	Същност на миграцията	Изяснява основното понятие
Причини	Политически, икономически, демографски и екологични фактори	Обяснява защо възниква миграцията

Раздел	*Основно съдържание*	*Функция*
Легална миграция	Разрешения за работа и пребиваване	Представя законовите възможности
Нов пакт на ЕС	Общи процедури и споделяне на отговорността	Разглежда институционалните решения

4. Анализ на причините за миграцията

4.1. *Социално-политически фактори*

Текстът посочва преследването, въоръжените конфликти, тероризма и нарушенията на човешките права като причини, които могат да принудят хората да напуснат страната си (ЕР 2020). Съществото тук е разграничението между миграция по личен избор и принудително разселване. Хората, които бягат от преследване или сериозна опасност, могат да имат основания да поискат международна закрила.

Това разграничение е важно, защото мигрант, търсещ убежище, и признат бежанец не са взаимнозаменяеми правни категории. Търсещият убежище очаква решение по молбата си, докато статутът на бежанец се предоставя при изпълнение на съответните правни критерии (CEU 2024).

В текста обаче тези категории не са разграничени достатъчно ясно. Изразът „бежанци по хуманитарни причини“ също е по-общ от точните правни определения, използвани в европейското и международното право.

4.2. *Демографски и икономически фактори*

Втората група фактори включва безработицата, ниските доходи, ограничените образователни възможности и различията в жизнения стандарт (ЕР 2020). Текстът насочва вниманието към двустранния характер на миграционното решение:

– фактори на подтикване – неблагоприятни условия, които насърчават напускането на страната на произход;

– фактори на привличане – възможности за работа, по-високи доходи, образование и по-добри условия на живот в държавата на местоназначение.

Тази рамка помага да се разбере защо миграцията не може да бъде обяснена само с един фактор. Икономическите мотиви могат да съществуват едновременно със семейни, социални и политически обстоятелства.

Посочените данни за 169 млн. трудови мигранти през 2019 г. също показват, че миграцията е глобално явление, което надхвърля границите на ЕС. Тези данни обаче са исторически и не трябва да се представят като актуална оценка за 2026 г. без допълнителна проверка.

4.3. *Екологични фактори*

Третата група включва природни бедствия и изменения на околната среда, които могат да направят дадено място трудно или невъзможно за обитаване (EP 2020). Особено важна е уговорката, че екологичните фактори често действат в комбинация с бедност, демографски натиск, конфликти и ограничен достъп до ресурси.

Например сушата сама по себе си не води непременно до миграция. Последиците зависят и от възможностите за адаптация, доходите на домакинствата, наличието на държавна подкрепа и достъпа до вода и храна.

Текстът споменава прогноза от 25 млн. до 1 млрд. екологични мигранти до 2050 г. Този диапазон е изключително широк и следва да бъде представен с конкретен източник, методология и обяснение на несигурността. Не е коректно той да се възприема като точна или общоприета прогноза (EP 2020).

5. Анализ на политиките на Европейския съюз

5.1. Легални пътища за миграция

Текстът разглежда три инструмента: Синята карта на ЕС, единното разрешение за работа и пребиваване и статута на дългосрочно пребиваващ гражданин на трета страна (EP 2020). Тези инструменти имат различни цели и условия за прилагане. Синята карта е предназначена за висококвалифицирани работници, докато единното разрешение обединява разрешението за работа и пребиваване в съответната правна процедура. Статутът на дългосрочно пребиваващ се придобива при изпълнение на определени условия и не представлява автоматично право на неограничено пребиваване за всеки чужд гражданин (EP 2020).

Съществената идея е, че ЕС се стреми да регулира част от миграцията чрез законни процедури, като същевременно отговаря на потребностите на пазара на труда. Тук обаче липсва по-задълбочена оценка на практическите ограничения – различията между националните системи, изискванията към кандидатите, признаването на квалификации и достъпът до жилище и услуги.

5.2. *Нов пакт на ЕС за миграцията и убежището*

Това е основната част от текста, посветена на общата европейска политика. Посочени са три водещи цели (CEU 2024):

– по-ефективно управление на пристигащите лица;

– по-унифицирани процедури за миграция и убежище;

– по-справедливо разпределение на отговорността между държавите членки.

Представено е и понятието за солидарност – държавите могат да допринасят чрез приемане на лица, финансови вноски или оперативна и техническа подкрепа (CEU 2024). Това обобщение отразява основната логика на пакта, но не разглежда подробно възможните трудности при прилагането му, включително различията в националните административни възможности, процедурите по разглеждане на молби и защитата на основните права.

Важна актуализация е, че текстът описва пакта като система, чието въвеждане предстои. Това вече не е актуално към 17 октомври 2026 г. Съветът на ЕС приема пакта на 14 май 2024 г., а правилата му започват да се прилагат на 12 юни 2026 г. Следователно материалът трябва да бъде редактиран, ако ще се използва като съвременен информационен източник (CEU 2024).

6. Проверка на фактите и актуалността на данните

Тъй като текстът съдържа статистически и правни твърдения, важно е да се разграничат данните, които са потвърдени за посочения исторически период, от информацията, нуждаеща се от актуализация.

Твърдение в текста	***Резултат от проверката***
23,7 млн. граждани на държави извън ЕС към 1 януари 2021 г., или 5,3% от населението (EP 2020)	Потвърдено в публикацията на Европейския парламент. Това е историческа стойност, а не актуален показател за 2026 г.
384 245 души са получили международна закрила в ЕС през 2022 г. (Eurostat 2023).	Потвърдено от Евростат. Това са лица, получили статут на закрила, а не всички, подали молби за убежище
Сирийци, афганистанци и венецуелци са основните групи сред получилите закрила през 2022 г. (Eurostat 2023).	Потвърдено: съответно 29%, 23% и 6% от общия брой на получилите закрила
Пактът за миграцията е одобрен през април 2024 г. (CEU 2024).	Частично точно. Европейският парламент го приема през април 2024 г., а Съветът на ЕС приема законодателния пакет на 14 май 2024 г. Правилата започват да се прилагат през юни 2026 г.

Твърдение в текста	*Резултат от проверката*
До 2050 г. екологичните мигранти ще бъдат между 25 млн. и 1 млрд. души	Необходимо е допълнително библиографско уточнение. Широкият диапазон не бива да се представя като прецизна прогноза без конкретен източник и методологичен контекст

7. Силни страни на текста

Основните предимства са следните:

– широк тематичен обхват – разгледани са политически, икономически, демографски и екологични причини;

– разбираем език – термините са обяснени по начин, подходящ за широка аудитория;

– използване на статистически данни – включени са конкретни числа и препратки към Евростат и международни организации;

– връзка между причините и политиките – текстът не се ограничава до описание на миграцията, а представя и механизмите за нейното управление;

– практическа насоченост – информацията за разрешенията за работа и пребиваване и за общата политика на ЕС има непосредствена обществена приложимост.

8. Ограничения и слабости

Въпреки информационната си стойност текстът има няколко ограничения

– липса на ясно посочена методология – не е уточнено как са подбрани източниците, как са съпоставени различните статистически показатели и по какви критерии са определени основните миграционни фактори;

– неравномерна актуалност – използват се данни от 2019, 2021 и 2022 г., докато разделът за миграционния пакт вече е остарял по отношение на етапа на прилагане. Тези времеви разлики трябва да бъдат ясно обозначени;

– недостатъчно разграничаване на правните категории – понятията „мигрант“, „търсещ убежище“, „бежанец“ и „лице, получило международна закрила“ имат различно значение. По-прецизното им използване би подобрило правната точност;

– ограничен анализ на последиците – текстът описва причините за миграцията и политическите инструменти, но почти не анализира после-

диците за пазара на труда, публичните услуги, демографското развитие, интеграцията и административния капацитет на приемащите държави;

– ограничена оценка на политическите мерки – представени са целите на ЕС, но не са разгледани систематично показателите, чрез които може да се оцени ефективността на политиките, нито трудностите при тяхното прилагане.

Това не означава, че текстът е непременно неверен или пристрастен. Означава, че той има предимно обяснителна, а не оценъчна функция.

Изводи

Въз основа на направения анализ може да се заключи, че миграцията към Европейския съюз е сложен процес, който се определя от съчетанието на различни обстоятелства. Военните конфликти, политическата нестабилност, бедността, липсата на работа и климатичните промени са сред основните причини хората да търсят по-сигурна и благоприятна среда за живот. Наред с тях важна роля имат възможностите за образование, професионално развитие и по-висок жизнен стандарт.

Първият основен извод е, че миграцията не може да бъде обяснена единствено с икономически причини. В много случаи решението за напускане на родната страна е резултат от едновременното действие на няколко фактора. Поради това е необходимо миграционните процеси да се разглеждат в тяхната цялост, като се отчитат условията в държавите на произход и възможностите в страните на местоназначение.

Вторият извод е, че Европейският съюз се нуждае от последователна и добре координирана миграционна политика. Законните възможности за работа и пребиваване, общите процедури за предоставяне на убежище и сътрудничеството между държавите членки са важни инструменти за по-ефективно управление на миграцията. Прилагането на тези мерки трябва да бъде съобразено с потребностите на европейските общества и със задължението за защита на човешките права.

Третият извод е, че успешното управление на миграцията не се изчерпва с контрола на границите. Необходимо е да се обръща внимание и на интеграцията на мигрантите, достъпа им до образование, здравни услуги и трудова заетост, както и на възможните последици за икономиката и обществените системи на приемащите държави. По този начин могат да се ограничат социалните затруднения и да се създадат условия за по-пълноценно участие на мигрантите в обществения живот.

Четвъртият извод е свързан с необходимостта от използване на актуална и достоверна информация. Статистическите данни и нормативните актове се променят с течение на времето, затова при анализа на миграцията трябва ясно да се посочват периодите, за които се отнасят. Също така е важно да се разграничават понятията „мигрант“, „търсещ убежище“ и „бежанец“, тъй като те имат различно значение и са свързани с различни права и правни процедури.

Заключение

Предоставеният текст представлява достъпно въведение в темата за миграцията към Европейския съюз. Основното му достойнство е, че свързва различните причини за миграция с правните и институционалните механизми за нейното управление.

Основните направления за подобрение са актуализирането на статистическите и правните сведения, по-прецизното използване на терминологията и включването на критичен анализ на ефективността на европейските политики.

В обобщение, миграцията е дългосрочно обществено явление, което изисква балансирани решения и съвместни действия на национално и европейско равнище. Ефективната политика следва да съчетава сигурността, спазването на закона, защитата на човешкото достойнство и създаването на законни възможности за миграция. Само чрез комплексен подход Европейският съюз може да отговори на предизвикателствата, свързани с миграционните процеси, и същевременно да отчита интересите на приемащите общества и на хората, които търсят по-добро бъдеще.

БЕЛЕЖКИ

1. Евростат. Статистика за миграцията и убежището. Официален статистически портал на Европейския съюз. https://ec.europa.eu/eurostat/web/migration-asylum

2. Евростат. (2023). Решенията по молбите за убежище се увеличават с 40% през 2022 г. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20230427-1 .

ЛИТЕРАТУРА

ЕП, 2020. Сигурност, бедност, климат: защо хората мигрират. Публикувано на 2 юли 2020 г., последна актуализация на 16 април 2024 г. *Официален сайт на Европейския парламент*. Достъпно на: https://www.europarl.europa.eu/topics/bg/article/20200624STO81906/sighurnost-bednost-klimat-zashcho-khorata-mighrirat

СЕС, 2024. Пакт за миграцията и убежището. *Официален сайт на Съвета на ЕС*. Достъпно на: https://www.consilium.europa.eu/bg/policies/eu-pact-migration-asylum/.

ЕВРОСТАТ, 2024. Миграция и убежище в Европа – издание 2023 г. Достъпно на: https://ec.europa.eu/eurostat/web/interactive-publications/migration-2023.

REFERENCES

EP, 2020. Sigurnost, bednost, klimat: zashto horata migrirat. Publikuvano na 2 yuli 2020 g., posledna aktualizatsia na 16 april 2024 g. *Ofitsialen sayt na Evropeyskia parlament*. Available from: https://www.europarl.europa.eu/topics/bg/article/20200624STO81906/sighurnost-bednost-klimat-zashcho-khorata-mighrirat. [In Bulgarian].

CEU, 2024. Pakt za migratsiyata i ubezhishteto. *Ofitsialen sayt na Saveta na ES*. Available from: https://www.consilium.europa.eu/bg/policies/eu-pact-migration-asylum/. [In Bulgarian].

EVROSTAT, 2024. *Migratsia i ubezhishte v Evropa – izdanie 2023 g.* Available from: https://ec.europa.eu/eurostat/web/interactive-publications/migration-2023. [In Bulgarian].

SECURITY, POVERTY, CLIMATE: WHY PEOPLE MIGRATE

Abstract. Migration is a complex process influenced by various political, economic, social, and environmental factors. People leave their home countries due to war, persecution, human rights violations, unemployment, low income, and adverse climatic conditions. At the same time, opportunities for a better life, education, and professional development in other countries also encourage relocation (EP 2020).

The European Union implements various measures to manage migration processes. These include legal avenues for work and residence, the provision of international protection, and cooperation among member states. An important step in this regard is the New Pact on Migration and Asylum, which aims to improve common procedures and ensure a fairer distribution of responsibilities among EU countries (CEU 2024).

Analysis shows that migration cannot be attributed to a single cause, as multiple factors often act simultaneously. Although the text under review provides useful information on the subject, some statistical data and legal details require updating. It is also necessary to clearly distinguish between migrants, asylum seekers, and refugees.

Migration is a phenomenon of significant social importance that requires a balanced approach. Its effective management entails

the protection of human rights, the creation of legal avenues for migration, and coordinated action among European states.

Keywords: migration; European Union; international protection; migration policy; economic and environmental factors; human rights

Hristo Marukov
Sofia, Bulgaria
E-mail: marukovbg@yahoo.com

https://doi.org/10. 66334/annu26_trudmigrpogled

ТРУДОВАТА МИГРАЦИЯ – НИЩО ТРЕВОЖНО, ПОГЛЕДНАТО И ОТ ДВЕТЕ СТРАНИ

Христо Маруков

Абстракт. Настоящата разработка анализира трудовата миграция като икономическо и социално явление, чиито последици засягат както държавите на произход, така и приемащите общества. Основната цел е да се представят различните измерения на миграционните процеси и да се оцени доколко разпространените опасения относно тяхното въздействие са обосновани. Разгледани са ролята на паричните преводи за домакинствата и местната икономика, проблемът с емиграцията на квалифицирани специалисти, влиянието на имигрантите върху заетостта и възнагражденията, както и отражението им върху публичните финанси и социалните системи. Анализът показва, че трудовата миграция може да създава възможности за икономическо развитие, но същевременно поражда рискове, свързани с недостига на кадри, неравнопоставеността и несигурните условия на труд. Изводът е, че нейните резултати зависят от икономическата среда, характеристиките на мигрантите и ефективността на провежданите политики. Необходим е балансиран подход, основан на проверими данни и отчитане на интересите на всички засегнати страни.

Ключови думи: изтичане на мозъци; икономическо развитие; миграционни политики; парични преводи; трудова миграция; трудов пазар

Увод

В условията на глобализация и нарастваща взаимосвързаност между националните икономики трудовата миграция се утвърждава като важен фактор, който оказва влияние върху развитието на пазара на труда, демографските процеси и социалната среда. Преместването на хора от една държава в друга с цел намиране на работа е свързано както със стремежа към по-добри доходи и професионална реализация, така и с различията в икономическите възможности, условията на труд и жизнения стандарт между отделните страни. Поради това трудовата миграция представлява явление, което изисква задълбочено разглеждане от икономическа и социална гледна точка (Makaulif, Oucho 2024).

Значението на проблема се определя от факта, че миграционните процеси пораждат последици както за държавите, от които заминават работници, така и за страните, които ги приемат. За първите емиграцията може да осигури допълнителни финансови средства чрез паричните преводи на работещите в чужбина, но същевременно може да доведе до недостиг на квалифицирани кадри и намаляване на трудоспособното население. За приемащите държави привличането на чуждестранни работници създава възможности за преодоляване на дефицита на работна сила и за поддържане на икономическата активност. Наред с това възникват въпроси, свързани с конкуренцията за работни места, равнището на възнагражденията и достъпа до социални услуги (Rata, Chandra, Kim, Mahmud, Plaza 2024).

Обект на изследването е трудовата миграция като социално-икономически процес, свързан с движението на работна сила между отделните държави.

Предмет на изследването са икономическите и социалните последици от трудовата миграция за държавите на произход и за приемащите общества, включително отражението ѝ върху заетостта, доходите, квалификацията на работната сила и публичните финанси.

Основната цел на разработката е да се анализират различните ефекти на трудовата миграция и да се изясни защо нейното въздействие трябва да се оценява от гледната точка на всички участници в миграционния процес.

За постигането на тази цел са поставени следните задачи:

– да се разгледат основните икономически и социални причини за трудовата миграция;

– да се анализират ползите и рисковете за държавите, от които заминават работници;

– да се изследва влиянието на имигрантите върху заетостта, заплатите и социалните системи в приемащите държави;

– да се открояят факторите, които определят положителните и отрицателните последици от миграционните процеси;

– да се формулират изводи относно необходимостта от балансирани и ефективни политики в областта на трудовата миграция.

В статията се прилага аналитичен и сравнителен подход, чрез който се съпоставят последиците от миграцията за изпращащите и приемащите държави. Основното разбиране е, че трудовата миграция не може да бъде определена еднозначно като проблем или като безусловна полза. Нейното въздействие зависи от конкретните икономически условия, квалификацията на работниците, възможностите за професионална реализация и механизмите за защита на трудовите права.

1. Основна тема и предмет на анализа

Основната тема на текста е трудовата миграция и нейното икономическо, социално и демографско въздействие както върху държавите, от които хората емигрират, така и върху държавите, които приемат чуждестранни работници.

Материалът разглежда миграцията като процес, който не трябва да се оценява единствено чрез негативните последици от напускането на работна сила или чрез опасенията, че чуждестранните работници отнемат работни места на местното население. Основният акцент е поставен върху необходимостта да се анализират едновременно ползите, разходите и дългосрочните последици от миграционните процеси.

2. Основна теза

Основната теза на текста е, че трудовата миграция не е непременно заплаха за икономическото и социалното развитие, а при подходящо управление може да създава ползи както за изпращащите, така и за приемащите държави.

Авторът се противопоставя на едностранчивото разбиране за миграцията като процес, при който едната страна задължително губи, а другата печели. Вместо това се застъпва позицията, че резултатите зависят от характеристиките на мигрантите, състоянието на трудовия пазар, институционалната среда и начина, по който се използват придобитите доходи и знания.

3. Структура и логическа последователност

Текстът е организиран тематично и следва сравнителен подход. Първоначално се представя общата идея за миграцията като част от глобализацията, след което изложението се разделя на две основни части – за държавите, които изпращат работници в чужбина, и за държавите, които приемат имигранти.

Таблица 1

Раздел	***Основно съдържание***	***Функция***
Въведение	Доклад на Международната организация по миграция и глобализацията	Обосновава значението на темата
Изпращащи държави	Парични преводи и икономическо развитие	Разглежда възможните ползи от емиграцията
Изтичане на мозъци	Миграция на квалифицирани специалисти	Оспорва схващането, че напускането на образовани хора винаги е загуба
Приемащи държави	Работни места, заплати и конкуренция	Анализира въздействието върху трудовия пазар
Социални системи	Данъци, осигуровки и публични услуги	Разглежда фискалните последици от имиграцията
Заключителна аргументация	Сравнение на ползите и разходите	Подкрепя тезата за необходимостта от балансирана оценка

Съществено предимство на структурата е, че тя разглежда миграцията от гледната точка на двете страни в процеса. Така се избягва ограничаването на анализа само до проблемите на държавата на произход или само до интересите на приемащата страна.

4. Анализ на последиците от трудовата миграция за изпращащите държави

4.1. Парични преводи и икономическо развитие

В първата част авторът разглежда схващането, че емиграцията възпрепятства икономическото развитие, защото страната губи част от своята работна сила, особено сред младото и икономически активното население.[64]

Създаване на предпоставки за икономическа активност в отрасли като търговията, строителството и туризма.[65]

Пренасяне на знания и професионални умения при завръщане на емигрантите.[66]

Този аргумент показва, че икономическият ефект от емиграцията не се изчерпва със загубата на работници. Доходите, придобити в чужбина, могат да се превърнат в допълнителен ресурс за домакинствата и местната икономика (Rata, Chandra, Kim, Mahmud, Plaza 2024).

Необходимо е обаче да се направи разграничение между подпомагането на семейното потребление и дългосрочния икономически растеж. Изразходването на получените средства за храна, жилище и образование подобрява благосъстоянието, но не води автоматично до производствени инвестиции. Освен това паричните преводи не могат сами по себе си да компенсират всички последици от загубата на работна сила, особено когато напускат специалисти в сектори с недостиг на кадри.

Следователно аргументът на автора е основателен като възможност, но не бива да се тълкува като доказателство, че емиграцията винаги ускорява развитието на изпращащата държава.

4.2. Проблемът с изтичането на мозъци

Втората основна тема, свързана с изпращащите държави, е емиграцията на висококвалифицирани специалисти и млади хора с високо образование.[67]

Авторът оспорва схващането, че напускането на образованите граждани задължително представлява загуба за страната. Според изложената позиция миграцията на квалифицирани кадри може да се разглежда и като резултат от недостатъчните възможности за професионална реализация в държавата на произход.[68]

Тук се открояват три основни аргумента. Първо, значението на възможностите за реализация. Второ, възможността за придобиване и пренасяне на знания. Трето, свободата на движение. Авторът подчертава правото на хората да избират къде да живеят и работят. Този аргумент добавя индивидуално и етично измерение към икономическия анализ.[69]

5. Анализ на последиците от трудовата миграция за приемащите държави

5.1. Въздействие върху заетостта и работните места

Втората голяма част на текста разглежда опасенията, че имигранти-

те отнемат работните места на местните граждани и увеличават безработицата.

Авторът оспорва това схващане, като посочва, че чуждестранните работници често се насочват към отрасли, в които има недостиг на работна ръка. Сред посочените примери са селското стопанство, строителството, ресторантьорството, ремонтните дейности и различни услуги. Отделено е внимание и на висококвалифицираната заетост, включително в информационните технологии (Kis, Maldonado, Turini, Van Herk 2026).[70]

Следователно не е правилно нито да се твърди, че имигрантите неизбежно отнемат работни места, нито да се приема, че подобен ефект е невъзможен. Необходимо е да се изследват конкретните отрасли, регионалните условия и квалификационният профил на работниците.

5.2. Влияние върху равнището на заплатите

Текстът разглежда и опасенията, че увеличаването на броя на имигрантите води до понижаване на възнагражденията на местното население.

Основният извод е, че ефектът върху заплатите не може да бъде определен само въз основа на броя на имигрантите. Необходими са данни за конкретния трудов пазар и за условията, при които се наема работната сила (Kis, Maldonado, Turini, Van Herk 2026).

5.3. Положение на имигрантите на трудовия пазар

В края на анализа на трудовата заетост авторът обръща внимание на факта, че имигрантите могат да бъдат по-уязвими при икономически спад. Посочва се, че те често получават по-ниски възнаграждения и могат да бъдат засегнати от дискриминация или от участие в неформалната икономика.[71]

Този аспект е съществен, защото допълва анализа на икономическите ефекти с въпроса за равнопоставеността на работниците.

По-ниското заплащане на чуждестранните служители невинаги се обяснява само с по-ниската им квалификация. Възможни причини са недостатъчното владеене на езика, трудностите при признаване на дипломи, ограничените професионални контакти, несигурният правен статут и дискриминационните практики.

При икономическа криза работниците с временни договори, ограничена социална защита или несигурно положение на пазара на труда могат да бъдат изложени на по-висок риск от безработица. Това обаче не означава, че всички имигранти са в еднакво положение или че във всички държави следват идентични тенденции.

От аналитична гледна точка този раздел показва, че последиците от имиграцията зависят не само от икономическите условия, а и от институционалната защита на работниците. Ефективният контрол върху трудовите отношения може да ограничи експлоатацията и да намали риска миграцията да бъде използвана като средство за заобикаляне на установените трудови стандарти.[72]

6. Проверка на фактите и актуалността на информацията

Тъй като материалът съдържа конкретни статистически стойности и препратки към изследвания, необходимо е да се направи разграничение между общите икономически аргументи и твърденията, които изискват проверка по първични източници.

Важно е да се подчертае, че самият предоставен текст не съдържа пълни библиографски данни за всички цитирани изследвания. Поради това не може да се потвърди независимо всяка посочена стойност само въз основа на материала.

Таблица 2

Твърдение в текста	Аналитична оценка
Около 90% от трудовите емигранти редовно изпращат пари на близките си[73]	Изисква посочване на източник, държава, период и методология. Не следва да се приема като универсален показател.
Паричните преводи стимулират икономическото развитие на изпращащите държави (Rata, Chandra, Kim, Mahmud, Plaza 2024)	Икономически обоснована възможност, но ефектът зависи от начина на използване на средствата и условията в местната икономика.
Емиграцията на квалифицирани специалисти не води непременно до обедняване на държавата	Основателно като общо твърдение, но не доказва, че загубата на кадри няма отрицателни последици за отделни отрасли.
Имигрантите не отнемат работни места от местните работници (ИПИ, 2006; Kis, Maldonado, Turini, Van Herk 2026)	Прекалено категорично, ако се разглежда като универсално твърдение. Ефектите зависят от конкретния трудов пазар.

Въздействието върху заплатите е сравнително малко (Kis, Maldonado, Turini, Van Herk 2026)	Необходимо е да се уточнят изследванията, периодът, използваната методология и групите работници, за които се отнасят оценките.
Имигрантите могат да допринасят повече чрез данъци, отколкото получават под формата на публични разходи (Makaulif, Oucho 2024)	Възможно е за определени групи и периоди, но не може да се обобщава за всички държави и мигранти.
Миграцията може да подпомогне икономическото развитие и на двете страни (Makaulif, Oucho 2024)	Обоснован общ извод, който трябва да бъде допълнен с анализ на разпределението на ползите и разходите.

8. Силни страни на текста

Материалът има няколко съществени предимства, които го правят подходящ за въвеждащ анализ на трудовата миграция.

8.1. Разглеждане на двете страни на миграционния процес

Най-голямото достойнство на текста е сравнителният подход. Авторът анализира както последиците за държавите, които губят част от работната си сила, така и ефектите за държавите, които привличат чуждестранни работници.

Това позволява да се разбере, че миграцията е трансграничен процес и че икономическите ползи и разходи могат да се разпределят неравномерно между държавите и отделните социални групи.

8.2. Оспорване на разпространени обществени представи

Използването на понятието „мит“ насочва вниманието към разликата между обществените страхове и икономическите аргументи. Текстът насърчава читателя да поставя под въпрос автоматичните заключения, че емиграцията непременно води до бедност или че имигрантите винаги натоварват социалната система.

9. Ограничения и слабости на текста

Въпреки достойнствата си, материалът има ограничения, които трябва да бъдат отчетени при използването му в академична работа.

9.1. Прекалено категорично представяне на някои изводи

Заглавието и употребата на понятието „мит“ предполагат, че негативните оценки на миграцията са предимно неоснователни. Подобна формулировка улеснява възприемането на основната теза, но може да ограничи критичния анализ.

В действителност икономическите последици от миграцията зависят от конкретните условия. Едно явление може да носи ползи за националната икономика като цяло и едновременно с това да създава затруднения за определени професии, региони или социални групи.

Затова по-научният подход е да се изследват условията, при които даден ефект възниква, вместо предварително да се определя като мит или неоспорим факт.

9.2. Ограничено разглеждане на отрицателните последици за изпращащите държави

Авторът обръща внимание на паричните преводи и възможността за завръщане на квалифицирани работници, но не разглежда достатъчно подробно рисковете от продължителното изселване.

Сред тях са недостигът на специалисти, загубата на публични инвестиции в образование и обучение, намаляването на населението в трудоспособна възраст и отслабването на икономическата активност в определени региони.

Тези последици са особено важни, когато емиграцията засяга отрасли, в които обучението на нови кадри изисква години.

9.3. Недостатъчно разграничаване между различните групи мигранти

Текстът понякога разглежда имигрантите като обща категория, въпреки че между тях могат да съществуват съществени различия.

Висококвалифициран специалист, сезонен работник, служител с временен договор и предприемач имат различни икономически характеристики и потребности. Техният принос към публичните финанси и влиянието им върху трудовия пазар също могат да бъдат различни.

По-прецизното разграничаване на тези групи би позволило по-надеждни заключения.

9.4. Ограничен анализ на разпределението на ползите и разходите

Материалът се съсредоточава върху общия икономически ефект, но не изследва достатъчно въпроса кой конкретно печели и кой може да понесе разходите.

Например работодателите могат да спечелят от по-лесния достъп до работна сила, докато някои работници в определен сектор могат да се сблъскат с по-силна конкуренция. Семействата на емигрантите могат да получат по-високи доходи, но същевременно да изпитат социални затруднения вследствие на продължителната раздяла.

Следователно националният икономически резултат не е достатъчен, за да се оцени цялостното обществено въздействие.

9.5. Исторически контекст и необходимост от актуализация

Материалът се позовава на събития и изследвания от началото на XXI век. Това означава, че част от неговите примери отразяват конкретната икономическа и политическа среда на онзи период.

При използването му днес е необходимо да се уточни кои твърдения имат общо теоретично значение и кои зависят от историческите условия.

Особено внимание следва да се отдели на промените в европейските трудови пазари, свободното движение на работници, демографското развитие и миграционните политики след публикуването на материала.

Изводи

Въз основа на направения анализ могат да бъдат формулирани няколко основни извода относно същността и последиците от трудовата миграция.

На първо място, трудовата миграция е сложен процес, чието въздействие не може да бъде определено еднозначно като положително или отрицателно. Тя е свързана с икономическите различия между държавите, възможностите за професионално развитие и стремежа на хората към по-добри условия на живот. Поради това оценката на миграционните процеси трябва да отчита както индивидуалните мотиви на работниците, така и потребностите на националните икономики.

На второ място, емиграцията може да носи определени ползи за държавите на произход. Доходите, изпращани от работещите в чужбина, подпомагат семейните бюджети, подобряват възможностите за потребление и могат да осигурят средства за образование, жилище или развитие на малък бизнес. Въпреки това тези положителни ефекти не компенсират автоматично загубата на работна сила. Когато напускат значителен брой млади и квалифицирани специалисти, държавите могат да се изправят пред недостиг на кадри и затруднения при предоставянето на определени услуги (Rata, Chandra, Kim, Mahmud, Plaza 2024).

На трето място, имиграцията може да допринесе за развитието на приемащите държави чрез попълване на свободни работни места, увеличаване на икономическата активност и осигуряване на допълнителни приходи от данъци и осигурителни вноски. Чуждестранните работници могат да подпомагат дейността на предприятията и да участват в сектори, в които местната работна сила не е достатъчна. Въздействието им върху заетостта и заплатите обаче зависи от особеностите на конкретния трудов пазар и не следва да се оценява чрез общи заключения за всички професии и отрасли (Kis, Maldonado, Turini, Van Herk 2026).

На четвърто място, икономическите резултати от миграцията трябва да се разглеждат заедно със социалните последици. Несигурните трудови договори, дискриминацията, неравното заплащане и ограниченият достъп до социална защита могат да поставят мигрантите в уязвимо положение. Ето защо спазването на трудовото законодателство и осигуряването на равнопоставено отношение са важни условия за ограничаване на негативните ефекти и за по-справедливо разпределение на ползите от миграцията.

На пето място, съществено значение има качеството на държавните политики. Ефективното управление на миграционните процеси изисква съобразяване с потребностите на работодателите, защитата на работниците и дългосрочните интереси на обществото. Политиките за професионално обучение, признаване на квалификациите, интеграция и задържане на специалисти могат да подпомогнат както приемащите държави, така и държавите на произход.[74]

Заключение

Текстът „Трудовата миграция – нищо тревожно, погледнато и от двете страни“ представя трудовата миграция като сложен икономически и социален процес, който не може да бъде оценяван единствено чрез негативните последици от напускането на работна сила или чрез опасенията за конкуренцията на трудовия пазар.

Основното му достойнство е сравнителният подход, чрез който се разглеждат както ефектите за изпращащите държави, така и последиците за приемащите общества. Материалът показва, че паричните преводи, професионалният опит, допълнителната работна сила и данъчните вноски могат да създават икономически ползи. Същевременно той поставя въпроси, свързани с изтичането на квалифицирани кадри, конкуренцията за работни места, възнагражденията и натоварването на публичните системи.

Основното ограничение на изложението е, че в стремежа си да оспори негативните обществени представи за миграцията, то понякога представя положителните ефекти по-убедително от възможните отрицателни последици. Част от статистическите твърдения също изискват допълнителна проверка и актуализация.

В заключение, трудовата миграция не трябва да се възприема единствено като загуба на човешки ресурси или като средство за преодоляване на недостига на работна сила. Тя представлява процес с различни измерения, чиито резултати зависят от икономическите условия, характеристиките на мигрантите и провежданите политики. Най-обоснованата оценка е тази, която отчита едновременно възможностите за развитие, съществуващите рискове и различията между отделните социални групи. Подобен подход създава основа за по-ефективно управление на миграцията и за постигане на по-добър баланс между икономическите интереси и социалната справедливост.

В обобщение, трудовата миграция не е нито безусловна икономическа полза, нито неизбежен обществен проблем. Нейното въздействие зависи от конкретните обстоятелства, от възможностите за трудова реализация и от политиките, които регулират миграционните процеси. Затова най-подходящият подход е основаното на доказателства изследване на ползите, разходите и тяхното разпределение между различните групи в обществото.

БЕЛЕЖКИ

1. ИПИ, 2006. Трудовата миграция – нищо тревожно, погледнато и от двете страни. ИПИ [online]. Available from: https://ime.bg/articles/trudowata-migraciq-nishto-trewovno-poglednato-i-ot-dwete-strani

2. ИПИ, 2006. Трудовата миграция – нищо тревожно, погледнато и от двете страни. ИПИ [online]. Available from: https://ime.bg/articles/trudowata-migraciq-nishto-trewovno-poglednato-i-ot-dwete-strani

3. ИПИ, 2006. Трудовата миграция – нищо тревожно, погледнато и от двете страни. ИПИ [online]. Available from: https://ime.bg/articles/trudowata-migraciq-nishto-trewovno-poglednato-i-ot-dwete-strani

4. ИПИ, 2006. Трудовата миграция – нищо тревожно, погледнато и от двете страни. ИПИ [online]. Available from: https://ime.bg/articles/trudowata-migraciq-nishto-trewovno-poglednato-i-ot-dwete-strani

5. ИПИ, 2006. Трудовата миграция – нищо тревожно, погледнато и от двете страни. ИПИ [online]. Available from: https://ime.bg/articles/trudowata-migraciq-nishto-trewovno-poglednato-i-ot-dwete-strani

6. ИПИ, 2006. Трудовата миграция – нищо тревожно, погледнато и от двете страни. ИПИ [online]. Available from: https://ime.bg/articles/trudowata-migraciq-nishto-trewovno-poglednato-i-ot-dwete-strani

7. ИПИ, 2006. Трудовата миграция – нищо тревожно, погледнато и от двете страни. ИПИ [online]. Available from: https://ime.bg/articles/trudowata-migraciq-nishto-trewovno-poglednato-i-ot-dwete-strani

8. Международна организация на труда (МОТ). *Глобални оценки за международните трудови мигранти – резултати и методология*. Трето издание. Женева, 2021 г.

9. Международна организация на труда (МОТ). *Глобални оценки за международните трудови мигранти – резултати и методология*. Трето издание. Женева, 2021 г.

0. ИПИ, 2006. Трудовата миграция – нищо тревожно, погледнато и от двете страни. ИПИ [online]. Available from: https://ime.bg/articles/trudowata-migraciq-nishto-trewovno-poglednato-i-ot-dwete-strani

1. Международна организация на труда (МОТ). *Глобални оценки за международните трудови мигранти – резултати и методология*. Трето издание. Женева, 2021 г.

ЛИТЕРАТУРА

МАКАУЛИФ, М.; ОУЧО, Л. А. (ред.), 2024. *Световен доклад за миграцията 2024*. Женева: Международна организация по миграция.

РАТА, Д.; ЧАНДРА, В.; КИМ, Е. Дж.; МАХМУД, А.; ПЛАЗА, С., 2024. *Паричните преводи се забавиха през 2023 г., но се очаква по-бърз растеж през 2024 г.* Вашингтон, Колумбия: Световна банка.

КИС, А.; МАЛДОНАДО, Х. Е.; ТУРИНИ, А.; ВАН ХЕРК, К., 2026. *Миграция, мобилност и пазарът на труда в Европейския съюз: актуални тенденции*. Европейска комисия, Генерална дирекция „Икономически и финансови въпроси“.

REFERENCES

KIS, A.; MALDONADO, H. E.; TURINI, A.; VAN HERK, K., 2026. *Migratsia, mobilnost i pazarat na truda v Evropeyskia sayuz: aktualni tendentsii.* Evropeyska komisia, Generalna direktsia „Ikonomicheski i finansovi vaprosi“ [in Bulgarian].

MAKAULIF, M.; OUCHO, L. A. (red.), 2024. *Svetoven doklad za migratsiyata 2024*. Zheneva: Mezhdunarodna organizatsia po migratsia [in Bulgarian].

RATA, D.; CHANDRA, V.; KIM, E. DZH.; MAHMUD, A.; PLAZA, S., 2024. *Parichnite prevodi se zabaviha prez 2023 g., no se ochakva po-barz rastezh prez 2024 g.* Vashington, Kolumbia: Svetovna banka [in Bulgarian].

LABOR MIGRATION – NOTHING TO WORRY ABOUT, VIEWED FROM BOTH SIDES

Abstract. This paper analyzes labor migration as an economic and social phenomenon, the consequences of which affect both countries of origin and host societies. The primary objective

is to present the various dimensions of migration processes and to assess the extent to which common concerns regarding their impact are justified. The study examines the role of remittances for households and local economies, the issue of the emigration of skilled professionals, the influence of immigrants on employment and wages, as well as their impact on public finances and social systems. The analysis indicates that while labor migration can create opportunities for economic development, it also gives rise to risks related to labor shortages, inequality, and precarious working conditions. The conclusion is that the outcomes depend on the economic environment, the characteristics of the migrants, and the effectiveness of the policies implemented. A balanced approach is required—one based on verifiable data and which takes into account the interests of all affected parties (IME, 2006).

Keywords: brain drain; economic development; migration policies; remittances; labor migration; labor market

Hristo Marukov
Sofia, Bulgaria
E-mail: marukovbg@yahoo.com

https://doi.org/10. 66334/annu26_uspacebezp

ПРЕДИЗВИКАТЕЛСТВОТО U-SPACE ЗА ИЗПЪЛНЕНИЕ НА ДЪРЖАВНИ ПОЛЕТИ С БЕЗПИЛОТНИ ВЪЗДУХОПЛАВАТЕЛНИ СРЕДСТВА

ас. д-р Христо Станев
Висше училище по телекомуникации и пощи

Абстракт. Войната в Украйна доказа възможностите на нов вид оръжие – безпилотното. Във въздуха то се използва за наблюдение, разузнаване, радиоелектронна война или комуникация, както и за нанасяне на прецизни удари. За мирно време е създадена нормативна регулация за въздушно пространство U-space в рамките на Европейски съюз. Изпълнението на полети с безпилотни въздухоплавателни средства в U-space се очаква да бъде в резултат на допълнителна услуга с висока автоматизация на дейностите. Очакванията за успешно въвеждане на U-space се основават на предположението за спазване на установените правила. На настоящия етап слабо се отчита необходимостта от интеграция на полети с държавни безпилотни въздухоплавателни средства в U-space. За осигуряване на операциите с безпилотни въздухоплавателни средства в U-space е необходимо изграждане на способности за противодействие на нарушителите на правилата. С настоящото изследване се определят предизвикателствата, чрез чието преодоляване да се създадат условия за безопасно изпълнение на функциите на държавата при изпълнение на държавни полети с безпилотни въздухоплавателни средства в U-space.

Ключови думи: държавен полет; държавно въздухоплавателно средство; безпилотно въздухоплавателно средство; U-space; гражданско-военна координация

I. Увод

Безопасното провеждане на държавни полети с безпилотни въздухоплавателни средства (БВС) във въздушно пространство, обслужвано от U-space оператор, е новото предизвикателство пред държавните институции, призвани да осигуряват отбрана, обществен ред и сигурност, както у нас, така и в Европейския съюз. Държавните институции изпълняват мисии в обществен интерес в условията на специфични правила за събиране и разпространение на информацията, при динамично променяща се оперативна среда. Характерно за непланираните държавни полети с БВС е времето за тяхното планиране и изпълнение, като правило в отговор на реакция при непредвидени обстоятелства, което предизвиква голямо напрежение в системата за управление на въздушното движение (УВД). Липсата на единен орган, който да обслужва (или контролира) изпълнението на държавни полети с БВС е организационната предпоставка, чието игнориране има потенциал да компрометира достигнатите нива за безопасно провеждане на въздухоплаване с пилотируеми и безпилотни въздухоплавателни средства (ВС).

В рамките на проект CORUS беше създадена основополагащата Концепция за операции в U-Space въздушно пространство, с идея за безопасно интегриране на голям брой безпилотни апарати в най-близкото до земята въздушно пространство, споделено с пилотирана авиация чрез услуги, като разрешаване на полети, геоинформираност, информация за трафика и разрешаване на конфликти[1] (Barrado et al. 2020).

Въоръженият конфликт в черноморския регион издигна на ново по-високо ниво ролята на БВС във въздухоплаването с ясно изразени два аспекта на приложение – използване като оръжие и при противодействие срещу дронове. Тактиките за тяхното използване във въоръжената борба се менят почти ежемесечно, в зависимост от постигнатия напредък в борбата срещу тях, като всяка нова тактика надгражда старите. Това означава, че в близост до конфликтната зона е напълно нормално за дълго време да няма покритие на GPS сигнала, както и да са налице резултати от провеждана радиоелектронна война. Поемането на контрола над чуждо БВС е стандартна практика, ако електрониката му за управление го позволява (до момента няма информация за отклонен дрон, управляван по оптично влакно). Затова и нарушаването на въздушното пространство на съседните на конфликта страни от който и да е дрон, не определя еднозначно принадлежността на нарушението към една от двете воюващи страни.

Когато регистрираме нарушения с дронове в близост до стратегически обекти или граждански летища, в много малко случаи може да се каже, че тези нарушения не са планирани в рамките на хибридна война, водена извън границите на Украйна. Нуждата от създаване на адекватни мерки за противодействие на новия вид заплаха е налице.

В това изследване под „държавни полети“ ще се разбира провеждането на операции на държавни институции (военни, полиция или митница)[2] със собствени или наети БВС при спешно реагиране в интерес на отбраната или вътрешния ред, наблюдение, инспекция, търсене и спасяване, и други мисии с публична цел. На този етап полети с БВС за HEMS (Helicopter Emergency Medical Service) не попадат в определението за държавен полет, но всяка страна има свободата да реши с какъв приоритет да се осигурява тяхното провеждане.

Наличната регулаторна рамка за U-space урежда трафика на граждански БВС, като предвижда изключения за полети при аварийно реагиране, чиято практическа интеграция предстои да бъде разработена и изпитана (Teomitzi et al. 2025).

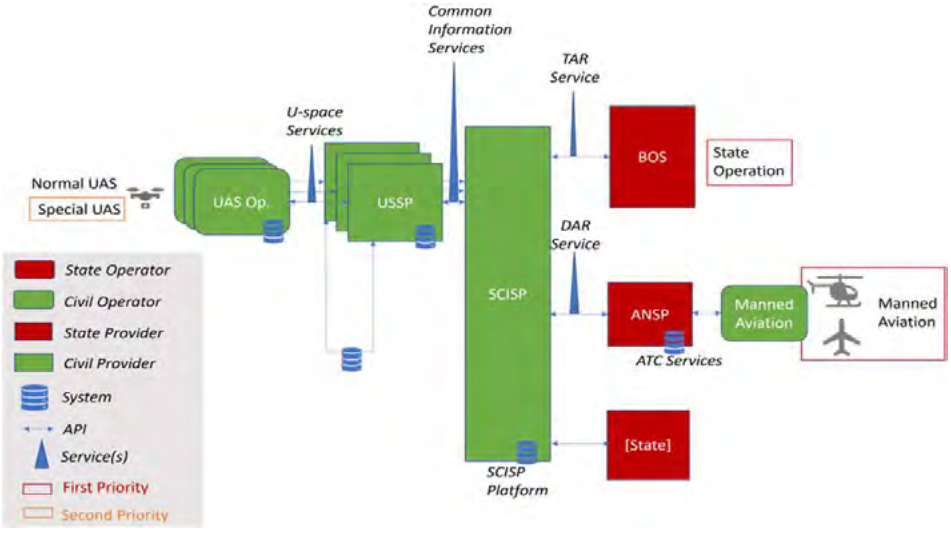
Темата е актуална поради факта, че няма много публикации в избрания контекст. Има концептуални и регулаторни анализи, симулации, прототипи и полеви демонстрации, но малко публикации предлагат изследване точно на държавни мисии в оперативно U-space въздушно пространство. Затова изследването отделя първичните експериментални резултати от нормативните и архитектурните предложения и оценява доколко вторите могат да бъдат отнесени към държавни операции.

II. Регулаторен и институционален аспект

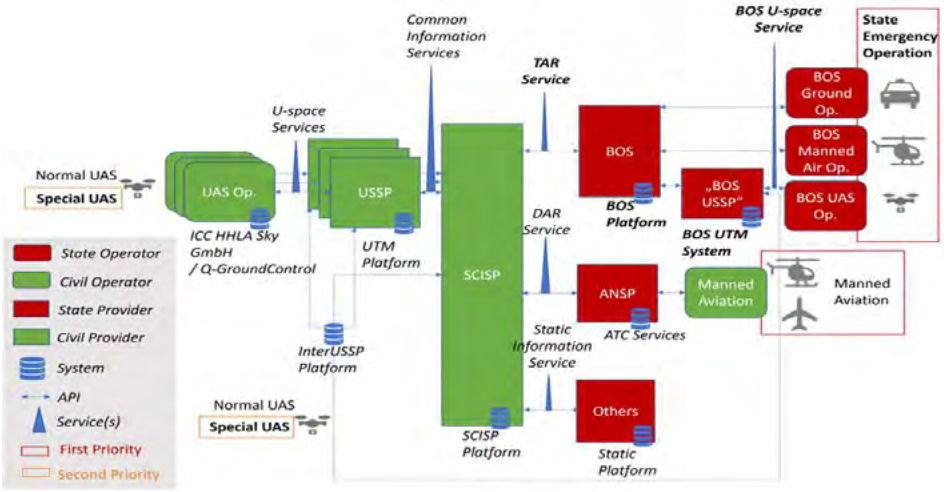
2.1. Гражданско ядро и държавни изключения

Важна особеност на концепцията за U-space са задължителните услуги и процедури за полети в предварително определените граници на U-space въздушно пространство. Анализът на регулаторната „неопределеност“ посочва, че операторите на дронове трябва да използват U-space услуги, но правилата не уточняват достатъчно отношенията между оператора и доставчика на U-space услуги, особено при разрешаването и активирането на полета (Grebner et al. 2023). За операторите на държавни БВС това означава, че общото правило може да е ясно на равнище принцип, но да е недостатъчно за мисии, при които целта, маршрутът или времето се променят внезапно. В изследване за германското въздушно пространство

по проект BLU-Space е направена връзка между U-space и държавните органи, реагиращи при извънредни ситуации с БВС (Teomitzi et al. 2025). В графичен вид е изобразена представата за връзката на държавните институции за реакция при извънредни обстоятелства с изградената инфраструктура за U-space, както е съгласно изискванията на Изпълнителен регламент (ЕС) 2021/664, видно на фигура 1. На фигурата се вижда варианта с един доставчик на информационни услуги и повече от един доставчик на обслужване в U-space. Пак в същото изследване се предлага създаването на единна платформа за свързване на операциите с държавни БВС с общия доставчик на информационни услуги, както е показано на фигура 2. Специфичното е, че се разглежда вариант с информация за всички операции на държавните институции, която да се обобщава в единен център (на фигурата е описано като BOS). Така за Германия се извежда ключовия проблем с интеграцията на държавни БВС в U-space, който трябва да бъде решен преди реалното въвеждане на U-space (Teomitzi et al. 2025). Следователно формалното наличие на изключение за участието на държавните силови институции не решава въпросите кой активира приоритета, как се информират останалите участници, кой носи отговорност при конфликт и как изключението се прекратява.



Фигура 1. Архитектура на U-space съгласно Регламент (ЕС) 2021/664



Фигура 2. Архитектура на U-space, допълнена с резултатите от изследванията по проекта BLU-Space

2.2. Разпределение на отговорностите

Видно от общата архитектура за U-space на фигура 1, същото се изгражда с ясно разпределени функции между държавата, общата информационна услуга, доставчика/ците на U-space обслужване (USSP/s), оператора/и на БВС и органите за обслужване на въздушното движение (ОВД), в рамките на обслужваното от тях въздушно пространство. В летищна среда данните за пилотиран и безпилотен трафик, географската информация и метаданните се консолидират чрез Common Information Service, до която достъп е осигурен на всеки USSP (Selvam & Lieb 2024). При изпълнение на държавен полет в U-space, държавният оператор трябва да запазва оперативния контрол върху мисията, като в същото време следва и да предоставя достатъчно точна информация, за да бъде полетът видим и координиран с останалия безпилотен трафик.

Тази структура може да се сблъска с институционални задължения за опазване на информация. Държавният орган може да има законово основание да ограничи разкриването на маршрут, докато системата за управление на въздушното движение се нуждае от информация за идентификация, позиция, намерение и статус. Литературата не дава единно решение за баланса между оперативната сигурност и информационната прозрачност, доколкото U-space е едновременно правна, техническа и публично-частна система, която изисква близка координация между регулатори, индустрия и публични институции (Huttunen 2019).

2.3. Приоритет, чувствителност и отчетност

Определянето на условията за даване на по-висок приоритет за държавен или спешен полет с БВС трябва да бъде нормативно уреден, включително с определяне на отговорния орган за това, а не оставен като общо изключение[3]. При симулация на аварийно кацане в споделено контролирано въздушно пространство и U-space, временната промяна на обема на U-space е наложила отклоняване или изчакване на пристигащ и заминаващ пилотиран трафик (Schwoch et al. 2023). Това показва, че приоритетът има измерими последици за други въздухоплавателни средства и изисква предварително дефинирани правила за уведомяване, времетраене, възстановяване на нормалния режим и запис на решенията.

За държавните мисии отчетността е ключова за осигуряване на безопасни операции с БВС. Освен че на държавните органи и организации им е вменена отговорност за безопасно използване на БВС и за вредите, причинени на трети лица от използването на БВС, същите следва „да документират всяко използване на БВС, като в случай на провеждане на разследване на инциденти или произшествия, причинени от или с БВС, предоставят данни на разследващите органи“[4]. От друга страна, когато държавният оператор е използвал изключение, трябва да може да докаже защо го е ползвал, кой е разрешил отклонението и как е оценен рискът за трети лица и пилотираната авиация. Публикациите за U-space подчертават, че системата включва и *legal recording*, но описват това като част от прототипната функционалност, а не като доказан режим за чувствителни държавни операции (Fas-Millán et al. 2024).

2.4. Оперативно разрешаване, планиране и изпълнение

Разрешението за операции в U-space е продължителен процес с отделно обособени фази – подаване на заявка, одобрение или отказ, активиране и деактивиране. Услугата за разрешаване на полети на безпилотни летателни системи (U-FAS – UAS Flight Authorization Service) е разработена на концептуално ниво и изисква операторът на БВС да получи разрешение от доставчик на U-space преди изпълнение на полета (Grebner & Fay 2022). При изпълнение на планови държавни полети с БВС (напр. за инспекция на критична инфраструктура или наблюдение на пътен трафик), тези дейности могат да се включат в процеса за разрешение, но при условия на спешност, времето за подготовка, заявяване, проверка, координация и промяна на маршрута може да стане част от оперативния риск.

В някои изследвания се посочва, че регулаторните изисквания към услугата за разрешаване са недостатъчно конкретизирани и трябва да бъдат трансформирани в технически изпълним процес (Grebner et al. 2023). Това е особено важно за държавните операции с БВС, при които може да има различни режими на разрешение: разрешение от държавния орган, условия за изпълнение на полетите в предварително одобрени коридори, необходимост от осигуряване на динамичен приоритет, незабавно аварийно активиране или полет в чувствителна зона. Без тези режими операторът може да бъде принуден или да наруши обичайния процес, или да забави мисията.

2.5. Промени в мисията и динамичен капацитет

Държавните мисии често не са статични. Ново местоположение на инцидента, промяна на зоната за търсене или появата на пилотиран трафик може да наложи пренасочване. U-space архитектурите предвиждат операции по подготовка и оптимизация на план, стратегическо и тактическо разрешаване на конфликти и управление на извънредни ситуации, но тестовете показват, че прилагането им зависи от конкретни решения за съвместимост, процедури, информация, използваемост и интеграция с наземната станция (Fas-Millán et al. 2024).

Моделите за динамично управление на капацитета предлагат едновременно планиране на траектории, конфигурация на въздушното пространство и баланс между търсене и капацитет. Симулационните резултати сочат по-добри показатели, когато тези функции се комбинират, вместо да се реализират частично (Tang, Xu & İnalhan 2022). Тези резултати са обещаващи за масови държавни операции, но остават симулационни, тъй като те не доказват, че алгоритъмът ще осигури необходимата предвидимост при реален спешен приоритет.

2.6. BVLOS (Beyond Visual Line of Sight) и автономност

Много държавни полети се изпълняват в условия без пряка видимост между оператора и БВС (BVLOS – Beyond Visual Line of Sight), за да обхванат големи райони за наблюдение, при търсене и спасяване, осъществяване на граничен контрол или инспекция на линейна инфраструктура. Сравнението на европейския CORUS ConOps с американския UTM ConOps показва, че нарастващото търсене на BVLOS операции изисква нови правила за безопасно споделяне на въздушното пространство и разчита на постоянно достъпна разпределена информационна мрежа (Lieb & Volkert 2020).

Полева демонстрация на U-space процедури е използвала до осем дрона и един пилотиран самолет, като е изследвала зони, сепарация и автономно detect-and-avoid. Резултатът е, че наблюдението на пилотираните въздухоплавателни средства може да позволи по-ефективно използване на пространството и да избегне прекомерно големи геозони (Alarcón et al. 2020). За държавните оператори това намалява риска от прекалено консервативни ограничения, но увеличава зависимостта от качеството и актуалността на наблюдението.

Подготовката на оператори и наземни системи за управление са ключови за изпълнение на полети в условия на BVLOS. Прототипни тестове са открили практически въпроси за съвместимостта, използваемостта, интеграцията с ground control station и ролите на екипажа по време на мисията (Fas-Millán et al. 2024). Това е съществено за държавни структури, които имат изградени собствени командни и комуникационни системи, различни от тези на търговските оператори. Свързването им с доставчика на обслужване по U-space е наложително, с оглед на възможността за провеждане на полети в активирано U-space въздушно пространство, както и при изпълнение на полицейски мисии при открити нарушители на правилата за използване на БВС в активирано U-space или друго въздушно пространство.

Изследванията за безопасността също посочват пропуск в обучението: процедурите и реда за използване на държавни БВС не е дефинирана достатъчно ясно, което може да създаде опасност (Milerová et al. 2022) при навлизане в активирана U-space зона. Следователно обучението трябва да обхваща не само пилотиране, а и работа с U-space услуги, действия при отказ на мрежова връзка, комуникация с органи за ОВД, управление на приоритет и координация с други държавни екипи.

III. Интеграционен аспект с пилотирана авиация

3.1. Ситуационна осведоменост и управление на въздушното движение

Интеграцията с УВД е критична там, където държавните полети с БВС се планират в близост до летища, визуални маршрути или контролирано въздушно пространство. Изпитването на U-FLY интерфейс в района на бившето летище Магдебург-Кохщедт показва, че той може да даде на кулата ситуационна осведоменост за безпилотния трафик и да обменя информация между предварително определен *safety pilot* и органите за ОВД (Selvam et al. 2025). Същото изследване обаче препоръчва осигуряването на

допълнителна информация за намеренията на екипажа на БВС и по-ефективна пряка гласова комуникация.

Този резултат има пряко значение за държавните мисии. При полицейски или спасителен полет само позицията и разрешеният маршрут може да не са достатъчни. Органите за ОВД трябва да са информирани дали БВС ще кръжи, ще променя височина, ще каца извън плана или ще прекрати мисията. Цифровото съобщение трябва да бъде допълнено с комуникационен канал, който позволява бързо уточняване на намеренията.

3.2. Споделено въздушно пространство и разделяне при аварийни ситуации

U-space не премахва конфликта между пилотиран и безпилотен трафик, а го превръща в управляема информационна и процедурна задача. Полетните изпитвания на SAFEDRONE комбинират процедури за забранени за дронове зони, разделяне от пилотирани въздухоплавателни средства и etect-and-avoid технологии (Alarcón et al. 2020). Изпитването на аварийно кацане в близост до писта показва потенциалните опасности при един отказ, което може временно да разшири U-space зоната и да наложи ограничаване на пилотираните полети (Schwoch et al. 2023).

За държавните оператори това означава, че не е достатъчно да планират собствената мисия. Те трябва да предвидят ефекта от отказа върху летището и съседния трафик. Особено важни са процедурите за прекратяване, аварийно кацане, напускане на геозона и предаване на управлението към органи за ОВД или друг компетентен орган, според оперативната среда и обстановка.

3.3. Междусекторна координация

Държавните полети често пресичат компетентности: операторът е полиция или пожарна, въздушното пространство се управлява от гражданска авиация, а мисията може да засяга военни, гранични или здравни структури. Литературата за U-space подчертава, че системата е публично-частно взаимодействие и че развитието ѝ без технологична и индустриална координация е контрапродуктивно (Huttunen 2019). При държавна употреба това трябва да се разшири до постоянна координация между USSP, CIS, ANSP/ATC, командния център и органа, който е обявил спешността.

Практическите изпитвания също показват, че организацията на дейности от разстояние, преносът на данни към симулационната среда и уеднаквяването на различни летищни среди са отделни проблеми (Schwoch et al.

2023). Те са аналогични на трансгранични или междуведомствени операции, при които общата мисия трябва да се представя еднакво на всички участници.

IV. Аварийно управление и устойчивост

4.1. Спешният полет като изключение

Аварийното реагиране е най-трудният тест за U-space, защото нарушава предпоставката за предварително планиран и стабилен полет. Рамката за интеграция на аварийни UAS в германски U-space изрично определя това като нерешен проблем и предлага архитектура, която се имплементира и тества чрез случаи в Хамбург (Teomitzi et al. 2025). Това е по-силна основа от чисто концептуален анализ, но все още е рамка и тестова разработка, а не доказана национална оперативна услуга.

Една работеща схема трябва да отговори на пет въпроса: кой има право да активира аварийния режим; как системата удостоверява това право; как се изчислява временната зона на защита; как се уведомяват другите оператори и АТС; и как се връща въздушното пространство към нормален режим. Литературата подкрепя необходимостта от тези функции, но не предоставя единен валидиран модел за всички държави и мисии.

4.2. Откази на бордови и наземни системи

Безопасността в U-space зависи от нормалната работа на всички бордови датчици, наземни съоръжения за навигация, комуникации, наблюдение и обработка на информацията. Експерименталното изследване на метрики за безопасност разглежда възможни откази на GPS и инерциални системи с различна продължителност, скорост на БВС, интервали на обновяване, плътност на трафика и метеорологични условия. Така се определят прагове за риск и се оценяват ограниченията на механизмите при грешно поведение на навигационните системи (Asghari et al. 2026). Изводът следва да бъде методологичен – отказите трябва да се оценяват като комбинации от фактори, а не поотделно. Защото държавен полет над населено място може да има различен приемлив риск от тренировъчен полет над изолирана зона, където същият GPS отказ може да стане критичен при висока плътност на трафика и слаб информационен обмен.

4.3. Пренастройване на въздушното пространство

При аварийното кацане по време на инспекция на полосата полетът е извършен в експериментална среда с виртуален U-space обем, а отказът е

довел до временно разширяване на този обем и до действия на органите за ОВД спрямо пилотирания трафик (Schwoch et al. 2023). Този първичен тест показва, че аварийното управление е съвместна функция на БВС, U-space системата и УВД.

За изпълнение на държавни мисии има необходимост от разработване на предварителни резервни сценарии – загуба на връзка, невъзможност за кацане на предвиденото място, отказ на позиционирането, възникнало внезапно препятствие (неосъвременена навигационна информация) и промяна на приоритета. Ако тези сценарии са оставени само на пилота или оператора, цифровата система няма да може да осигури предвидимо поведение за останалите въздушни участници.

4.4. Устойчивост на автоматизацията

Автоматизацията спомага за намаляване натоварването на персонала при провеждане на много полети, но създава нови зависимости. Анализът на U-space като инфраструктура идентифицира три групи рискове: надеждност на инфраструктурата, преход от ориентирани към човека към ориентирани към автоматизацията системи и нередности в европейската регулаторна рамка (Nawaz 2025). За държавните органи това е особено важно, защото резервният режим може да трябва да запази мисията, а не просто да прекрати полета.

Следователно устойчивостта трябва да включва деградирали режими, локална автономност, резервни комуникации, ясни граници на автоматичното решение и човешка възможност за намеса. Наличните публикации подкрепят тези направления като проблеми на системния дизайн, но не доказват как трябва да бъдат конфигурирани за конкретна национална служба.

V. Заключение

U-space трябва да може да предложи надеждна архитектура за интегриране на държавни БВС, но задължително при отчитане на високата неопределеност при изпълнение на непланирани държавни полети. Решаващото предизвикателство е оперативната граница между стандартизирана гражданска услуга за управление на трафика и държавни мисии, които като правило са спешни, класифицирани, динамични или правно комплицирани. Най-защитимият път на внедряване е многопластовия. Планирането на редовни държавни полети чрез обичайните услуги за оторизация, геоинформация, информация за трафика и идентификация е добрия първо-

начален подход. Добавянето на следващ етап на особеностите при провеждане на държавни полети в авариен режим с установен приоритет, при ясни ефекти върху пилотирания трафик, бърза рекоординация на въздушното пространство и автоматизация на процесите изисква валидиране на цялата верига. Това ще се постигне чрез симулации, тестове в изолирана среда и при реални полети, които включват BVLOS, симулации на навигационни и комуникационни повреди, динамична реконфигурация на въздушното пространство и междуведомствено командване (най-добре от единен команден център). Данните от тестовете подкрепят тази посока, но остават по-верни за прототипи и контролирани демонстрации, отколкото за реални държавни полети. Следователно U-space трябва да се третира като оперативна система, чиято безопасност зависи от технологиите, процедурите, човешките функции, закона и институционалната координация заедно, а не като услуга, която може да бъде възприета само след инсталиране на цифров интерфейс за оторизация на полети.

БЕЛЕЖКИ

1. CORUS & SESAR, 2017. Exploratory research [project]. Concept of Operations for EuRopean UTM Systems – CORUS [online]. Available from: https://www.sesarju.eu/projects/corus.

2. В пълно съответствие с определението за държавен полет в чл. 3 на Международната конвенция за гражданското въздухоплаване.

3. МИНИСТЕРСКИ СЪВЕТ, 2026. Проект на Наредба за условията и реда за координация на полетите с държавни безпилотни въздухоплавателни средства за дейности, извършвани в обществен интерес. *Портал за обществени консултации.* [онлайн]. Достъпно на: https://www.strategy.bg/bg/public-consultations/12515.

4. Пак там.

REFERENCES

ALARCÓN, V. et al., 2020. Procedures for the Integration of Drones into the Airspace Based on U-Space Services. *Aerospace,* vol. 7, no. 9, p. 128. [online]. Available from: https://doi.org/10.3390/aerospace7090128.

ASGHARI, O.; IVAKI, N. & MADEIRA, H., 2026. Safety Assessment of UAV Operations in U-Space: A Comprehensive Study on Key Safety Metrics. *IEEE Transactions on Dependable and Secure Computing,* [online]. Available from:

https://doi.org/10.1109/TDSC.2026.3690902.

BARRADO, C. et al., 2020. U-Space Concept of Operations: A Key Enabler for Opening Airspace to Emerging Low-Altitude Operations. *Aerospace.* [online]. Available from: https://doi.org/10.3390/aerospace7030024.

FAS-MILLÁN, M.-Á.; PICK, A.; DEL RIO, D.; TINEO, A.P. & GARCIA, R., 2024. Implementing and testing a U-space system: lessons learnt. *Aerospace.* [online]. Available from: https://doi.org/10.1088/1742-6596/2716/1/012082.

GREBNER, T. & FAY, A., 2022. Concept for a U-Space Compliant UAS-Flight Authorization Service: The Flight Authorization and Activation Process. In: *International Conference on Unmanned Aircraft Systems.* [online]. Available from: https://doi.org/10.1109/icuas54217.2022.9836148.

GREBNER, T. et al., 2023. Analysis and Concretization of Fuzziness in the U-space Regulation. [online]. Available from: https://doi.org/10.25967/570073.

HUTTUNEN, M., 2019. The U-space Concept. *Air & Space Law.* [online]. Available from: https://doi.org/10.54648/aila2019005.

LIEB, J. & VOLKERT, A., 2020. Unmanned Aircraft Systems Traffic Management: A comparsion on the FAA UTM and the European CORUS ConOps based on U-space. In: *Symposium on Dependable Autonomic and Secure Computing.* [online]. Available from: https://doi.org/10.1109/DASC50938.2020.9256745.

MILEROVÁ, E.; KLECZATSKÝ, A. & KRAUS, J., 2022. Systemic Safety Evaluation of U-space Concept. *Transportation Research Procedia.* [online]. Available from: https://doi.org/10.1016/j.trpro.2022.11.011.

NAWAZ, S.A., 2025. Law and Infrastructure: Reliability, Automation Transition, and Irregularities of 'U-Space'. *Regulation & Governance.* [online]. Available from: https://doi.org/10.1111/rego.70046.

SCHWOCH, G.; LIEB, T.J. & LENZ, H., 2023. Flight Testing Drone Contingencies during Runway Inspection in U-space Shared Airspace. In: *International Conference on Networking and Services.* [online]. Available from: https://doi.org/10.1109/ICNS58246.2023.10124322.

SELVAM, P.K. & LIEB, T., J., 2024. How to Implement U-Space at an Airport – A General Overview of an Interaction and Synchronization Concept. In: *2024 AIAA DATC/IEEE 43rd Digital Avionics Systems Conference.* [online]. Available from: https://doi.org/10.1109/dasc62030.2024. 10749538.

SELVAM, P.K.; LIEB, T.J.; RUDOLPH, M.C. & TILGNER, L., 2025. Requirements and Implementation of a User Interface for the U-Space Collaborative Interface with Air Traffic Control. In: *2025 AIAA DATC/IEEE 44th Digital Avionics Systems Conference.* [online]. Available from: https://doi.org/10.1109/dasc66011.2025.11257266.

TANG, Y.; XU, Y. & İNALHAN, G., 2022. An Integrated Approach for On-Demand Dynamic Capacity Management Service in U-Space. *IEEE Transactions on Aerospace and Electronic Systems.* [online]. Available from: https://doi.org/10.1109/taes.2022.3159317.

TEOMITZI, H.E.; QUELAL, C.; MARTIN, H.; VICTOR, K. & TOPP, M., 2025. Integrating Emergency Response UAV Units into U-Spaces: A Solution Framework for German Airspaces. *Deutsche Gesellschaft für Luft- und Raumfahrt.* [online]. Available from: https://doi.org/10.25967/650283.

THE U-SPACE CHALLENGE TO PERFORM STATE FLIGHTS WITH UNMANNED AIRCRAFT

Abstract. The war in Ukraine has demonstrated the capabilities of a new type of weaponry: unmanned systems. In the air, these are employed for surveillance, reconnaissance, electronic warfare, and communications, as well as for conducting precision strikes. For peacetime operations, a regulatory framework known as „U-space“ has been established within the European Union to govern airspace. Flight operations by unmanned aircraft within U-space are envisioned as a specialized service characterized by a high degree of automation. The successful implementation of U-space relies on the assumption that established rules will be followed. Currently, however, insufficient consideration is given to the integration of state-operated unmanned aircraft flights into U-space. To ensure the safe conduct of unmanned aircraft operations within this environment, it is essential to develop capabilities to counter those who violate the rules. This study identifies the challenges that must be addressed to create the necessary conditions for the state to safely carry out its functions when conducting state-operated unmanned aircraft flights within U-space.

Keywords: state flight; state aircraft; unmanned aircraft; U-space; civil-military coordination

Dr. Hristo Stanev, Assist. Prof.
SCOPUS ID: 59247506500/
ORCID iD: 0000-0002-8161-8106
Department of Telecommunications
University of Telecommunications and Post
1, Akad. Stefan Mladenov St.
1700 Sofia, Bulgaria
E-mail: h.stanev@utp.bg

https://doi.org/10. 66334/annu26_shengeoriskukr

ШЕНГЕН КАТО ГЕОПОЛИТИЧЕСКИ РИСК-МУЛТИПЛИКАТОР: РАЗПРОСТРАНЕНИЕТО НА АДИТИВНО ПРОИЗВЕДЕНИ ОГНЕСТРЕЛНИ ОРЪЖИЯ В КОНТЕКСТА НА ВОЙНАТА В УКРАЙНА И СИГУРНОСТТА НА ИЗТОЧНИЯ ФЛАНГ НА ЕС/НАТО

Чавдар Георгиев[1], Димитър Рангелов[2,3]
[1]Академия на МВР
[2]Saxion University of Applied Sciences (Netherlands)
[3]The Police Academy of the Netherlands (Netherlands)

Абстракт. Статията разглежда разпространението на адитивно (3D) произведени огнестрелни оръжия като елемент от геополитическа динамика, свързана с членството на България и Румъния в Шенгенското пространство, войната в Украйна и средата за сигурност в Югоизточна Европа. Тезата е, че взаимодействието между регионалното наследство от незаконно оръжие, риска от диверсия на въоръжение след войната и технологичната трансформация на производството може да създава уязвимост, по-голяма от сбора на отделните рискове. Шенген не е причина за адитивното производство, но променя средата за откриване на трансграничното движение на оръжия. Анализът използва 31 публично верифицирани случая, интервюта с експерти и случая от Бургас (18.06.2026 г.).

Предложени са разграничени препоръки за действащите механизми и за нови законодателни мерки.

Ключови думи: геополитика на сигурността; Шенгенско пространство; източен фланг на НАТО; война в Украйна; адитивно производство на оръжие; регионална сигурност

I. Увод

Присъединяването на България и Румъния към Шенгенското пространство бе извършено по време на интензивната фаза на военния конфликт в Украйна и на фона на нарастващия потенциал за производство на оръжия чрез адитивни технологии. Двата фактора, при които се случи присъединяването, са със стратегическо значение за сигурността на региона и със съществен потенциал да я засегнат негативно. Българската литература разглежда контрола над оръжията най-често през призмата на тероризма и радикализацията (Petrova 2023, Ivanov 2024, Marinov 2022, Yordanov 2025), а политиките на Европейския съюз (ЕС) срещу трафика на оръжие – в по-общ план (Veshkov 2013). Затова трите процеса не бива да се разглеждат изолирано, а в тяхната свързаност, като една геополитическа конфигурация. Следва да се отчита и влиянието на други фактори, тъй като все още интензивно се използват и други способи за криминално въоръжаване. Процесите, които са предмет на изследването, обаче са определени заедно с респондентите като такива с изключително висок потенциал за въздействие върху сигурността.

На 18 юни 2026 г. Главна дирекция „Борба с организираната престъпност“ (ГДБОП) проведе в Бургас първата в България, по данни на дирекцията, оперативна реализация срещу производство на 3D-принтирани огнестрелни оръжия, при която бяха разкрити принтери, консумативи и файлове с чертежи за различни модели оръжия и боеприпаси[1, 2]. Случаят е необичаен, защото се развива при дефицит на актуално законодателство, криминализиращо такива дейности. От това възниква остро въпросът дали регионалната архитектура за сигурност е адекватна на феномен, който вече не изисква незаконните оръжия физически да бъдат пренасяни през граница, за да стигнат от производителя до потребителя. Целта на статията е да изведе и подчертае геополитическото значение на така констатираната трансформация на заплахите за източния фланг на ЕС и НАТО при три регионални условия: наследените от разпадането на Югославия арсенали,

войната в Украйна и пълноправното членство на България и Румъния в Шенген.

Емпиричната част е спомагателна. Търсенето е илюстративно, а не изчерпателно. Основният корпус включва 31 публично документирани случая на адитивно производство, а още 14 случая на конвенционален трафик са включени само за сравнение (общо 45 записа в Приложение 1). Използвани са и 18 полуструктурирани интервюта с експерти[3].

II. Геополитическа рамка: три пресичащи се процеса

2.1. Наследство от разпадането на Югославия

Балканските страни все още страдат от незарастнали рани на историята, защото народите на полуострова от векове са разделяни от интересите на силните на деня. Разпокъсаността и враждебността пораждат напрежение и агресия, а оттам и нужда от самоотбрана с цел възстановяване на доминацията на по-слабия над по-силния. Такава доминация осигурява оръжието.

Проф. Трпе Стояновски отбелязва, че проблемът с малките оръжия „особено се засили по време на разпадането на бивша Югославия, когато хората бяха въоръжавани по различни причини, както от държавни институции, така и от паравоенни групи“, и припомня 1997 г., когато складовете в Албания бяха отворени, а „по-голямата част от дългите оръжия […] все още циркулират в региона“[4]. Paul Ianovici от UNODC е категоричен, че бившият югославски регион остава един от основните доставчици на оръжие[5], а Fedir Sydoruk от GI-TOC допълва, че повечето незаконни оръжия на европейския пазар все още идват от постюгославските държави[6].

Законодателната неоднородност в региона не следва модела „строг център срещу либерална периферия“. В България газово-сигналните оръжия се придобиват при пълнолетие, гражданство на държава от ЕС и вписване на търговеца, без индивидуално разрешение[7]. Сърбия ги поставя в категория Ц, за която е нужно само уведомление в 8-дневен срок[8]. Властите в Северна Македония пък са възприели много рестриктивно законодателство за придобиване на законно оръжие, а това се е отразило на обществената осведоменост. В последните години убийствата с малки оръжия чувствително са намалели. Днес, ако някой държи незаконно малко оръжие, наказанието е минимум пет години затвор и то се прилага ефективно благодарение на добрата съвместна работа на прокуратурата и полицията. Все пак в обществото остава огромен брой незаконно притежавани оръжия:

оценките на Стояновски са между 250 000 и 400 000 за страната[9]. Румъния изисква уведомление и сертификат в 5-дневен срок, но не и разрешение[10], а Северна Македония забранява газовите оръжия и изисква разрешение за алармените[11]. Въпреки общата рамка на Директива (ЕС) 2021/555[12]. България има най-либералния режим сред тези съседи.

Регулаторна арбитража означава използване на разликите между националните правни режими: лице или мрежа избира юрисдикцията, в която дадено придобиване, притежание или производство е най-слабо регламентирано, и оттам снабдява пазари с по-строг режим. Несъответствието между режимите, а не строгостта на всеки от тях, създава тази възможност: изделие, свободно достъпно в България, може да бъде преправено и трафикирано към по-строги юрисдикции. Кристиян Тодоров от ГДБОП потвърждава този механизъм: всяка организирана престъпна група, която се занимава с трафик на оръжия, търси слабите места, а разликата в законодателството между държавите подпомага тази дейност[13]. Преработката на внесен газов пистолет в бойно оръжие носи на престъпните синдикати значителна печалба[14].

2.2. Войната в Украйна като фактор за диверсия на въоръжение

На изток от България, по оста Украйна – Русия – постсъветски блок, виждаме сюжет, сходен с балканския, но в много по-голям мащаб, защото там се сблъскват интересите на многомилионни държави. Религиозните различия допълнително засилват напрежението и създават почва за интензивна организирана престъпност. Колкото по-интензивна е тя, толкова по-голяма е нуждата от въоръжаване с цел доминация и самоотбрана.

Военните конфликти пораждат нужда от въоръжаване на собствените въоръжени сили и от защита на населението от военни действия, включително самоотбрана. Затова в момент на въоръжен конфликт снабдяването на конфликтните зони е предимно легално и според Тодоров не се наблюдава трафик на незаконни оръжия, който да ги захранва. Практиката обаче показва, че след затихване на подобни конфликти оръжието в ръцете на обществеността се монетизира, за да могат притежателите му да преживеят тежките времена на възстановяване, а на това съдействат и престъпни структури, търсещи бърза реализация. Подобен е примерът след войната в Югославия, когато на българския криминален пазар можеха да се намерят оръжия на сравнително ниски цени и лесно достъпни[15]. Sydoruk предупреждава, че „трябва да има план преди демобилизацията и разоръжаването, а не само реактивен отговор след това“[16]. Рискът е предмет и на

анализа на GI-TOC за въздействието на войната върху оръжейните пазари на Балканите[17].

Според Sydoruk към момента не се наблюдава организиран износ на оръжия от Украйна към съседните държави от престъпни групи. Има обаче потенциална опасност от такова инфилтриране, особено при нарастване на броя на оръжията вътре в страната. В района на Одеса има натрупани значителни количества, най-вече в Бесарабия, която граничи с Румъния. Може да се предположи, че оръжия от Украйна ще навлизат в България, но като транзитна дестинация, а крайни ще бъдат Чехия, Германия, Австрия и Франция. Част от оръжията, които населението съхранява сега, неизбежно ще бъдат трафикирани по няколко причини, сред които нуждата от пари и разрешаване на лични проблеми.[18]

2.3. Технологичната трансформация като ускорител

Адитивните технологии променят връзката между незаконното производство и физическото придвижване на оръжия. Докато при конвенционалния модел веригата включва придобиване и транспортиране на физически обекти, при адитивното – критичната информация е цифров файл, който се копира и споделя независимо от готовото изделие[19, 20].

В практиката за тези оръжия е възприето названието "ghost guns" („призрачни оръжия"), което обяснява затрудненото им проследяване до производителя или трафиканта. Традиционното документално проследяване е силно затруднено, тъй като оръжията нямат серийни номера, идентификационни белези или документи, свързани с придвижването им. Освен това вече не е необходимо между престъпните организации да се изгражда доверие като условие за сделка с незаконни оръжия: една престъпна организация може да придобие 3D принтер и да произведе оръжия за собствените си цели, без да рискува контакт с незаконни производители или трафиканти, които може да са служители под прикритие. Според изчисленията на Ianovici с по-малко от 2500 щатски долара може да се сглоби много добър комплекс за производство, включително 3D принтери с различни филаменти и CNC машини, а файловете могат да се намерят с малко проучване дори в отворения интернет, не само в даркнет[21].

Законодателните отговори са фрагментирани. Нов Южен Уелс криминализира неразрешеното боравене с цифрови чертежи (чл. 51F от Firearms Act 1996) след заложническата криза "Martin Place" (2014 г.), Сингапур въвежда подобна забрана през 2021 г. след атентата в Хале (2019 г.), а Северна Македония предлага закон, който за пръв път регулира чертежите,

в съответствие с проекта на Директива COM(2026)102, която предвижда наказания за създаването, придобиването, притежаването и споделянето на чертежи за 3D-печатани оръжия[22] (Georgiev 2026). В OSINT корпуса публично верифицируемите случаи растат от единични инциденти до няколко годишно (в периода 2021 – 2025 г.)

2.4. Механизъм на взаимодействие между факторите

Така идентифицираните три процеса, предмет на интереса на изследването, не следва да се разглеждат като самостоятелни, независими една от друга причини. В логиката на статията мултиплицирането на риска означава взаимодействие между няколко елемента на средата за сигурност, при което комбинираната уязвимост надхвърля сумата от отделните. Един от факторите влияе върху другите, като увеличава експлоатируемостта им.

Адитивното производство възникна извън системата на останалите фактори. То задоволява глада на пазара за евтини оръжия, придобивани с минимален риск, а неактуализираното законодателство го улеснява, тъй като при законодателен вакуум липсва страх от наказание.

Регулаторната арбитража (т. 2.1) би съществувала и без Шенген, но премахването на системния граничен контрол отстранява елемента, който частично компенсираше правната нееднородност. Потенциалната диверсия от Украйна (т. 2.2) увеличава значението на регионалния резервоар от оръжие, а адитивното производство (т. 2.3) засилва и двата механизма, като прави географския източник на оръжието все по-маловажен за контрола.

Понятието „риск-мултипликатор“ тук е аналитичен модел, а не количествено доказана причинно-следствена зависимост. Мултиплициране се приема при конкретен механизъм на усилване, наблюдаема уязвимост и данни, които отделят ефекта от самостоятелното действие на факторите. Наличните OSINT данни и интервюта позволяват обосновани хипотези, но не и измерване на допълнителния ефект.

III. Шенгенското разширяване и емпирична основа

3.1. Шенген през геополитическа призма

Отказът на държавите от систематични проверки по вътрешните сухопътни граници не означава, че контролът върху свободното движение на стоки отпада. Той следва да се разглежда като промяна в неговия характер: ефективността все повече зависи от придобиването, обработката и отработването чрез контролни действия на предварителна информация, анализ

на риска и последващи проверки. Това създава възможност за изместване на регионалния обхват на престъпните дейности, при което България и Румъния променят статута си на свързващо пространство между Западните Балкани и вътрешния пазар на ЕС. Наличният материал обаче не позволява да се установи, че действащите криминални мрежи вече са пренасочили дейността си вследствие на присъединяването към пространството без вътрешни гранични проверки. Ефектът на изместване остава работен сценарий. Кристиян Тодоров от ГДБОП допуска, че липсата на постоянен граничен контрол улеснява трафика и намалява броя на задържаните оръжия, но очаква компенсаторните мерки бързо да се уеднаквят и в дългосрочен план ефектът да бъде по-скоро положителен[23]. В корпуса случаите на конвенционален трафик се концентрират около установими логистични направления, а адитивното производство е географски по-разпръснато.

3.2. Методика на OSINT корпуса

OSINT анализът е допълващ инструмент. Периодът е март – август 2026 г., с разширение назад до ноември 2025 г. за случай с връзка към по-ранен трансграничен инцидент. Всички единадесет държави – членки на SELEC, са обходени последователно по единна методика, защото формират геополитическата екосистема на Балканите, чрез която регионът взаимодейства с Европа, Азия и Африка, в духа на понятието за регионален комплекс на сигурност (Buzan et al. 1998).

Периодът на търсене (март – август 2026 г.) е различен от периода на самите събития, които в Приложение 1 обхващат 2013 – 2026 г. Като случаи са разглеждани публично документирани събития с установима връзка с конкретна незаконна дейност, свързана с огнестрелно оръжие, а не публикации или цифрови файлове без данни за събитие. Всеки случай има идентификатор във формат ДЪРЖАВА-ГГГГММДД-##-КОД. Кодовете означават доказан трафик (S), иззето или произведено оръжие без доказан трансграничен елемент (W), организирана престъпна група (O) и използване на документи (D). При две или повече независими публикации за едно събитие се запазва един идентификатор, а останалите са допълващи източници. Всички 45 записа в Приложение 1 отговарят на този критерий. От тях 31 са на адитивно производство и образуват основния корпус, а 14 са на конвенционален трафик и не се включват в изчисленията за адитивното производство. Изключвани са дублирани публикации, общи твърдения без конкретно събитие и случаи без установима връзка с огнестрелно оръжие. „Верифициран“ тук означава индивидуално проследим до публичен източник, а не непременно потвърден от официален.

Методиката има собствени ограничения. Приемащата държава документира трансграничните инциденти по-подробно от изпращащата, а доказаният трафик е установен почти изцяло от митнически органи на входящи пунктове. Наблюдаваният ръст може да отразява развитие на явлението, по-добро откриване или по-широко отразяване.

IV. Случаят от Бургас като индикатор

На 18 юни 2026 г. ГДБОП проведе в Бургас специализирана операция, определена от дирекцията като първа по рода си в България. Според публикация на БНТ са иззети 3D принтери, полимерни суровини, сушилня и електронни устройства с чертежи, а материалите са предадени на Окръжна прокуратура – Бургас[24]. В публикацията на ГДБОП се виждат и части от 3D-принтирани пистолети[25].

Оперативната реализация на ГДБОП в Бургас не съставлява изолирано доказателство за наличие на транснационална мрежа или проява на ефект на изместване. Извеждането на подобни изводи изисква допълнителни доказателства от конкретното разследване, каквито в публично достъпните данни липсват. Случаят би могъл да насочи към извода, че технологично трансформираният модел на производство на незаконни огнестрелни оръжия е пряко относим за България, а не е само хипотеза в потенциално състояние. Характерът на оборудването насочва към предположение за създаване и експлоатиране на капацитет, надвишаващ единичен случай на производство на едно изделие за еднократно индивидуално ползване. Той не определя и мащаба, предназначението на изделията, нито връзките на задържания с местни или транснационални криминални структури.

V. Импликации и препоръки

Подробният анализ на уязвимостите след присъединяването и теоретичната рамка на ситуационната превенция са представени в Georgiev (2026), предложен за публикация. Изводът е: премахването на граничния контрол отстранява компетентния пазач (Cohen & Felson 1979), но не създава самата заплаха. Ген. Калин Георгиев предупреждава, че „ФБР въвежда софтуерни ограничения, но престъпният ум ги заобикаля“ и че идва производство без човешки оператор, задвижвано от изкуствен интелект[26].

Препоръките се разграничават по степен на готовност. За нуждите на международното сътрудничество между правоприлагащите органи меж-

дународните организации са създали и експлоатират канали за комуникация. Такива са криптираният комуникационен канал на SELEC, мрежата SIENA, използвана от Европол и нейните партньори, и обменът на информация с Europol Analysis Project Weapons & Explosives по Регламент (ЕС) 2016/794[27]. Добър пример за европейско сътрудничество е и участието на България в Европейската мултидисциплинарна платформа срещу заплахите от престъпност (EMPACT).

Необходимо е законодателно предефиниране на заплахата от Народното събрание. Предлага се законодателна инициатива за нова ал. 3 към чл. 242 Наказателния кодекс (НК), която да квалифицира контрабандата на оръжие като по-тежко наказуем състав (сега оръжията са в чл. 242, ал. 1, буква „г“). Необходимо е и криминализиране на притежанието на цифрови чертежи, когато е налице намерение за производство на огнестрелни оръжия. При следваща ревизия на административните процедури следва да се обсъди задължителна регистрация на 3D принтери, годни за печат на компоненти за оръжия. Необходими са и законодателни промени, които да осигурят достъп до трафични данни по чл. 159а НПК на компетентните държавни органи, които противодействат на контрабандата.[28]

Таблица 1. Връзка между констатации, уязвимости и мерки

Констатация	***Уязвимост***	***Мярка***	***Ограничение***
Различия в режимите за газово-сигнални оръжия (т. 2.1)	Регулаторна арбитража	Координация на режимите чрез SELEC и в рамките на директивата	Зависи от политическа воля в компетентността на българските институции
Адитивното производство е децентрализирано (т. 2.3, 2.4)	Контролът само върху физическото движение е недостатъчен	Криминализация на чертежите с доказано намерение и регистрация на принтери	Разграничаване от законна употреба и пропорционалност
Конвенционалният трафик следва установими логистични направления (т. 3.1)	Загуба на видимост при смяна на режима на проверките	По-интензивен анализ на риска и обмен през SELEC и Europol	Зависи от качеството и своевременността на информацията
Публичният корпус не измерва реалния мащаб (т. 3.2)	Решения при непълна картина	Систематизирано наблюдение и съпоставяне на данни	Публичните данни не заменят официалната статистика

Хармонизирането на режима за цифрови чертежи изисква приемане на директивата на ниво ЕС. Изравняването на режимите за придобиване и притежание на газово-сигнални оръжия зависи от политическа воля в компетентността на българските институции. По отношение на срока се предлагат краткосрочни мерки, а именно прилагане на действащия чл. 339 НК, съчетано с оперативно-издирвателна дейност, и средносрочни, а именно транспониране на COM(2026)102.

VI. Заключение

Статията изхожда от тезата, че Шенгенското разширяване, войната в Украйна и технологичната трансформация на незаконното производство на оръжие трябва да се анализират като взаимно свързана конфигурация. Идентифицирани са три механизма, които илюстрират тази конфигурация: регулаторната арбитража, като използване на разликите между националните режими за газово-сигнални оръжия за снабдяване на по-строги пазари; потенциалната диверсия (инфилтриране) на леко въоръжение след войната и децентрализацията на производството чрез засилване на използването на адитивни технологии. Всеки от тях е познат и документиран. Анализът очертава как могат взаимно да усилват въздействието си, така че комбинираната им уязвимост да надхвърля сумата от отделните рискове. Премахването на системния граничен контрол между държавите – членки на ЕС, и държавите по Шенгенското споразумение ограничава контролните възможности на държавите, които досега частично компенсираха останалите фактори.

Случаят от Бургас е проверим индикатор, че технологично трансформираният модел е релевантен за България, но не доказва транснационална мрежа. Корпусът от 31 случая подкрепя динамиката количествено, но измерва публично откриваемото, а не реалния обем на явлението. Изводите не претендират да установяват причинно-следствена зависимост, а следва да се разглеждат като обоснован риск-сценарий за самовъзпроизвеждане и превръщане на конкретна заплаха от потенциална в проявена в настоящето и в близкото бъдеще. Необходимо е в спешен порядък, но разумно и обосновано, въз основа на вече съществуващ опит, празнотите в законодателството да бъдат запълнени. След въвеждането на нова криминализация следва продължително да се проследява ефектът ѝ върху средата за сигурност и при необходимост да се коригира адекватно. Затова се предлага двуетапен законодателен подход: приемане на законодателство и мониторинг на въздействието.

Благодарности. Авторите благодарят на респондентите, цитирани с информирано съгласие, на проф. д-р Йордан Пенев и на катедра „Оперативно-издирвателна дейност“ във факултет „Полиция“ при Академията на Министерство на вътрешните работи.

Използване на изкуствен интелект. За структуриране, езикова редакция и форматиране е използван езиков модел (Claude, Anthropic). Съдържанието, анализът и изводите са на авторите, които носят отговорност за тях.

Приложение 1

СЛУЧАИ НА АДИТИВНО И КОНВЕНЦИОНАЛНО ПРОИЗВЕДЕНИ/ТРАФИКИРАНИ ОГНЕСТРЕЛНИ ОРЪЖИЯ В ЕВРОПА (2013 г. – 2026 г.)

Методологична бележка. Таблицата представя публично идентифицирани случаи и не е изчерпателен регистър. Посочването на източник не означава, че всички характеристики на събитието са потвърдени от него. Данните за конвенционални оръжия са включени само за сравнение и не са пряко съпоставими с данните за адитивно произведени оръжия. Редовете с източник “SEESAC 2025” или “SEESAC (Fig. …)” се позовават на доклада на SEESAC (2025); за тези случаи не е намерена отделна публично достъпна публикация, поради което детайлите са ограничени до тези в статията.

Event ID	*Тип*	*Държава*	*Дата*	*Кратко описание*	*Източник*
2013-UK-01	Ад.	Обединено кралство	2013	Първият документиран европейски случай – арест на лице, притежаващо 3D принтирано оръжие	The Conversation; 3DPrint.com
2017-UK-02	Ад.	Обединено кралство	2017 – 2019	Лондон – T. Muswere, първата присъда във Великобритания за производство на оръжие с 3D принтер	Gulf News/AFP: https://gulfnews.com/world/europe/uk-man-becomes-first-convicted-in-britain-of-making-3d-printer-gun-1.1560955476289

Event ID	*Тип*	*Държава*	*Дата*	*Кратко описание*	*Източник*
2019-DE-01	Ад.	Германия	09.2019	Хале – терористична атака срещу синагога; ролята на 3D-печатни компоненти в използваните оръжия е оспорвана	SEESAC 2025; ICSR (3D Printing Industry): https://3dprintingindustry.com/news/interview-with-the-icsr-a-3d-printed-gun-was-not-used-in-the-halle-terror-attack-163643/
2020-ES-01	Ад.	Испания	2020 – 2021	Работилница за 3D-принтирани оръжия (Испания)	SEESAC 2025
2020-UK-01	Ад.	Обединено кралство	12.2020	Есекс – FGC-9 и Cheetah-9 Hybrid SMG, планиран атентат	GNET
2020-RO-01	Ад.	Румъния	2020	Първи документиран случай в региона на ЮИЕ	SEESAC (Fig.32)
2021-UK-02	Ад.	Обединено кралство	05.2021	Кийли – тричленна крайнодясна клетка, PG22	ITV News, 14.05.2021: https://www.itv.com/news/calendar/2021-05-14/three-people-from-keighley-charged-with-right-wing-terrorism-offences
2021-ES-02	Ад.	Испания	2021	Баска провинция (Бермео) – арест за производство на оръжие с 3D принтер	Министерство на вътрешните работи на Испания: https://www.interior.gob.es/opencms/es/detalle/articulo/Detenido-por-fabricar-armas-con-una-impresora-3D-en-su-vivienda-en-Bermeo/
2021-ES-03	Ад.	Испания	2021 – 2022	А Коруня – производство на саморъчно оръжие с 3D принтер	SEESAC 2025

Event ID	*Тип*	*Държава*	*Дата*	*Кратко описание*	*Източник*
2021-NL-01	Ад.	Нидерландия	11.2021	Роон (Rhoon) – производител на 3D-принтирани оръжия	OM (Нидерландия), 04.10.2024: https://www.om.nl/actueel/nieuws/2024/10/04/om-eist-gevangenisstraf-voor-fabrikant-3d-wapens
2021-SE-01	Ад.	Швеция	11.2021	Фалшьопинг – бивш член на NRM, прекурсори	GNET
2021-NL-03	Ад.	Нидерландия	2021	Професионална работилница (Politie Nederland)	SEESAC (Fig.40)
2022-NL-02	Ад.	Нидерландия	02.2022	Схаувен-Дёйвеланд – FGC-9, нацистка символика	NL Times, 12.02.2022: https://nltimes.nl/2022/02/12/video-man-arrested-3d-printed-gun-ammunition-nazi-flags
2022-UK-N01	Ад.	С. Ирландия	04.2022	Белфаст — ÓNH, демонстрация с FGC-22	Irish News, 27.04.2022: https://www.irishnews.com/news/
2022-SK-01	Ад.	Словакия/ Чехия	05.2022	Разпространение на инструкции за 3D печат на оръжие	Infosecurity Magazine
2022-UK-04	Ад.	Обединено кралство	2022	NCA – ръст от 3 (2021) на 17 (2022) случая	3DPrint.com
2022-IS-01	Ад.	Исландия	09.2022	4-ма арестувани, планиран терористичен акт	Euronews, 23.09.2022: https://www.euronews.com/2022/09/23/four-arrested-as-iceland-rocked-by-first-terror-attack-plot
2022-UK-03	Ад.	Обединено кралство	10.2022	Северозападен Лондон – оръжеен арсенал	GI-TOC
2020-BE-01	Ад.	Белгия	~2020 – 22	Льовен – работилница за 3D оръжия	SEESAC (Fig.37)
2021-FR-01	Ад.	Франция	~2021	Марсилия	SEESAC (Fig.38)

Event ID	*Тип*	*Държава*	*Дата*	*Кратко описание*	*Източник*
2022-FI-01	Ад.	Финландия	~2022	Trojan Shield – 2 бр. FGC-9	SEESAC (Fig.34-35)
2022-SE-02	Ад.	Швеция	~2022	Митническо засичане на цеви от Китай	SEESAC (Fig.36)
2023-DE-02	Ад.	Германия→ Португалия	2023	J. Thome, екстрадиран от Португалия	CTC West Point
2023-FI-02	Ад.	Финландия	10.2023	Осъдени неонацисти	Euronews, 01.11.2023: https://www.euronews.com/2023/11/01/finnish-neo-nazis-convicted-in-race-war-terror-plot-using-3d-printed-guns
2023-UK-05	Ад.	Обединено кралство	12.2023	Разкрити терористични заговори	The Sun
2024-GR-01	Ад.	Гърция	02.2024	Самос – 4-ма арестувани	To Vima: https://tovima.com/society/samos-criminal-organization-made-guns-with-3d-printer-4-arrests
2024-FR-02	Ад.	Франция	2024	Мрежа за трафик на оръжие	EPRS 2025
2025-UK-06	Ад.	Обединено кралство	05.2025	3-ма осъдени, планиран атентат	EPRS 2025
2025-FI-03	Ад.	Финландия	2025	Крайнодясна клетка, 4 бр. 3D оръжия	EPRS 2025
2025-IE-01	Ад.	Ирландия	2025	3D пистолети, Garda Síochána	EPRS 2025
2026-BG-01	Ад.	България	18.06. 2026	Бургас – референтен казус	BNT News 2026; GDBOP 2026; материалите са предадени на Окръжна прокуратура – Бургас
C2020-EU-01	Конв.	ЕС (общо)	2020	Операция Bosphorus – 191 оръжия	EPRS 2022
C2020-NL-01	Конв.	Нидерландия/ Франция	07.2020	Десетки автоматични оръжия	EUR-Lex

Event ID	*Тип*	*Държава*	*Дата*	*Кратко описание*	*Източник*
C2020-ES-01	Конв.	Испания	2020	730 оръжия, 21 арестувани	EUR-Lex
C2020-SEE-01	Конв.	ЮИЕ (33 държави)	09.2020	166 арестувани, 51+ оръжия	Frontex; INTERPOL
C2021-BA-01	Конв.	Босна и Херцеговина	08.2021	Арсенал, трафик към Франция	GI-TOC
C2021-EU-02	Конв.	24 държави	12.2021	Op. Conversus – 1534 алармени пистолета	Europol
C2022-SEE-01	Конв.	ЮИЕ (28 държави)	10.2022	382 арестувани, 100+ оръжия	Frontex; OCCRP
C2023-EU-01	Конв.	31 държави	04.2023	22 арестувани, 1621 оръжия (129 огнестрелни + 1492 алармени/ сигнални), турски произход	Europol
C2023-NL-02	Конв.	Нидерландия/ Чехия/Словакия	03.2023	18 арестувани, 350 оръжия	Europol
C2024-RS-01	Конв.	Сърбия	01.2024	45 оръжия със заглушители	GI-TOC
C2024-XK-01	Конв.	Албания/ Косово	12.2024	Разбита група за трафик	Eurojust
C2024-PL-01	Конв.	Полша/Австрия	12.2024	Škorpion оръжия за наемни убийци	Europol
C2025-FR-01	Конв.	Франция/ Испания/ Словения/ Босна	04.2025	Op. Charon – 25 АК, 126 гранати	Europol
C2025-BE-01	Конв.	Белгия/Австрия	2025	74 оръжия, наколаборатория	Europol

БЕЛЕЖКИ

1. BNT NEWS, 2026. Producer of 3D-printed weapons arrested in specialised operation in Burgas, 19 June 2026 [online]. Available from: https://bntnews.bg/news/producer-of-3d-printed-weapons-arrested-in-specialised-operation-in-burgas-1399312news.html. [last viewed: 19 October 2026].

2. ГДБОП – Министерство на вътрешните работи, 2026. Публикация за оперативна реализация в Бургас. [Facebook, 19 June 2026] [онлайн]. Достъп-

но на: https://www.facebook.com/share/p/1Ds4uy89Ub/. [Последно видян: 20 октомври 2026].

3. Георгиев, Ч. Емпирично изследване: 18 полуструктурирани интервюта, юни 2026 г. Личен архив на автора. Цитираните респонденти са дали информирано съгласие.

4. Интервю с проф. Трпе Стояновски, Факултет по сигурност – Скопие, Университет „Св. Климент Охридски“; изследовател в GI-TOC; бивш заместник-министър на вътрешните работи на Северна Македония.

5. Интервю с Paul Ianovici, UNODC.

6. Интервю с Fedir Sydoruk, GI-TOC, Украйна.

7. Закон за оръжията, боеприпасите, взривните вещества и пиротехническите изделия. *Държавен вестник,* бр.73 от 17.09.2010 г., посл. изм. бр. 55 от 16.06.2026 г.

8. Закон о оружју и муницији на Република Сърбия, чл. 5, т. 14; чл. 8, ал. 1, т. 6; чл. 10, ал. 5; чл. 25.

9. Интервю с проф. Трпе Стояновски (вж. бел. 2). Цифрите са негова оценка.

10. Legea nr. 295/2004 privind regimul armelor și al munițiilor, чл. 2, ал. II, т. 3 и ал. III, т. 3; чл. 12, ал. 1; чл. 58, ал. 1; чл. 59, ал. 1.

11. Предлог на закон за оружјето на Република Северна Македония, чл. 3, т. 10 и 11; чл. 4, ал. 1, б. „А“, подт. 8 и б. „Б“, подт. 19; чл. 5, ал. 1.

12. EUROPEAN UNION, 2021. Directive (EU) 2021/555 of the European Parliament and of the Council of 24 March 2021 on control of the acquisition and possession of weapons.

13. Интервю с Кристиян Тодоров, експерт в ГДБОП.

14. По емпиричните данни от дисертационния труд на автора.

15. Интервю с Кристиян Тодоров, експерт в ГДБОП.

16. Интервю с Fedir Sydoruk, GI-TOC.

17. GLOBAL INITIATIVE AGAINST TRANSNATIONAL ORGANIZED CRIME, 2023. Weapons in the Balkans: The Impact of the War in Ukraine.

18. Интервю с Fedir Sydoruk, GI-TOC, Украйна.

19. SEESAC, 2025. 3D-Printed Firearms, State of Play, Challenges and Law Enforcement Approach. Belgrade: UNDP SEESAC.

20. GLOBAL INITIATIVE AGAINST TRANSNATIONAL ORGANIZED CRIME, 2025. Criminal Plasticity: The Growing Threat of 3D-Printed Weapons in South Eastern Europe. Risk Bulletin, no. 21.

21. Интервю с Paul Ianovici, UNODC. Цифрата е негово изчисление.

22. EURONEWS, 2026. Brussels seeks EU-wide jail sentences for firearms offences including 3D-printed weapons, 26 February 2026, updated 3 March 2026 [online]. Available from: https://www.euronews.com/my-europe/2026/02/26/brussels-seeks-eu-wide-jail-sentences-for-firearms-offences-including-3d-printed-weapons [last viewed: 20 October 2026].

23. Интервю с Кристиян Тодоров, експерт в ГДБОП.

24. BNT NEWS, 2026. Producer of 3D-printed weapons arrested in specialised operation in Burgas, 19 June 2026 [online]. Available from: https://bntnews.bg/news/producer-of-3d-printed-weapons-arrested-in-specialised-operation-in-burgas-1399312news.html. [last viewed: 19 October 2026].

25. ГДБОП – Министерство на вътрешните работи, 2026. Публикация за оперативна реализация в Бургас. [Facebook, 19 June 2026] [онлайн]. Достъпно на: https://www.facebook.com/share/p/1Ds4uy89Ub/. [Последно видян: 20 октомври 2026].

26. Интервю с ген. Калин Георгиев, бивш главен секретар на МВР.

27. EUROPEAN UNION, 2016. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol).

28. Интервю с гл. комисар Ивайло Иванов, бивш главен секретар на МВР.

REFERENCES

BUZAN, B.; WÆVER, O. & DE WILDE, J., 1998. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers.

COHEN, L. E. & FELSON, M., 1979. Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, vol. 44, no. 4, pp. 588 – 608. ISSN 1939-8271.

GEORGIEV, CH., 2026. From Code to Cartridge: The Rise of 3D-Printed Firearms and the Fragmented Global Legal Response. *Conference paper,* [9 – 11 September 2026]. Velingrad: Academy of the Ministry of Interior.

IVANOV, D., 2024. The Nuclear Family in Modern Terrorism. In: *15th International Scientific and Practical Conference "Environment. Technology. Resources",* vol. 4, pp. 121 – 124. Rezekne: Rezekne Academy of Technologies. ISSN 1691-5402.

MARINOV, P., 2022. Preventing Radicalism, Anarchism and Ultra Nationalism. In: YALÇINKAYA, H. (ed.), *Good Practices in Counter-terrorism*, vol. 2, pp. 147 – 163. Ankara: COE-DAT. ISBN 978-605-74376-1-7.

PETROVA, ST., 2023. *Myastoto na kontrola nad orazhiyata v konteksta na borbata s terorizma.* Veliko Tarnovo: Natsionalen voenen universitet „Vasil Levski", pp. 247 – 254. [in Bulgarian].

VESHKOV, S., 2013. *Politiki na ES za protivodeystvie na nezakonniya trafik na orazhie*, [Avtoreferat]. Sofia: Nov balgarski universitet. [in Bulgarian].

YORDANOV, S., 2025. Swarming Terrorist Attack as an Evolving Threat for the European Security. In: *16th International Scientific and Practical Conference "Environment. Technology. Resources"*, vol. 5, pp. 341 – 348. Rezekne. ISSN 1691-5402.

SCHENGEN AS A GEOPOLITICAL RISK-MULTIPLIER: THE PROLIFERATION OF ADDITIVELY MANUFACTURED FIREARMS IN THE CONTEXT OF THE WAR IN UKRAINE AND THE SECURITY OF NATO‘S EASTERN FLANK

Abstract. The article examines the spread of additively manufactured (3D-printed) firearms as part of a geopolitical dynamic linked to the Schengen membership of Bulgaria and Romania, the war in Ukraine and the security environment of Southeast Europe. The thesis is that the interaction between the regional legacy of illicit weapons, the risk of post-war arms diversion and the technological transformation of illicit production may create a vulnerability greater than the sum of the individual risks. Schengen does not cause additive manufacturing, but it changes the environment for detecting cross-border movement of weapons. The analysis draws on 31 publicly verified cases, expert interviews and the Burgas case of 18 June 2026. Separate recommendations are offered for existing mechanisms and for new legislative measures.

Keywords: security geopolitics; Schengen area; NATO‘s eastern flank; war in Ukraine; additive weapons manufacturing; regional security

Chavdar Georgiev, PhD Student
ORCID iD: 0009-0004-6950-3447
Department of Operational-Investigative Activity
Academy of the Ministry of Interior
Director of Operations, SELEC
Deputy Director of the Inspectorate Directorate
Ministry of Interior
1, Alexander Malinov Blvd.
1799 Sofia, Bulgaria
E-mail: ChGGeorgiev@mvr.bg

Dimitar Rangelov, Senior Researcher
ORCID iD: 0009-0005-8511-1555
Technologies for Criminal Investigations
Saxion University of Applied Sciences /
The Police Academy of the Netherlands
Enschede, The Netherlands
E-mail: d.g.rangelov@saxion.nl

https://doi.org/10. 66334/annu26_civicident

MILITARY HISTORY AS A POTENTIAL MECHANISM OF CIVIC IDENTITY FORMATION: PUBLIC PERCEPTIONS OF PATRIOTIC EDUCATION IN KAZAKHSTAN AND THE BULGARIAN EXPERIENCE

Yelvira Ibadullayeva
Abai Kazakh National Pedagogical University (Kazakhstan)

Abstract. The article looks at how people in Kazakhstan assess military history and military traditions as part of patriotic education and civic identity. The empirical material is a nationwide survey of 1247 respondents, administered in Kazakh and Russian language. Study of the military history of Kazakhstan and the Armed Forces was named by 40,7% of respondents among the most effective forms of patriotic education. The figure is almost the same as for the general history of Kazakhstan (40.6%). At the same time, 81.3% agreed that learning the history of the army and military traditions can help form civic identity among the young. The results are read through historical memory, civic socialization and patriotic education and are set against Bulgarian institutional practice of placing military history inside school programmes. The argument is modest. Military history may link memory, belonging, civic duty and ideas of national security, but only if teaching does more than list battles and dates.

Keywords: civic identity; military history; historical memory; patriotic education; civic responsibility; national secutiry

I. Introduction

History teaching is no longer treated only as a transfer of facts. It also shapes how people read a shared past, where they place themselves, and what they take a political community to be. Korostelina (2008) showed that historical narratives can form and reproduce social identities by fixing certain readings of the past and drawing the line around “us”. That Point matters in states where civic identity is still being assembled in a multilingual and multi-ethnic setting.

Kazakhstan is such a case. After independence the country had to build a civic community that could hold territorial belonging and common citizenship together with cultural difference. Seidikenova et al. (2020) describe citizenship there as an unfinished process, marked by the Soviet inheritance, post-1991 nation-building and globalization. Recent school-level work points in the same direction. Khlebnikov et al. (2025) found that civic and patriotic attitudes among secondary-school graduates vary with language and region and that schools remain a central site of civic socialization. Gerfanova et al. (2025), working with 488 adolescents, treat civic identity as a mix of cognitive, affective, behavioural and motivational parts. Civic values came out strong. Readiness to act did not always follow. The gap between recognition and action is one of the reasons this article does not collapse civic identity into pride or into a wish to serve in the army.

Patriotic education is one of the tools through which the state tries to join historical knowledge, civic values and a sense of duty. Tolen et al. (2014), drawing on survey of 1000 young people aged 14 – 29 in fourteen regions, already treated patriotic education and civic duty as linked parts of youth development. What remains thinner in that literature is the place of military history inside the same field.

Military history is not just another chapter of the national past. It deals with armed conflict, defence of territory, service, security institutions and the people who stood in those roles. Because of that, it can tie memory to present talk of civic responsibility. It doesn’t do so by itself. Much depends on how the stories are chosen, framed and joined to contemporary civic questions.

Work on historical memory supplies the middle term. Family stories, commemorations and school practice pass representations of the past to the next generation (Rozhkov et al.2021). In a digital setting the same process becomes less orderly. Young people meet many competing versions of the past at once (Rozhkov et al.2021). Knowledge of events and memory of those events aren’t the same thing. The second is about meaning and belonging.

Kazakhstan has given military-patriotic education a formal policy frame. The concept of Military-Patriotic Education of Youth until 2030, approved by Government Resolution No. 1039 of 24 November 2023[1], sets a long horizon for work that is meant to join patriotic values, civic duty and national security. The Rules approved by Resolution No. 597 of 24 August 2022[2] already defined institutional duties. Policy, however, doesn't tell us how citizens themselves rate military history among other educational forms. That is the empirical gap this paper fills.

The comparative thread is Bulgaria. Hranova (2011), reading more than eighty history and civic textbooks from the late nineteenth century onward, showed that history and civic education have long been written into each other in the Bulgarian school tradition. Today the Ministry of Education and Science and the Ministry of Defence run a national programme on the study and preservation of the traditions and history of the Bulgarian Army. The comparison is limited on purpose. There is no second survey. Bulgaria is used as an institutional case: how military history can be built into school practice through joint work of civilian education and defence bodies. The research question is therefore simple. To what extent to respondents in Kazakhstan see military history and military traditions as effective instruments of patriotic education and as a possible mechanism of civic identity formation? Three tasks follow. First, to identify which forms of patriotic education are judged most effective for civic responsibility and readiness to take part in state security. Second, to measure how far respondents link the study of military history and traditions with civic identity. Third, to read those findings against the Bulgarian institutional arrangement.

The article offers two things. It reports nationwide perception data on military history inside patriotic education. It also treats military history as a possible hinge between memory and civic identity, using the Bulgarian programme only as an illustration of how such a hinge can be institutionalised. The survey is cross-sectional. It cannot prove that studying military history produces civic identity. What it can show is a perceived association.

II. Theoretical framework

2.1. Civic identity

Civic identity is a sense of belonging to a political community and an acceptance of the rights, duties and values that go with membership. It is not the same as ethnicity or language. In a multi-ethnic state that distinction is practical, not decorative. Gerfanova et al. (2025) split the construct into cognitive, affective,

behavioural and motivational layers. Patriotism may feed civic identity, but the two should not be treated as one word. A person can feel attached to the country and still hesitate before military service. The link, if it exists, runs through duty, trust and ideas of security rather through enlistment alone.

Seidikenova et al. (2020) place Kazakhstan citizenship at the crossing of Soviet legacies, independent state-building and globalization. Assyltayeva et al. (2024) later examined the civic identity of young Kazakhstanis against the background of the Russian-Ukrainian conflict. Both studies warn against reducing belonging to a single cultural marker.

2.2. Historical memory and history education

Historical memory is the stock of socially carried pictures of the past. Schools, families, museums, ceremonies and, now, digital media keep it in circulation. Korostelina (2008) argued that history education supplies frames for "who we are?" and for which experiences count. Fadlallah and Janmaat (2024), writing on Lebanon, show how the selection of events can harden or soften group lines in a divided society. The civic effect of military history therefore depends less on the mere presence of battles in a textbook than on how those battles are discussed.

Smakhanova et al. (2025) trace the place of historical memory in Kazakhstani secondary education from 1991 to 2021 and find that it has shaped historical consciousness and patriotic attitudes. Satanov (2021) looks at the memory of the Great Patriotic War among school students. Military history is a narrower slice of the same field. It concentrates defence, service and security institutions. That concentration is why it can also become one-sided if teaching stays at the level of dates and commanders.

2.3. Patriotic education and military history

Patriotic education sits between history teaching and civic education. It aims at attachment to the country, respect for symbols and heritage, and a readiness to contribute to its protection. It is not identical with military preparation. Family talk, school history, volunteering, meetings with veterans, clubs, camps and digital projects all belong to the same loose set. The questionnaire used here listed that range on purpose, so that military history could be compared with alternatives rather than standing alone.

Ziambetov (2019) treats Russian military history as a resource for patriotic work with students. Muzykantov (2024) examines civic identity in military training centres. Both studies are institutionally narrower than a nationwide

public survey, but they justify the question this paper puts to a general sample: do citizens themselves think that army history and military traditions can feed civic identity?

Myrzakhmetova et al. (2024) review the normative base of civic education in Kazakhstan and list history teaching, youth programmes and related acts as parts of state policy. The 2022 Rules and the 2023 Concept give military-patriotic education its own legal shelf. Public perception is still a separate question.

2.4. The Bulgarian case and the analytical model

Petrova (2021) describes the remaking of Bulgarian citizenship education after 1989. The present national programme "Study and Preservation of the Traditions and History of the Bulgarian Army"[3] adds a concrete channel: school projects on the army's past and a national forum for students. The National Museum of Military History runs programmes that mix talks, visits and practical work and tie them to national memory[4]. The National Military University "Vasil Levski" publishes themes for secondary-school citizens that place patriotism and civic duties next to current security threats[5]. The model is useful because it treats military history as history, as memory work, as student research, as patriotic education and as a meeting point of education and defence.

The literatures on civic identity in Kazakhstan, on history and social identity, on memory, on patriotic education and on the Bulgarian school tradition rarely sit in one frame focused on military history. That is the gap. The working model is not a causal chain. It is a reading grid:

military history education → historical knowledge and memory → civic belonging → civic responsibility → perceived readiness to take part in national security.

The survey tests two pieces of that grid: whether military history is named as an effective form of patriotic education, and whether it is thought to help form civic identity. The Bulgarian material then shows one way of turning the same idea into school practice.

III. Methodology

3.1. Design and sample

The study uses a quantitative descriptive design. A nationwide online survey in Kazakhstan produced 1247 valid responses. Two language versions were offered. The Kazakh version collected 930 responses (74.6%), the Russian version 317 (25.4%). The questions were substantively equivalent. The survey

belongs to a wider project on civic identity and military policy. This paper uses the block on patriotic education, military history and military traditions.

In the Kazakh-language group about 69% of respondents were aged 18 – 34 and about 30.5% were aged 35–54. In the Russian-language group the shares were about 54.7% and 44.6%. The youth tilt fits the topic. It also means the sample shouldn't be read as an age-balanced portrait of the whole adult population. Recruitment wasn't framed as a strict probability sample pf the country.

3.2. Indicators

Question 19 asked: *Which forms of patriotic education, in your opinion, most effectively contribute to the formation of civic responsibility among young people and their readiness to participate in ensuring the security of the state?* Up to three options could be chosen. The list covered the history of Kazakhstan; the military history of Kazakhstan and the history of the Armed Forces; state symbols and the history of independent Kazakhstan; gamily education and transmission of historical memory; military-patriotic classes and clubs; the "Zhas Sarbaz" movement; the "Aibyn" camp; meetings with military personnel and with veterans; visits to units; military-sport competitions; student research projects on the army, service and security; classes on civic duties and national security; volunteering; social networks and digital projects; other; and "difficult to answer". Because up to three answers were allowed, percentages do not sum to 100.

Question 21 asked: *Do you think that studying the history of the army and military traditions can contribute to the formation of young people's civic identity?* The five options were: yes, to a significant extent; mostly yes; mostly no; no; difficult to answer. The two positive options are also reported as a combined share.

3.3. Analysis, comparison and limits

The analysis is descriptive. Language versions were pooled for the main figures and then checked separately to see whether the central pattern held in both groups. Bulgaria is not a second sample. It's an institutional case built from public programme documents and academic work.

Participation was voluntary. No personal identifiers are used here. The paper contains no classified military information. Several limits follow from the design. The data record perceptions, not measured educational outcomes. Question 21 doesn't measure civic identity itself. A person who already feels a strong civic attachment may simply value military history

more. Reverse causation is possible. The Bulgarian part is documentary, not statistical. Those limits set the level of claim: perceived association, not proven effect.

IV. Research results

4.1. Forms of patriotic education

Question 19 produced a tight cluster around history and memory. Study of the military history of Kazakhstan and the Armed Forces was chosen by 40.7% of respondents. Study of Kazakhstan's history was chosen by 40.6%. The two figures sit almost on top of each other. Family education and the transmission of historical memory came third (29.4%), followed by state symbols and the history of independent Kazakhstan (27.9%). The remaining options fell well below that band. Table 1 sets out the distribution.

Table 1. Forms of patriotic education judged most effective
(Question 19; up to three answers; N = 1247)

Form of patriotic education	*% of respondents*
Study of the military history of Kazakhstan and the history of the Armed Forces	40.7
Study of the history of Kazakhstan	40.6
Family education and transmission of historical memory	29.4
Study of state symbols and the history of independent Kazakhstan	27.9
"Aibyn" military-patriotic camp	13.1
Military-patriotic classes and clubs	12.4
"Zhas Sarbaz" movement	11.3
Student research projects on the army, military service and national security	9.9
Military-sport competitions and military-tactical games	9.7

Meetings with military personnel, visits to units, classes on civic duties and national security, meetings with veterans and digital educational projects each stayed under 10%. The split is clear. Knowledge and memory dominate. Direct contact with military institutions and personnel is chosen less often. That is not the same as rejection. It's a ranking of what respondents think works best for civic responsibility and readiness to take part in security.

4.2. Military history and civic identity

Question 21 is the direct test. In the Kazakh-language version 59.1% chose “to a significant extent” and 22.6% chose “mostly yes” (81.7% together). In the Russian-language version the shares were 52.1% and 28.1% (80.2% together). For the whole sample the combined positive answer is about 81.3%. About one in ten chose “difficult to answer”. Negative answers were fewer still. Table 2 summaries the two language groups.

Table 2. Perceived contribution of army history and military traditions to civic identity (Question 21)

Response	*Kazakh version*	*Russian version*	*Combined*
Yes, to a significant extent	59.1%	52.1%	57.3%
Mostly yes	22.6%	28.1%	24.0%
Combined positive answers	81.7%	80.2%	81.3%

Note. Combined percentages for the first two rows are weighted by the size of the language subsamples (Kazakh version n = 930; Russian version n = 317). The published text reported only the pooled positive share (81.3%).

The two questions don’t say the same thing. Four in ten pick military history as one of the most effective educational forms. Four in five accept that it can contribute to civic identity. A respondent doesn’t have to rank military history first in order to grant it an identity-forming role. That gap is theoretically useful. As a concrete practice, military history shares the top of the list with general national history. As a symbolic resource, it’s recognized more widely.

4.3. Memory and the Bulgarian parallel

Almost three in ten respondents named family education and the passing on of historical memory. Civic and patriotic work is not, in this picture, a school monopoly. The finding sits well with Rozhkov et al. (2021). A multi-level reading suggests itself: family and school memory work, knowledge of national and military history, a sense of belonging, then civic duty. The survey cannot prove the sequence. It does make the sequence worth testing later.

Student research projects on the army, service and security were chosen by 9.9%. The share is modest. It’s also the point at which the Bulgarian programme becomes relevant. That programme turns military history into school research and into a national student forum, rather than leaving it inside a convetional

history lesson[6]. The two countries aren't being scored against each other. The comparison only shows that a participatory route exists.

V. Discussion

Taken together, the two questions support a careful claim. Military history is seen as more than a subfield of school history. It's also tied, in public judgement, to patriotic education, civic duty and civic identity. The 40.7% and the 81.3% measure different things: relative effectiveness among many forms, and recognition of a possible identity link. Military history need not win the ranking in order to be widely accepted as an identity resource.

That reading fits a multidimensional view of civic identity (Gerfanova et al. 2025). Military history can work mainly on the cognitive and affective sides: it supplies a shared past and a story through which a person can place herself in relation to the state and earlier generations. Behavior doesn't follow automatically. The same caution applies to causality. People with a stronger civic attachment may simply be more willing to value army history. Compatibility is what the data show. Production of identity is not.

Smakhanova et al. (2025) already placed historical memory inside Kazakhstani school content. This paper narrows the lens to military history because that slice joins memory of defence, sovereignty, service and security. Family memory, chosen by nearly a third of the sample, reminds us that socialization is spread across homes, schools, museums and civil society. A programme that speaks only through the classroom will miss part of what respondents themselves treat as effective.

The wording of Question 19 tied patriotic education to "readiness to participate in ensuring the security of the state". Participation here is broader than military service. It can include civil defence, volunteering, public responsibility and resistance to disinformation. Civic responsibility is the middle term between belonging and security. That is also why the article stays inside the author's wider work on civic identity and military policy without claiming a direct line from identity to policy.

Institutional policy in Kazakhstan and public ranking of historical forms point in a similar direction. Convergence is not proof that policy created the attitudes. The arrow can run both ways. If the aim is civic responsibility rather than a stock of patriotic phrases, programmes will need room for sources, argument and a link between past wars and present citizenship. Wang (2008), on a different national case, showed how tightly history teaching can be bound to

patriotic campaigns. The present data don't license that reading for Kazakhstan. They do suggest that historical content already carries civic weight in public eyes.

The Bulgarian arrangement is helpful precisely because it moves students from reception to work with sources. Museum programmes at the National Museum of Military History join knowledge with practical tasks and with talk of identity[7]. Themes issued by the National Military University place patriotism and civic duties next to cybersecurity, disinformation and hybrid threats[8]. History then becomes a door into a wider security citizenship, in which the citizen is not only protected but also asked to keep social resilience. Copying the Bulgarian design would be a mistake. Using it as a reminder that military history can be taught as research, museum work and current security talk is not.

One tension remains. Respondents lean toward knowledge and memory. Volunteering, digital projects, meetings with personnel and student research sit lower. Gerfanova et al. (2025) already separated values from behavior. If military history is meant to feed responsibility, teaching will have to give students something to do with the past, not only something to remember.

VI. Conclusion

Among 1247 respondents in Kazakhstan, 40.7% named the study of military history and of the Armed Forces as on of the most effective forms of patriotic education, almost level with general national history (40.6%). A larger share, 81.3%, agreed that studying army history and military traditions can contribute to civic identity among the young. The positive reading held in both language versions (81.7% in Kazakh, 80.2% in Russian). Family memory and national symbols also ranked high. Direct military-institutional activities ranked lower.

The pattern supports a limited proposition. Military history may work as a mechanism of civic socialization when knowledge is turned into memory and then joined to belonging, duty and a part in the security of the political community. The survey doesn't show that this happens. It shows that many respondents think it can. The Bulgarian programme, museum work and university themes illustrate one institutional way giving students an active role in that process.

Further work should test whether views of military history line up with trust in the Armed Forces, attitudes to service, civic duty and readiness to take part in security. Longitudinal or experimental designs would be needed to speak of effect rather than perception. For Kazakhstan the practical hint is modest.

Military history belongs not only the history syllabus. It can sit inside civic education, provided the stories are opened to argument, to family memory and to forms of participation that go beyond the page.

Acknowledgements. The author thanks all respondents who took part in the nationwide survey conducted in Kazakhstan.

Ethics and consent. Participation was voluntary and anonymous, and electronic informed consent was obtained before completion of the survey. The study documentation supplied for manuscript preparation did not include an ethics committee name, approval number, or approval date. The author will provide the editorial office with the applicable institutional record or a documented determination that formal review was not required.

Generative artificial intelligence. OpenAI ChatGPT in Codex work mode was used for language, structural, bibliographic, and technical editorial support. No survey data were generated or altered by the tool. The author retains full responsibility for independently verifying the sources, calculations, interpretations, and declarations and for the scientific content of the submitted manuscript.

NOTES

1. GOVERNMENT OF THE REPUBLIC OF KAZAKHSTAN, 2023. On approval of the Concept of military-patriotic education of youth until 2030. *Resolution No. 1039 of 24 November 2023*. [online]. Available from: https://adilet.zan.kz/rus/docs/P2300001039.

2. GOVERNMENT OF THE REPUBLIC OF KAZAKHSTAN, 2022. On approval of the Rules for military-patriotic education of citizens. *Resolution No. 597 of 24 August 2022*. [online]. Available from: https://adilet.zan.kz/rus/docs/P2200000597.

3. MINISTRY OF EDUCATION AND SCIENCE AND MINISTRY OF DEFENCE OF THE REPUBLIC OF BULGARIA, 2025. *National Programme No. 21 "Study and Preservation of the Traditions and History of the Bulgarian Army"*. Sofia: Ministry of Education and Science. [online]. Available from: https://www.mon.bg/dokumentatsiya/programi-i-proekti/naczionalni-programi-2025/.

4. NATIONAL MUSEUM OF MILITARY HISTORY, BULGARIA, 2026. *Educational programmes.* Sofia: National Museum of Military History. [online]. Available from: https://militarymuseum.bg/en/visit/.

5. NATIONAL MILITARY UNIVERSITY "VASIL LEVSKI", 2026. *Topics for training of Bulgarian citizens in the two stages for acquiring secondary education for the academic year 2026/2027.* [online]. Available from: https://www.nvu.bg/bg/temi-za-obuchenie-na-blgarskite-grazhdani-v-dvata-etapa-za-pridobivane-na-sredno-obrazovanie.

6. MINISTRY OF EDUCATION AND SCIENCE AND MINISTRY OF DEFENCE OF THE REPUBLIC OF BULGARIA, 2025. *National Programme No. 21 "Study and Preservation of the Traditions and History of the Bulgarian Army".* Sofia: Ministry of Education and Science. [online]. Available from: https://www.mon.bg/dokumentatsiya/programi-i-proekti/naczionalni-programi-2025/.

7. NATIONAL MUSEUM OF MILITARY HISTORY, BULGARIA, 2026. *Educational programmes.* Sofia: National Museum of Military History. [online]. Available from: https://militarymuseum.bg/en/visit/.

8. NATIONAL MILITARY UNIVERSITY "VASIL LEVSKI", 2026. *Topics for training of Bulgarian citizens in the two stages for acquiring secondary education for the academic year 2026/2027.* [online]. Available from: https://www.nvu.bg/bg/temi-za-obuchenie-na-blgarskite-grazhdani-v-dvata-etapa-za-pridobivane-na-sredno-obrazovanie.

9. GOVERNMENT OF THE REPUBLIC OF KAZAKHSTAN, 2005. On Defence and Armed Forces of the Republic of Kazakhstan. *Law No. 29 of 7 January 2005.* [online]. Available from: https://adilet.zan.kz/rus/docs/Z050000029_.

10. GOVERNMENT OF THE REPUBLIC OF KAZAKHSTAN, 2012. On military service and status of military personnel. *Law No. 561-IV.* [online]. Available from: https://adilet.zan.kz/rus/docs/Z1200000561.

REFERENCES

ASSYLTAYEVA, E.; ISHMUKHAMEDOV, S.; MUKHAMBEDYAROVA, A.; TARMAN, B.; TOLEN, Z. & YUSSUPOVA, S., 2024. Civil identity of young Kazakhstanis in the context of the Russian-Ukrainian conflict. *Journal of Ethnic and Cultural Studies*, vol. 11, no. 2, pp. 81 – 104. [online]. Available from: https://doi.org/10.29333/ejecs/2052.

FADLALLAH, H. & JANMAAT, J.G., 2024. *History education and the construction of identities in divided societies: the case of Lebanon*, vol. 26, no. 1, pp. 65 – 85. National Identities. [online]. Available from: https://doi.org/10.1080/14608944.2023.2282479.

GERFANOVA, E.; RUDIK, Z. & NEMCHENKO, N., 2025. Exploring the multidimensional civic identity of adolescents in Kazakhstan. *Journal of Culture and Values in Education*, vol. 8, no. 3, pp. 284 – 316. [online]. Available from: https://doi.org/10.46303/jcve.2025.36.

HRANOVA, A., 2011. History education and civic education: The Bulgarian case. *Journal of Social Science Education,* vol. 10, no. 1, pp. 33 – 43. [online]. Available from: https://doi.org/10.4119/jsse-553.

KHLEBNIKOV, I.; MYRZAKHMETOVA.A.; SATANOV, A. & MATORINA, Y., 2025. The civic identity of graduates (11th grade students) of secondary schools at the current historical stage of Kazakhstan's development: the results of a quantitative study. Bulletin of the Karaganda University. History. *Philosophy Series*, vol. 30, no. 2, pp. 181 – 194. [online]. Available from: https://doi.org/10.31489/2025hph2/181-194.

KOROSTELINA, K.V., 2008. History education and social identity. *Identity: An International Journal of Theory and Research,* vol. 8, no. 1, pp. 25–45. [online]. Available from: https://doi.org/10.1080/15283480701787327.

MUZYKANTOV, A., 2024. Civil identity of students at a military training center: empirical research experience. *Tambov University Review, Series: Humanities,* vol. 29, no. 1, pp. 7 – 18. [online]. Available from: https://doi.org/10.20310/1810-0201-2024-29-1-7-18.

MYRZAKHMETOVA.A.; KHLEBNIKOV, I.; MOMOSHEVA, N. & OTE, D., 2024. The civic education of young people in the education system: A review of the normative and legal acts of the Republic of Kazakhstan. *Bulletin of the Karaganda University, History, Philosophy Series*, vol. 29, no. 4, pp. 114 – 123. [online]. Available from: https://doi.org/10.31489/2024hph4/114-123.

PETROVA, S., 2021. Bulgarian civic and citizenship education in transition. In: MALAK-MINKIEWICZ, B. & TORNEY-PURTA, J., eds. *Influences of the IEA Civic and Citizenship Education Studies,* pp. 13 – 23. Cham: Springer. [online]. Available from: https://doi.org/10.1007/978-3-030-71102-3_2.

ROZHKOV, A.; RUNAEV, T.; STUDENIKINA, E. & DONTSOVA, M., 2021. Historical memory as young people's civic identity formation resource in digitalization context. *European Proceedings of Social and Behavioural Sciences,* vol. 120, pp. 753 – 760. [online]. Available from: https://doi.org/10.15405/epsbs.2021.12.03.100.

SATANOV, A., 2021. On the formation of historical memory of the Great Patriotic War among students of secondary schools of Kazakhstan. Bulletin of the Karaganda University. History. *Philosophy Series*, vol. 26, no. 1, pp. 29 – 35. [online]. Available from: https://doi.org/10.31489/2021hph1/29-35.

SEIDIKENOVA, A.; AKKARI, A. & BAKITOV, A., 2020. The construction of citizenship in Kazakhstan between the Soviet era and globalization. In: AKKARI, A. & MALEQ, K., eds. *Global Citizenship Education: Critical and International Perspectives*, pp. 57 – 69. Cham: Springer. [online]. Available from: https://doi.org/10.1007/978-3-030-44617-8_5.

SMAKHANOVA, Z.; ORAZAYEVA, Z.; KALIBAYEVA, A. & SHNANOV, O., 2025. Analysis of the influence of historical memory on the content of secondary education in Kazakhstan (1991–2021). *Bulletin of the Karaganda University, History, Philosophy Series*, vol. 30, no. 2, pp. 152 – 161. [online]. Available from: https://doi.org/10.31489/2025hph2/152-161.

TOLEN, Z.; TULENOVA, S.; ASSYLTAEVA, E. & AITYMBETOV, N., 2014. Formation of civil and patriotic education of youth in Kazakhstan. *Procedia – Social and Behavioral Sciences,* vol. 116, pp. 4859 – 4863. [online]. Available from: https://doi.org/10.1016/j.sbspro.2014.01.1038.

WANG, Z., 2008. National humiliation, history education, and the politics of historical memory: Patriotic Education Campaign in China. *International Studies Quarterly*, vol. 52, no. 4, pp. 783 – 806. [online]. Available from: https://doi.org/10.1111/j.1468-2478.2008.00526.x.

ZIAMBETOV, V., 2019. Patriotic education of students by studying the bases of the Russian military history. *Business, Education, Law*, vol. 4, no. 49, pp. 410 – 414. [online]. Available from: https://doi.org/10.25683/VOLBI.2019.49.412.

Yelvira Ibadullayeva, PhD Student
ORCID iD: 0009-0008-4563-1726
Department of Social Science
Faculty of History and Law
Abai Kazakh National Pedagogical University
13, Dostyk Avenue
050010 Almaty, Kazakhstan
E-mail: yelvira.1996@gmail.com