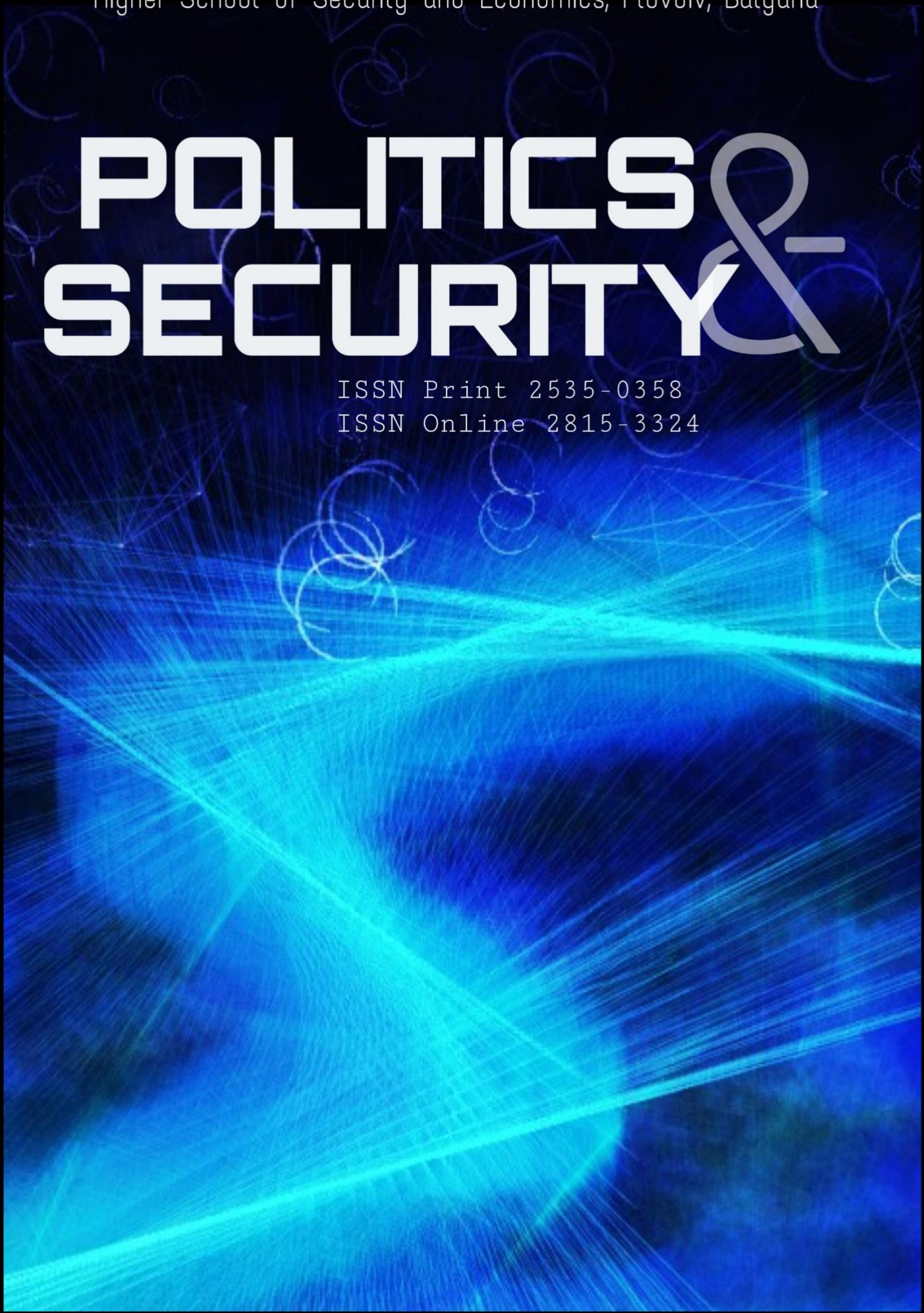
Higher School of Security and Economics, Plovdiv, Bulgaria

# POLITICS & SECURITY

ISSN Print 2535-0358
ISSN Online 2815-3324



# EDITORIAL BOARD

POLITICS & SECURITY
ISSN 2815-3324 Online, ISSN 2535-0358 Print

# FOREWORD

Vol. 16 No. 2 (2026)

**Dear Readers, Colleagues, and Partners,**

We are pleased to present Volume 16, Number 2 (2026) of Politics & Security, the peer-reviewed, open-access journal of the Higher School of Security and Economics in Plovdiv. This issue appears at a moment when the very idea of security is being contested and reshaped at once across several dimensions — conceptual, technological, informational, and geopolitical. The dangers that state and societies now confront rarely announce themselves as conventional military threats; they arrive as hybrid campaigns, algorithmic systems, disrupted supply chains, and contests over information and perception. The eight studies gathered in this volume respond to that complexity with analytical rigour and interdisciplinary breadth, moving deliberately from the foundations of security theory to its application in intelligence, information, foreign policy, and the human dimensions of security.

The volume opens with the study by Jan Jakimiec, which sets the conceptual frame for the issue. Clarifying the scope of external security, and distinguishing the internal from the external and the national from the international, the article maps the transformation of the threat environment from predominantly military dangers toward hybrid, informational, and societal ones, and argues that institutional capacity and an informed public together serve as a safeguard against the threats of our time.

Vasil Stankov turns from concepts to capability, examining intelligence superiority at the operational and tactical levels. Drawing on the experience of the high-intensity war in Ukraine, the article shows how timely, accurate, and well-integrated intelligence acts as a decisive force amplifier, and how the side that more effectively converts information into understanding gains an advantage that material strength alone cannot secure.

The governance of emerging technology is the subject of the third contribution, on artificial intelligence in intelligence and security services. Comparing the regulatory approaches of the European Union, the United States, the United Kingdom, and Israel, the article advances an original Security–Oversight Balance framework for reconciling operational effectiveness with democratic accountability, and confronts the risks of algorithmic bias, opacity, and the erosion of human responsibility for consequential decisions.

Nelly Bencheva examines parliamentary oversight of intelligence at a time of intensifying information sharing among European Union Member States. Using the case of Bulgaria, and attentive to the constraints of the third-party rule, the article demonstrates how deeper cross-border cooperation reshapes the demands placed on democratic control, and why oversight institutions must evolve if accountability is to keep pace with capability.

Kateryna Tiazhkorob addresses the informational dimension of contemporary conflict, analysing strategic communications in the armed forces as an integrated system for planning and coordinating communicative activity. Situating the discussion within current NATO doctrine and the experience of hybrid warfare, the article identifies the principal obstacles to building such a system and proposes concrete directions for its development and institutionalisation.

Vasil Georgiev assesses the cohesion of European Union foreign policy after 24 February 2022. The article traces how the Union has sought to preserve unity under the pressure of the war against Ukraine,

weighing the tension between national vetoes and collective action, and considering how a shifting transatlantic relationship bears on the prospects for European strategic autonomy and defence.

Dawid Jakimiec traces the evolution and contemporary challenges of Japan's security and defence policy. From the long isolation of the Tokugawa period, through post-war reconstruction and the pacifist commitment of Article 9, to the alliance with the United States and the pressures of a contested Indo-Pacific, the article examines how Japan balances dependence on its principal ally against its aspirations to regional leadership amid unresolved territorial disputes.

The volume concludes with the study by Mihail Mihaylov and Valentina Nikolova-Alexieva on food security, which broadens the analytical lens from the state to the human and economic dimensions of security. Reviewing the role of international institutions, the pillars of food security, and the deepening global food crisis, the article situates food security — including its European and Bulgarian aspects — firmly within the architecture of contemporary security studies.

Taken together, these contributions articulate a common thesis: security in 2026 can no longer be adequately theorised or governed through narrowly military or territorially bounded frameworks. From the conceptual foundations of security, through the gathering and democratic control of intelligence, the conduct of information and foreign policy, and the widening of security to its human dimensions, the issue underscores the need for multi-level conceptual tools, resilient institutional architectures, and sustained collaboration between scholars and practitioners across disciplines and borders.

We extend our sincere gratitude to the authors for their scholarly contributions, to the members of the Editorial Board and our reviewers for their diligence and care, and to our readers for their continued engagement with the journal. We warmly invite the submission of original research to Politics & Security at editor@politics-security.net, in the hope that the studies collected here will both inform and provoke further inquiry.

Sincerely,

The Editorial Board

Politics & Security

**POLITICS & SECURITY**
ISSN 2815-3324 Online, ISSN 2535-0358 Print

# CONTENTS

Jakimiec, J. (2026). Contemporary challenges and threats to the state's external security. Politics & Security, 16(2), 6–11. https://doi.org/10.54658/ps.28153324.2026.16.2.pp.6-11

# CONTEMPORARY CHALLENGES AND THREATS TO THE STATE'S EXTERNAL SECURITY

Jan Jakimiec
Lublin Academy of Economics and Management
Lublin, Poland
https://orcid.org/0000-0002-7926-5786
janjaki5959@gmail.com

***Abstract.*** *Security is one of the most fundamental values and a precondition for the stable development of individuals, societies, and states. This article examines the catalog of contemporary threats to the external security of the state and clarifies the scope and objectives of security as an analytical category. It distinguishes between internal and external, national and international security, and reviews the principal scholarly approaches to defining national security, drawing on the Polish and international literature. Particular attention is devoted to the institutional dimension of security – the role of state bodies, local government, and non-governmental actors acting within a single, coherent national security system – and to the transformation of the threat environment from predominantly military threats toward hybrid, informational, cyber, financial, and social ones. The study argues that, alongside institutional capacity, security education and public awareness function as a "safety valve" that mitigates the effects of contemporary threats, and that no state can sustain lasting security without international cooperation.*

**Keywords:** external security; internal security; national security; international security; security threats; hybrid threats; security education.

## 1. INTRODUCTION

This article analyzes the catalog of contemporary threats to state security. Considerable attention is paid to the scope and objectives of security, as well as the actions of entities responsible for ensuring the desired level of security, both for the state itself and for various aspects of society's functioning. Furthermore, the importance of an adequate level of security is emphasized, not only for the proper functioning of the state and its institutions, but also for society as a whole. Security has long been perceived as a fundamental existential foundation and one of the most cherished values, both in the social and individual dimensions. Ensuring an acceptable level of state security is an indispensable condition for the harmonious and effective development of society, individuals, individual institutions, and the efficient organization of the entire state. The subject of security is analyzed broadly, and the desire to understand and study it is an extremely complex and multifaceted task. Therefore, attempts to comprehensively address this fundamental, existential phenomenon may prove problematic.

## 2. CONDITIONS OF THE STATE'S EXTERNAL SECURITY

Understanding the specific nature of security as a key value and a foundation for creating a catalog of essential human values, as well as a condition for state development, provides the basis for a deeper analysis of the scope and fundamental goals of security. Looking through the lens of its scope and goals, security is divided into internal and external security, national and international. External security can be understood as the absence of threats to the state from other entities. In terms of internal security, it

ISSN 2815-3324 Online, ISSN 2535-0358 Print

constitutes its internal stability (Berent, 1988, p. 112). This means striving to ensure state security by creating the best possible internal conditions for the development of important elements of the system, but also by eliminating potential external threats by shaping a favorable external environment that will facilitate the harmonious development of the state (Dobrosielski, 1973, p. 14). Z. Nowakowski believes that internal security is a type of state security that eliminates all threats and protects both the state itself and its citizens from them. This type of security is directly focused on building a stable and harmonious functioning of the state, while simultaneously protecting the interests of individuals and society. Building such a state is possible through effectively implemented internal state policy. Internal security primarily encompasses securing vital interests against threats resulting from the actions of organizations, institutions, and individuals operating within the state or on its territory. (Nowakowski, 2009, p. 51).

Internal security, therefore, primarily refers to the effectiveness of state and institutional actions, whose primary task is to safeguard the national interest. Initiatives undertaken by the state should encompass a comprehensive catalog of possible threats resulting from specific activities, thus posing a threat to internal security. External security, on the other hand, is a type of security whose primary goal is to secure national interests, assets, values, and, above all, quality of life free from threats originating outside the state's borders. We can distinguish the following types of threats:

- military threats, i.e. threats related to illegal trade or other illegal acts;

but also:

- espionage;
- the penetration of foreign cultural and moral patterns;
- the propagation of hate speech and the dissemination of fake news internationally.

The foundation for effective external security management can be established through recognized priorities, recognized principles of international collective security, and a sound, balanced, and effective foreign policy in its economic, social, political, and military dimensions. It should be focused on ensuring the preservation of vital national interests in the international arena. Here, the state plays a crucial role in assessing and defining the most important national interests, as well as in establishing international relations to safeguard them.

W. Kitler believes that there is considerable latitude in understanding and defining the concept of national security. This means that the concept encompasses too broadly a wide range of issues. In his opinion, such an approach is too imprecise and doomed to failure. Virtually any problem relating to any threat to individuals, society, or institutions falls within the scope of national security (Wejkszner & Wojciechowski, 2019, pp. 10–13). It follows that Kitler, similarly to Nowakowski, considers national security to encompass those elements that condition the undisturbed existence and development of the nation. Therefore, we can assume that these are values that both individuals and groups of people not only recognize as common but also pursue together. They are important for the state as a political institution, even in the presence of certain divergences in individual interests. Furthermore, W. Kitler also draws attention to another, no less important, issue: historical experience demonstrating a certain evolutionary relationship between the state and security. This interdependence demonstrates a process in which security encompasses many values that are characteristic not only of individuals but also of social groups, previously not included in the classically interpreted concept of state security.

For many years, researchers have presented various approaches to identifying essential values that should be protected by the state. The dominant view in the realist approach was that the state constructs a certain catalog of values, in which the national interest was embodied in specific postulates (Zięba, 1997, p. 9).

The list is constantly changing and serves as a barometer of the current political situation, depending on emerging threats and concerns. The two most important values are territorial integrity and political independence (Klafkowski, 1985, p. 37).

When analyzing issues related to national security, it is important to consider significant threats to the state and society, both political and military. This approach was presented in the mid-20th century in Paris in the Dictionnaire Diplomatique, which interpreted the concept of sécurité as "a set of circumstances that prevents a state from becoming the target of an attack. Generally, the idea is to ensure that any attack against the state is ineffective." This definition of national security clearly demonstrates that potential threats originate externally, and the fundamental goal determining the actions taken by a state in a situation of direct international conflict is the survival of the nation and its organizational structure. A paradigm shifts in the perception of the role and importance of national security and its "demilitarization" began immediately after the end of World War II. The most important issue at that time was stable and dynamic development and the pursuit of improved living conditions for citizens. However, the rapid socio-political, economic, and military transformations, particularly in the context of the development of weapons of mass destruction, did not eliminate the military element from the security sphere. An attempt was made to re-examine threats. One of the researchers who advocated balancing the protection of national interests with the interests of individuals (citizens of smaller communities). During the period of socio-political transformation in Poland after 1989, the concept of national security increasingly focused on improving the quality of life, ensuring development, and ensuring prosperity.

Analyzing various approaches and determinants of national security, we conclude that the institutional dimension of the state plays a fundamental role in ensuring the protection of its citizens' lives, health, and property at all times. Society has a constitutional right to this, guaranteeing universal protection against threats resulting from natural and industrial disasters, natural disasters, and military threats. Actions to ensure national security are the responsibility of all bodies, not only the central government, but also local governments, as well as non-governmental institutions that closely cooperate with governmental and local government entities. These institutions are responsible for fulfilling and implementing constitutional guarantees in times of peace and war. Citizen assistance and involvement, depending on the values established in a given state, become a moral and natural obligation. Recognizing the potential for various threats arising from a dynamically evolving security environment, specialized institutions are established to ensure security at the state level, including forces responsible for taking specific responses and actions depending on the type of threat. In order to ensure the expected level of security, all these entities must function within a single, coherent and continuously operating system, both in peacetime and in times of threats, including armed aggression (Siuda & Zaczek-Zaczyński, 1999, p. 33). Ensuring security at the state level involves a well-functioning security system. Therefore, the state's national security system is composed of all bodies and institutions responsible for security, belonging to the legislative, executive, judicial, and local authorities (Korzeniowski, 2017).

Currently, security is broadly understood as a process influenced by factors that determine specific areas of life and functioning of individuals, as well as state institutions and authorities. Security is characterized by significant fluctuations, variability, and dynamics. This understanding of the concept of security reflects the proper functioning and appropriate actions of entities responsible for its level. Maintaining an acceptable level of national security is the result of constant monitoring and analysis of the catalog of threats characterizing the contemporary international environment. To achieve this, it is also necessary to systematically review the nature of mutual international relations. Entities responsible for ensuring and maintaining security create guidelines for specific policies and should also define the main objectives and scope of security within its individual types, building a catalog of specific guidelines that take into account key components essential for defining external, internal, national, and international security. Delineating the scope of national security is an important guarantee of defining and maintaining the raison d'état and guaranteeing the state's position in the international arena. Defining goals is key to conducting a proper analysis of individual security types. Each researcher analyzing a selected type of security should generate a specific list of needs/goals in a given area. Ensuring and maintaining the state of security expected and accepted by society at the state level, and thus the smooth functioning of individual units, refers to the effective operation of the state's security system and its individual security subsystems. Institutions operating within each subsystem should be assigned specific competencies in the National Security Strategy to achieve the list of security goals.

ISSN 2815-3324 Online, ISSN 2535-0358 Print

The volatility of the security environment means that the effective operation of all elements of the Polish security system is only possible through constructive cooperation. This is exemplified by the activities of the Government Security Centre, which, in the face of a crisis, implements an action plan involving individual entities from various subsystems of the national security system. Their effective cooperation, competences, and skills are crucial for neutralizing not only crisis situations but also other threats to the security of the state and society. A fundamental task in an efficiently functioning security system seems to be the continuous acquisition and monitoring of knowledge about potential threats at the state level, and their neutralization or mitigation. All entities operating within these subsystems should also be responsible for conducting extensive educational, informational, and preventive activities at the societal level. The possession of basic security knowledge by the majority of society, as well as the awareness of the possibility of practical application of this knowledge in the face of a threat, constitutes a "safety valve" that can significantly mitigate the negative effects of existing threats. Security plays an important role in international relations, constituting their foundation. Its fundamental goal is to build institutional structures and mechanisms that maintain security, peace, and stability at the desired level, thus creating conditions for development in all dimensions. No state is capable of building and maintaining lasting peace, order, and harmony in international relations on its own, without cooperation with others (Cziomer, 2010, p. 7).

Building lasting peace, order, and security today must take into account the diverse needs and goals of countries building international alliances. In today's environment, threats are growing dynamically and systematically, completely changing the nature of challenges and leading to numerous misunderstandings, dismantling, and damaging relationships between states. However, from a different perspective, there is synergy and the combining of joint efforts and actions to build and conclude agreements, arrangements, various alliances, strengthen ties, mutual assistance, and solidarity between individual countries. In the area of security, a key issue is recognition, that is, identifying the constantly evolving catalog of threats, not only in the military dimension but also in non-military or hybrid ones. Systematic analysis and analysis of the sources and factors influencing the growth of threats in the modern world are essential. Constantly examining the security environment and its types, across all dimensions, is the foundation for effectively developing concepts for countering threats and taking action to eliminate their sources and causes. Analyses based on historical sources and research into security conditions offer numerous opportunities to assess the effectiveness of methods, forms, and tools used by state bodies and institutions in the past in the fight to maintain the level of security expected by society. The fundamental goal of security efforts should be to outline and precisely define a global approach to security. Such a concept will enable us to understand the causes and effects, but also to determine the nature and types of threats, and thus the difficulties and scale of the challenges to be addressed. Conducting thorough analyses will allow us to formulate certain tenets and regularities regarding the dynamic changes taking place in the security environment, both in the context of individual states' security strategies and in broader, international, and global perspectives. This approach to understanding and acting creates conditions for a responsible approach to security issues and for more effective implementation of security-related tasks in the constantly evolving field of international relations (Lasoń, 2010, p. 9).

Since the dawn of our civilization, security issues have been considered one of the most important foundations for the peaceful coexistence of nations, states, and societies. Protecting security has meant preserving the highest and most essential values for the survival and survival of humanity. Maintaining security at an appropriate level, accepted by society, constitutes the fundamental framework for the functioning of a given state. The dynamically evolving catalog of contemporary threats in the security environment also changes the perspectives and perceptions of the conditions influencing the sense of security or its insecurity. Therefore, it is possible and justified to classify various types of security on several levels and dimensions. The substantive division of security reflects its subjective and semantic content in research and cognitive-empirical concepts. The current division widely accepted by researchers in security sciences is more an expression of a certain pragmatism and an attempt at systematization than an attempt to encompass and create a strict and comprehensive catalog that fully encompasses the subject of security. Political, social, economic, ecological, health, and financial security are merely a preliminary,

ordering classification, not a complete set. Moreover, considering the contemporary timeframe, public discourse often employs concepts related to security, such as the protection of national identity or the protection of fundamental human and civil rights and freedoms. Research is underway to develop a comprehensive, horizontal theory built on a model based on dynamically changing conditions on a global scale. The foundation of this research is the analysis and identification of threats and emerging challenges, as well as the development of a strategy and systemic approach that will create opportunities for effective security management across various scales and dimensions (Ciekanowski, 2010, p. 28).

## 3. CONCLUSION

The dynamic changes in the security environment, resulting from globalization and affecting every aspect of our lives and the functioning of individuals and states, are contributing to a growing number of new threats. These threats have evolved significantly in recent years, from military threats to hybrid threats. Not only individuals and society as a whole, but also state institutions are increasingly faced with threats in the areas of health, cyberspace, finance, and the broader social sphere. Emerging threats generate serious and often unpredictable negative consequences for human life and health. State action, for example, in the information and education spheres, should be a response to this constantly evolving catalog of threats. People should be equipped not only with key competencies and skills but also with theoretical knowledge in the areas of national security, rescue operations, first aid, and health. The knowledge, competencies, and skills imparted through education are intended to help them behave appropriately and respond to difficult, dangerous, and crisis events, and above all, to develop the habit of coping appropriately and effectively in situations of immediate threat to life and health. Such a systemic, well-thought-out, well-organized and implemented process of building public awareness of potential threats can contribute to more effective prevention of dangerous situations and events, increase confidence and provide guarantees that in difficult situations, citizens will be able to act to ensure their own safety and will be able to protect themselves against the negative effects of threats.

## REFERENCES

Berent, Z. (1988). Pokój międzynarodowy i bezpieczeństwo – próba definicji [International peace and security – An attempt at a definition]. Sprawy Międzynarodowe, (6).

Ciekanowski, Z. (2010). Rodzaje i źródła zagrożeń bezpieczeństwa [Types and sources of security threats]. Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy.

Cziomer, E. (2010). Bezpieczeństwo międzynarodowe w XXI wieku: Wybrane problemy [International security in the 21st century: Selected problems]. Krakowskie Towarzystwo Edukacyjne.

Dobrosielski, M. (1973). Problemy współczesnych stosunków międzynarodowych [Problems of contemporary international relations]. Sprawy Międzynarodowe, (12).

Klafkowski, A. (1985). Podstawy prawne bezpieczeństwa Polski [The legal foundations of Poland's security]. Ruch Prawniczy, Ekonomiczny i Socjologiczny, (4).

Korzeniowski, L. F. (2017). Podstawy nauk o bezpieczeństwie: Zarządzanie bezpieczeństwem [Foundations of security sciences: Security management] (2nd ed.). Difin.

Lasoń, M. (2010). Bezpieczeństwo w stosunkach międzynarodowych [Security in international relations]. Krakowskie Towarzystwo Edukacyjne.

Nowakowski, Z. (2009). Bezpieczeństwo państwa w koncepcjach programowych ugrupowań parlamentarnych w Polsce po 1989 roku [State security in the programmatic concepts of parliamentary groups in Poland after 1989].

Siuda, T., & Zaczek-Zaczyński, K. (1999). Edukacja obronna młodzieży szkolnej i akademickiej [Defense education of school and academic youth]. In R. Stępień (Ed.), Współczesne zagadnienia edukacji dla bezpieczeństwa [Contemporary issues in education for security].

ISSN 2815-3324 Online, ISSN 2535-0358 Print

Wejkszner, A., & Wojciechowski, S. (2019). Współczesne bezpieczeństwo Polski: Międzynarodowy wymiar instytucjonalny [Contemporary security of Poland: The international institutional dimension].

Zięba, R. (1997). Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych [The category of security in the study of international relations]. In D. B. Bobrow, E. Haliżak, & R. Zięba (Eds.), Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku [National and international security at the close of the 20th century].

Stankov, V. (2026). Advantage in operational and tactical intelligence: A force amplifier for Ukraine. Politics & Security, 16(2), 12–21. https://doi.org/10.54658/ps.28153324.2026.16.2.pp.12-21

# ADVANTAGE IN OPERATIONAL AND TACTICAL INTELLIGENCE: A FORCE AMPLIFIER FOR UKRAINE

Vasil Stankov
Academy of National and Information Security
Plovdiv, Bulgaria
https://orcid.org/0009-0002-5757-1499
vassilst@abv.bg

***Abstract.*** *The article analyses the core problems of intelligence superiority as a premise for prevailing in modern warfare. Addressing the problem in a situational context, related to the high-intensity war in Ukraine, the study defines the intangible non-material prerequisites Ukraine needs to pursue to achieve it. The article then highlights the key elements of intelligence advantage on a tactical and operational level and suggests avenues to further enhance and uphold it as a force amplifier for Ukraine. Moreover, these elements are identified as a set of interrelated and interdependent factors, stemming directly from the unified objectives of the overall battlefield engagement. The article argues that battlefield intelligence should be directed at countering the efforts of the adversary to gain tactical and operational surprise, disrupting their capacity to execute their tactical doctrine, thus denying them their preferred and prepared style of warfare. It goes on to explore the tools that intelligence structure may use to further empower the drone warfare. Furthermore, the article reveals specific avenues to transform the advantage in tactical and operational intelligence into decisive superiority through combining different, but interlinked intelligence priorities that trace a distinctive course of action ultimately leading to a breakthrough in the war. Finally, the study highlights several key requirements that would enable the Ukrainian intelligence system to unfold its potential as a force amplifier, including an upper hand in frontline intelligence technology, all-source data integration, enhancing the interlink between the net-centric approach and drone warfare, and elevating tactical and operational intelligence to the status of a strategic instrument.*

**Keywords:** intelligence; tactics; advantage; drones; Ukraine; war.

## 1. INTRODUCTION

Intelligence superiority has long been known as one of the decisive factors in armed conflict, because it exploits the battlefield and overcomes capability gaps. As a force amplifier, intelligence dominance is not merely a function of assets and data; rather, its true importance lies in the ability to influence the intent and decisions of the commanders on the ground. Its value to the warfighter derives from the capacity to disrupt enemy objectives, thus systematically denying them victory.

This concept shifts the analytical focus toward several essential problems. First, it requires defining the intangible non-material elements of intelligence superiority and establishing how they vary depending on the specific operational environment. Second, what tactical and operational boundaries must a warring party cross to achieve and confidently exploit it? Finally, it raises the question about the comprehensive approach towards its assessment, considering the diversity of intelligence requirements across different campaigns, from the ongoing Arab-Israeli conflict to the recent war against Iran.

This article addresses these questions in a purely situational context, related to the high-intensity war in Ukraine.

There are indications suggesting that Ukraine has achieved a certain operational and tactical intelligence superiority at this point of the war. Although Russia possesses greater numbers of intelligence

ISSN 2815-3324 Online, ISSN 2535-0358 Print

assets and electronic warfare (EW) capabilities, Ukraine has pursued technological edge through domestic First-Person View (FPV) drone production and Western support, most importantly in satellite reconnaissance. Ukraine plans to produce approximately 7 million drones of various types in 2026, compared to 4 million produced in 2025 (Ryan, 2026). Moreover, the effective employment of Unmanned Aerial Vehicles (UAVs) as tactical reconnaissance and air strike platforms compels both sides to continuously maneuver their forces along the Forward Edge of the Battle Area (FEBA). This significant change objectively reduces the number of stationary targets, severely limiting the impact of field artillery compared to the opening stages of the war. Therefore, further development of tactical intelligence in this direction is going to substantially erode Russia's quantitative superiority in artillery and mortars.

These signs clearly indicate that Kyiv is successfully implementing a plan to turn the asymmetry of forces and means to its advantage. However, to set a permanent trend powerful enough to reach a strategic tipping point, this advantage must be methodically maintained until it becomes the decisive factor shaping the outcome of all major battlefield engagements in the Ukrainian theatre.

In an attempt to point out a clear way of achieving this, the article analyzes the key elements of intelligence advantage on a tactical and operational level and suggests avenues to further enhance and uphold it as a force amplifier for Ukraine. To this end, a number of Ukrainian, Russian, and Western media and analytical sources were researched and cross-referenced to explore the general problem of the study. Consequently, the need for thorough, structured, and comprehensive studies and explorations of the problem became evident.

The methodology of the article includes analysis of the key requirements of tactical and operational intelligence as dictated by the imperatives of the events unfolding on the ground and their impact on the overall situation across the frontline. The results outlined a model of achieving advantage, comprising a set of non-material elements, deduced through a careful survey of the factors shaping the balance of forces in the war. Afterwards, the prerequisites to transform the advantage into superiority were defined following a structured analysis of the current tactical and operational dynamics in the Ukrainian theatre.

## 2. RESULTS AND DISCUSSION

### 2.1 Key elements of intelligence advantage

Although for political reasons Russia avoids mass mobilization to replenish rising battlefield losses, it still maintains superiority in manpower, armament, and resources. This disparity compels Ukrainian commanders to swiftly maneuver ground troops, assets, and reserves along the frontline to repel continuing assaults. Such operational agility strongly requires advance intelligence on Russian intentions and movements, supported by robust tactical collection, as well as rapid processing, analysis, and dissemination. For Ukraine, field intelligence at this point is not just a combat support activity, but a crucial factor in the balance of forces, capable of determining the outcome of the war. Therefore, pursuing a policy of gaining advantage in tactical and operational intelligence may produce a strategic result by turning the tides of the entire campaign.

Let us examine the main qualitative elements of such an advantage given the combat environment in the Ukrainian theatre. Interrelated and interdependent, these elements stem directly from the unified objectives of the overall battlefield engagement.

First, an essential element is the ability to deny the adversary both tactical and operational surprise.

To achieve this, the intelligence must be organized and conducted according to the prevailing method of tactical warfare, implemented by both sides, which comprises operating small assault teams against dispersed enemy troops that avoid amassing in large numbers to steer clear of aerial and missile strikes. Typically, the teams have a common objective, which demands coordination to reach a larger end-result by combining a number of small-scale actions. This requires detailed intelligence information tailored to the needs of both the individual teams and the overall mission.

To counter efforts aiming at tactical surprise, intelligence activities must focus on thwarting Russia's small assault group tactics, which at present is broadly divided into two types of actions: Spetsnaz-like assaults and “thousand cuts” tactics.

The Spetsnaz-like assaults are carried out by both Special forces and regular infantry. Relying on stealth, speed, self-sufficient communications and logistics, these highly mobile units carry out rapid advances along a pre-selected route to mount surprise attacks. They are deployed for capturing strongpoints, territory, and settlements, conducting reconnaissance, ambushes, and maneuver defense by exploiting camouflage, darkness, and poor visibility for maximum surprise effect.

The “thousand cuts” tactics is another way to gain the element of surprise, which the Russians introduced in 2025. To counter Ukraine’s extensive drone coverage, they deploy ultra-small assault teams of just two to four soldiers. Equipped with portable electronic warfare (EW) devices, these dispersed units aim to quickly infiltrate and breach the Ukrainian drone defense line. This approach relies on speed, which deprives the opponent of a timely reaction. These teams aim to maintain absolute stealth under Ukrainian drone surveillance. To evade thermal imaging sensors, soldiers use special blankets or camouflage cloaks, keeping the fabric away from their bodies to reduce heat signatures.

The Russian Defense Minister Andrey Belousov declared that over 38,000 motorcycles, ATVs, and buggies were delivered to front-line troops in 2025, which comprised a tenfold increase compared to the previous year. He noted that the Russian Armed Forces are intended to achieve near-full complement for these light tactical vehicles in the near future (NVO, 2025). These vehicles are used primarily to launch surprise attacks across the drone engagement zone, where much depends on high mobility.

Maintaining intelligence advantage, capable of denying the opponent the element of tactical and operational surprise demands compressing the intelligence cycle even further by deeply integrating reconnaissance with precision strike systems, as well as employing an effective network of stationary and mobile ground observation posts, night-vision equipment, and thermal imaging systems, all operating in unison with the overhead reconnaissance platforms.

Second, the intelligence advantage must disrupt the enemy's capacity to execute their tactical doctrine.

The traditional Russian pre-war doctrine relied on holding the initiative across the entire theater and establishing overwhelming superiority in troop numbers and firepower at the main points of effort. Despite assessments that Ukrainian forces have seized the initiative for the first time in three years (Pokotylo, 2026), the recent advance by Russian Army Group “North” in the Sumy region, where the frontline has been static for a while now, demonstrates that Moscow retains the ability to gain operational surprise.

However, with casualties reaching 35,000 per month, Russia is losing soldiers faster than it can replace them. Notably, FPV drones loaded with explosive inflict up to 80% of these casualties. They hunt individual soldiers and disrupt medical evacuations, substantially increasing the death toll on the battlefield (Kapital, 2026). In a war of attrition, the loss of life on the battlefield causes loss of initiative in the war.

The war has demonstrated that wide-ranging field intelligence, surveillance, and reconnaissance (ISR) deny the opponent the ability to accumulate forces to reach superiority, thus severely curbing the scope and depth of offensive actions. Moreover, all-encompassing satellite and drone reconnaissance prevents the concentration of troops deep within strike range, making dangerous any troop build-up in the rear echelon. Hence, the operational employment of full-sized Battalion Tactical Groups (BTGs) as a primary combat formation for airborne, motorized rifle, tank, and marine units has been completely abandoned. In this way, enhanced reconnaissance coverage of the combat zone prevents the opponent from utilizing the battlefield, deploying forces, and achieving far-reaching operational objectives.

To fully grasp the scale of this transition, we must consider the importance of the BTG concept within the Russian ground forces doctrine.

ISSN 2815-3324 Online, ISSN 2535-0358 Print

A BTG is a combat formation possessing all the forces and means to independently carry out a mission, both offensive and defensive, having the capability to defend itself from any possible threat. Therefore, the main characteristics of BTGs are independence, self-sufficiency, and operational flexibility. The order of battle varies depending on the specific mission, but generally it would comprise three motorized rifle companies; a tank company; one or two artillery batteries; a mortar battery; an air defense platoon; grenade launcher and anti-tank units; communications, reconnaissance, and engineering platoons; electronic warfare and UAV units; repair and evacuation and rear support units. Total personnel strength amounts to 700-800 troops.

In August 2021, the former Defense Minister Shoigu announced, that there were as many as 168 BTGs in the Russian Armed Forces (UK Ministry of Defence, 2022).

According to expert assessments, as of January 2022, a month prior to the invasion approximately 60 of them were deployed close to the border with Ukraine (Centre for Eastern Studies, 2022).

To better understand why the employment of these formations was abandoned, let us envision a hypothetical scenario where a BTG operates in strict accordance with Russian Ground Forces doctrine, but within the drone-infested environment of the present Ukrainian theater.

The Ground Forces Field Manual stipulates the marching order of a BTG to include a field security detachment, support detachment, main forces column, and a column of technical, logistical, and medical support units. A Forward March Outpost (FMO) is assigned to protect the marching troops, comprising a motorized rifle (tank) company, reinforced by tanks (a motorized rifle unit), artillery, and air defense and NBC units. To the flanks and the rear, if needed, other march outposts are assigned, consisting of motorized-rifle platoons with tanks. The FMO is 5-10 km ahead of the main forces, while the flank and rear elements keep a distance of 3-5 km. The main forces column may include a motorized rifle (tank) battalion, an artillery battalion, and other units. Distances between battalions are 2-3 km, between companies – up to 1 km, between vehicles – 25-50 meters. When moving across open terrain under the threat of enemy precision-guided weapons, vehicles maintain 100-to-150-meter intervals, while companies and battalions are separated by 500 meters and 1 kilometer, respectively (Bstudy.net, n.d).

Obviously, this is entirely flawed and irrelevant in an environment with an extremely high drone density, where the airspace is so proliferated with reconnaissance-attack UAVs, that it absolutely prohibits this type of troop movements.

In the reality of the combat zone, troop movements from the rear areas to the forward edge are conducted in dispersed groups rather than in organized columns. Persistent aerial reconnaissance-strike operations force the adversary to rely heavily on dismounted infantry, thus significantly increasing their vulnerability and diminishing their offensive potential. The Ukrainian edge in tactical intelligence has effectively compelled Russian forces to abandon almost completely the use of tanks and other armored vehicles during direct assaults against frontline defenses.

Therefore, the intelligence advantage becomes a primary deterring factor, denying the adversary the opportunity to conduct their preferred and prepared style of warfare. By minimizing their superiority in material assets, it forces them outside their doctrinal and operational boundaries and compels them to continuously adapt to the changing environment. Consequently, ultimate advantage belongs not to the stronger side, but to the one that adapts faster (Ryan, 2026).

Tactical intelligence transforms the battlespace, reshaping the tools of ground warfare and the rationale of small-unit combat. Secure communications, concealment, and rapid decision-making have become more important than raw firepower. Furthermore, interoperability between infantry, drone operators, artillery, and electronic warfare units is now essential. Victory no longer depends on manpower advantages, but on technical solutions that guarantee battlefield visibility, resilient drone command-and-control, and real-time data sharing across units (Liang, 2025). Adversely, lack of detailed and reliable battlefield information can significantly restrict situational awareness and coordination. Ukrainian intelligence sources report that Russian commanders of the Army Group “South” were using inaccurate

maps, while large groups of Russian soldiers were deployed to forward areas without proper communication, and were therefore highly vulnerable to Ukrainian counterattacks (Sedlak, 2026).

Simultaneously, frontline intelligence analysts must look with great attention into the evolution of tactical and operational methods, specifically examining the impacts and shortcomings of the small-unit assault tactics currently implemented by Russian forces. Some observers analyze it as an adaptation of Soviet-era covert penetration methods from World War II. In any case, while this approach does not always yield territorial gains, it reflects a fundamental shift in perceiving and employing the assault tactics – moving away from the pursuit of a decisive, large-scale blow in favor of high-persistence attrition. It is worth exploring whether Russian high command resorted to this approach due to an acknowledged inability to achieve a genuine strategic breakthrough (RUSI, 2025).

Operationally, maintaining simultaneous pressure across multiple avenues appears to be the only possible alternative given Russia's reluctance to declare general mobilization, continuing manpower shortages, and a deficit in the tactical proficiency required to breach layered defenses and hold captured areas. An obvious disadvantage is the fact that the small-group tactics render the Russian Armed Forces deeply fragmented and unable to rapidly exploit local successes. Furthermore, if a defensive sector begins to collapse, the Ukrainian Armed Forces (AFU) remain capable to rapidly redeploy reserves.

At this stage Moscow's operational logic outlines an obvious preference for enemy attrition over territorial acquisition. Notably, this attrition targets human resources rather than military hardware, promptly replenished by western allies. Most probably, the aim is to exhaust Ukraine's core cadre of experienced, capable, high-quality soldiers and mid-level commanders—the critical personnel meant to keep the morale of frontline troops by mentoring newly mobilized recruits. Arguably, Moscow's long-term rationale may include the assumption that degrading the AFU's human potential will inevitably trigger a broader collapse of entire sections of the front, ultimately forcing the surrender of Ukraine's remaining contested regions without the need for high-casualty advances (France 24, 2026).

Third, advantage in tactical reconnaissance translates into advantage in drone warfare.

No other armed conflict has emphasized the interdependence between ISR and drone warfare as heavily as the war in Ukraine. An effective drone capability has become a decisive factor in the balance of forces, carrying important operational and strategic implications for the entire campaign.

Field reconnaissance drones are increasingly implemented as loitering munitions, turning the multi-role UAVs as the most widely used weapon in the theatre. FPVs, including small Mavic quadcopters, are operated as both reconnaissance and strike platforms to drop munitions like grenades, mortar shells, and bottles of petrol (Liang, 2025) upon enemy trenches, shelters, vehicles, and personnel. The integration between intelligence collection and precision strikes establishes so-called lethal surveillance tactics (Mai, 2021). This approach severely restricts the maneuver room of enemy units and degrades the effectiveness of their fire destruction system. For example, Multiple Launch Rocket Systems (MLRS), conventional artillery, and tanks primarily fire from concealed positions, abandoning them rapidly to evade counter-battery response.

Moreover, drones have the ability to disrupt enemy counter-attacks against important tactical areas, which define the situation on specific operational avenues, thus preventing them from seizing the initiative.

Ukrainian naval drones inflicted severe damage on Russia's Black Sea Fleet, demonstrating how tactical reconnaissance can yield strategic results. It becomes increasingly clear that remotely controlled naval systems present a formidable asymmetric threat to surface ships, sea lines of communication (SLOCs), and maritime port infrastructure (Liang, 2025).

ISSN 2815-3324 Online, ISSN 2535-0358 Print

### 2.2. Turning the advantage into superiority

Turning the advantages into true intelligence and overall combat superiority depends on implementing and developing the intangible factors to meet the changing imperatives of the war. In practice, this requires maintaining the upper-hand in field-applied intelligence technology; integrating all-source data to achieve comprehensive battlefield visibility; accepting the drone-centric aspect as the essence of the network-centric approach to field intelligence, and further strengthening the connection of tactical and operational intelligence with strategic planning. Meeting these requirements would help the intelligence system unfold its true potential as a force amplifier.

First, advanced field-applied technology is vital to enhancing both reconnaissance-strike and counter-drone capability.

Further development of drone warfare requires a comprehensive use of Artificial Intelligence (AI) to empower the swarm technology, where hives of remotely controlled drones carry out missions semi-independently under limited human control. Artificial intelligence and robotic devices should no longer be considered supplementary, but essential for routine tactical operations. Advanced drones with software-driven target recognition and AI-assisted control systems should no longer be experimental, but standard-issue weaponry. They should be deployed, utilized, lost, produced, and redeployed in rapidly repeating cycles (Digital State UA, 2026). We have to bear in mind, however, that a number of ethical issues would arise if humans were completely excluded from the targeting (SWJ Staff, 2026) and decision-making process within the reconnaissance-strike missions, especially when it comes to assessing the risk of collateral damage.

Technological advantage invariably carries operational and strategic implications. According to Russian drone manufacturers, Moscow has lost its leadership in drone production and warfare over the past six months. This severely hampered troop movements to and alongside the FEBA due to heavy losses and logistical issues. As a result, Russia was forced to restrict supply convoys in Donetsk to a maximum of two trucks to avoid detection (Kapital, 2026). These operational constraints fundamentally prevent them from maneuvering forces, bringing in reserves, or carrying out routine frontline rotations.

Following indications that the Ukrainian Armed Forces had launched a new offensive in early 2026, the US company SpaceX severed the Russian military's unauthorized access to its Starlink satellite network. Days later, Ukrainian forces successfully breached the defenses of Army Group South, recapturing critical territory in the Zaporizhzhia region (Sedlak, 2026). Actually, this was probably related to another development, which might precede the powering down of all Starlink terminals now illicitly used by the Russian military. In late September 2025, Starlink, together with the Ukrainian telecom Kyivstar, started testing the Direct to Cell (DTC) technology, designed to allow regular 4G smartphones to connect directly to the Starlink satellites. This technology greatly facilitates battlefield communications and bypasses the ground terminals, significantly reducing the frontline infrastructure, now frequently targeted by Russian electronic warfare assets and strike drones. Moreover, DTC is a vital capability, greatly contributing to mobile communications, command-and-control, data transmission, and drone operations. A smartphone will be enough to a frontline soldier to always stay connected and updated. As early as 2024 this technology provided transfer speed of 17 Mbps via a smartphone, which is considered sufficient for the Ukrainian military, but is expected to rise as the number of satellites increases (Kyiv Post, 2025).

Portable anti-drone equipment is another field-applied technology that needs to be developed further. Since FPV drones and reconnaissance UAVs are a primary threat to the frontline troops, effective field-applied countermeasures are vital to detect and destroy them before they reach their targets. To this end, Ukrainian engineers developed Chuyka 3.0—a three-band portable drone detector designed to intercept video signals from drones in real time. In fact, this electronic warfare (EW) trench equipment is what the troops actually need as an early warning tool against FPV strikes. Traditional large-size equipment can no longer be adequate to the realities of the highly agile frontline defense, along with the rapidly evolving radio-electronic environment across the modern battlefield. Consequently, there will be

a transition from cumbersome centralized EW infrastructure to individual portable devices (Fakty.ua, 2026).

Second, close integration of aerial reconnaissance and satellite imagery with tactical level Electronic Intelligence (ELINT), Human Intelligence (HUMINT) and Open-Source Intelligence (OSINT) is instrumental in creating a comprehensive picture of the battlefield. Such an integration has the potential to bring about an operational breakthrough in the entire theatre.

In an environment, where UAVs provide live footage, military satellites deliver continuous, detailed, and high-resolution imagery, and citizens crowdsource situational updates, raw data can only be converted into actionable information through an integration framework operating within the intelligence cycle. Without integration and fusion, valuable information will be used only intermittently, when it is already too late, and on a limited scale.

Battlefield OSINT suffers significant shortcomings (Rasak, 2021), but is not obsolete and can still be adapted to the tactical requirements of the Ukrainian theatre. As a publicly available collection method, crowdsourcing allows citizens the opportunity to send via internet relevant open-source information about events they witness. It remains a viable tool to gather battlefield intelligence to support friendly forces, as well as detect enemy infiltrations and other suspicious activities in the rear areas. Ukrainian intelligence has required public support to track Russian formations. Citizens report Russian unit positions and movements through government chatbot networks, transmitting photos and videos containing geospatial metadata.

However, field OSINT and crowdsourcing in particular have several critical vulnerabilities, which need to be addressed:

- Vulnerability to “Event Barraging”: The adversary can execute organized disinformation operations, either by creating plausible false data or by 'flooding' social media with contradictory and deceptive information to obscure the reality on the ground (Rasak, 2021).

- Vulnerability to cyber warfare: The government chatbot networks can be susceptible to Distributed Denial-of-Service (DDoS) attacks. In February 2022, the diia.gov.ua portal was targeted by a massive attack designed to overwhelm the servers (van Beek & Rietjens, 2024).

- Vulnerability to Risks, related to the International Humanitarian Law: Under the 1949 Geneva Conventions, active civilian participation blurs the distinction between combatants and non-combatants. This allows the adversary to argue that civilians gathering intelligence lose their protected status.

Third, the drone-centric aspect needs to become the essence of the network-centric approach to field intelligence, placing the emphasis on the drone warfare according to the imperatives of the war.

The tactical and operational intelligence process will be largely subordinate to drones as the main reconnaissance-strike platforms. This grants UAV units independent organizational status as separate combat formations. Drones modify force structure by transforming ISR from an auxiliary support function into a distinct service branch under direct military command. The Armed Forces of Ukraine led this transformation, becoming the first to integrate special UAV strike companies and separate combat groups directly into the combat brigades (Samus, M, 2026).

Drone-centric framework will facilitate intelligence advantage by abandoning rigid hierarchy and adopting a resilient combat-oriented structure, which channels operational and tactical intelligence directly to the warfighters on the ground. This structure will ensure a smooth and rapid workflow within the system, integrating the collection assets (aerial platforms, satellites, human sources, open sources) along with the processing, analysis and dissemination, into a single unified sequence taking place in the combat units themselves. This approach further blurs the distinction between tactical and operational levels, often merging reconnaissance with actual combat, and planning with decision-making.

Theoretically and in practice, the drone-centric approach is easily accommodated within the broader network-centric concept, which involves more than just the integrated use of intelligence assets to ensure

ISSN 2815-3324 Online, ISSN 2535-0358 Print
all-encompassing exchange of tactical information between the participants in a given operation. It demands evolving the modus operandi of the combat formations from a concentrated to a dispersed deployment model, optimizing reconnaissance, enabling coordination and targeting, and establishing a balanced distribution of assets across command levels. This directly corresponds to the imperatives of the war in Ukraine.

Fourth, tactical and operational intelligence should be intertwined with strategic planning.

The advancement in tactical and operational intelligence invariably enhances strategic targeting, based on establishing the opponent's key vulnerabilities and defining their strategic centers of gravity. Thus, the drone-centric warfare aims at strategic objectives. In fact, the evolution of tactical and operational intelligence produced a leap in strategic capabilities, allowing the long-range drone operations deep within Russian territory to transform into an impactful strategy aimed at forcing Russia to stop the war. Instead of attritional frontline operations, which proved costly in every way, Ukraine begins to conduct an asymmetric warfare intended for degrading the Russian economy, disrupting military production, and undermining public morale (Nesterova, 2026).

Ukraine's strategic campaign, targeting key military capabilities and critical energy infrastructure, has penetrated deep into the Russian rear, reaching as far as the Ural Mountains. In late April, a drone strike on the Shagol military airfield in Chelyabinsk, situated about 1700 km from the Russian-Ukrainian border, damaged three jets, including two Su-57 fighters and one Su-34 fighter-bomber. Days later, in early May, an oil refinery and pumping station in Perm were destroyed as part of a coordinated wave of drone attacks on energy plants and export terminals. Media reports reveal that April's strikes reduced the daily production volume by 400,000 barrels. According to Ukrainian assessments, major export terminals in Novorossiysk and Ust-Luga operate at less than half capacity.

It is noteworthy that the Su-34 serves as the primary strike platform and is capable of carrying a wide range of guided bombs and missiles, striking critical infrastructure, military installations, and civilian targets at ranges of up to 1,000 kilometers. The Su-34 is the main carrier of Russia's makeshift glide bombs, which continue to inflict great damage across the FEBA and the close rear areas. These bombs represent regular unguided bomb bodies, equipped with a conversion kit, called the Universal Gliding and Correction Module (UMPK). The Su-57, in turn, is Russia's most advanced stealth fighter and poses a particular threat to aviation and air defense systems. The estimated cost of a single Su-34 is between $35 and $50 million, while the Su-57 costs between $100 and $120 million (Kyiv Independent, 2026). Moreover, Ukraine launched a massive drone strike on the Russian capital in mid-May, the largest in more than a year, hitting a military-industrial complex enterprise and key oil facilities in the Moscow region: the Moscow Oil Refinery and two oil pumping stations.

Naturally, this strategy is closely linked to the tactical and operational dynamics within the combat zone. It remains to be seen whether it would prevent Russia from seizing Donbas and force it to negotiate on terms more favorable to Ukraine. It certainly has the potential to deter Russian offensive operations, thus reducing the overall pressure along the frontline. Moreover, it really affects the attitudes of the Russian public. Although polls show that 73% of Russians still approve of Putin as president, this is the lowest level of support since February 2022 (Novaya Gazeta Europe, 2026).

The behavior of the Russian high military command can be considered an indication that the current Ukrainian strategy is working. The Russian Chief of the General Staff Valery Gerasimov once again demonstrated a very inaccurate assessment of the situation on the battlefield, claiming that Russian troops were advancing west of Kupyansk in the Kharkiv region, whereas the city still remained under Ukrainian control.

This reluctance to acknowledge the realities on the ground indicates that the tides may be really turning in Ukraine's favor, largely due to the advantage in operational and tactical intelligence achieved during the last months of the war.

## 3. CONCLUSION

Ukraine has the opportunity to gain a lasting advantage in the war by upholding the intangible elements of intelligence superiority, defined by the tactical and operational imperatives of the theatre. The intelligence effort must aim at denying the adversary both tactical and operational surprise, disrupting their capacity to execute their tactical doctrine and facilitating the drone warfare.

This advantage is poised to yield strategic superiority through maintaining the upper-hand in advanced field-applied reconnaissance-strike and counter-drone capability, integrating all-source intelligence to make the battlefield visible to the frontline warfighters, regarding the UAVs as the main component of the net-centric approach to modern warfare, and empowering tactical and operational intelligence to serve the needs of strategic planning.

## REFERENCES

Bstudy.net. (n.d.). Osobennosti primeneniya batal'onnoy takticheskoy gruppy v razlichnykh vidakh deystviy [Features of the employment of the battalion tactical group in various types of operations]. https://bstudy.net/760717/bzhd/osobennosti_primeneniya_batalonnoy_takticheskoy_gruppy_razlichnyh_vidah_deystviy

Defence24. (2022, March 14). Russia losing 22 battalion tactical groups: Is BTG a myth, or is it truly effective in combat? [Analysis, citing OSW Centre for Eastern Studies]. https://defence24.com/armed-forces/land-forces/russia-losing-22-battalion-tactical-groups-is-btg-a-myth-or-is-it-truly-effective-in-combat-analysis

Digital State UA. (2026). How Ukraine became a global reference point for AI-driven warfare. https://digitalstate.gov.ua/news/tech/shi-na-viyni-chomu-ukrayinskyy-dosvid-vykhodyt-za-mezi-defens-i-zminiuye-model-tsyfrovoyi-derzavy

Fakty.ua. (2026). Radioelektronna rozvidka v Ukrayini: rol' i mozhlyvosti Chuyky [Electronic intelligence in Ukraine: The role and capabilities of Chuyka]. https://fakty.com.ua/ru/ukraine/20260122-radioelektronna-rozvidka-v-ukrayini-rol-i-mozhlyvosti-chujky/

France 24. (2026, February 24). How Russia's 'thousand cuts' tactic is straining Ukraine's frontline forces. https://www.france24.com/en/europe/20260224-how-russia-thousand-cuts-tactic-is-straining-ukraine-frontline-forces

Kapital. (2026, May 13). Analiz: Rusiya se pripva na boynoto pole [Analysis: Russia is straining on the battlefield].https://www.capital.bg/politika_i_ikonomika/redakcionni_komentari/2026/05/13/4913238_analiz_rusiia_se_prepuva_na_boinoto_pole/

Kyiv Independent. (2026, May 1). Ukraine strikes Russian airfield nearly 1,700 kilometers away, damages 4 fighter jets, military confirms. https://kyivindependent.com/ukraine-strikes-russian-airfield-damaging-2-fighter-jets/

Kyiv Post. (2025, December 5). The Starlink-Kyivstar direct-to-cell service will help Ukraine's war effort. https://www.kyivpost.com/post/65489

Kyiv Post. (2025, November 25). Ukrainian carrier Kyivstar launches Europe's first Starlink Direct to Cell service. https://www.kyivpost.com/post/64962

Liang, C. S. (2025). Ten lessons from the Russia-Ukraine War. Geneva Centre for Security Policy. https://www.gcsp.ch/publications/ten-lessons-russia-ukraine-war

Mai, C. (2021). The impact of drone technology on intelligence practices: Revolutionary or evolutionary?. *The Student Strategy & Security Journal*. University of Glasgow. Third Edition. https://3sjournal.com/third-edition-main-page/

Nesterova, I. (2026). U Ukrainy poyavilas' novaya strategiya voyny, i ona uzhe dayet rezul'taty [Ukraine has a new war strategy, and it is already producing results]. UNIAN. https://www.unian.net/war/voyna-v-ukraine-u-ukrainy-poyavilas-novaya-strategiya-i-ona-uzhe-prinosit-rezultaty-13386375.html

Nezavisimoye Voyennoye Obozreniye. (2025, December 26). Taktika boevykh deystviy rossiyskoy armii v zone SVO radikal'no izmenilas' [The Russian army's combat tactics in the special-operation zone have radically changed]. https://nvo.ng.ru/armies/2025-12-26/11_9409_4.html

Novaya Gazeta Europe. (2026, May 1). Another new poll shows Russians' support for Putin at its lowest since February 2022. https://novayagazeta.eu/en/articles/2026/05/01/another-new-poll-shows-russians-support-for-putin-at-its-lowest-since-february-2022-en-news

Pokotylo, O. (2026). Ukraine has seized the initiative in the war against Russia for the first time in three years — expert opinion. Online.UA. https://news.online.ua/en/ukraine-has-seized-the-initiative-in-the-war-against-russia-for-the-first-time-in-3-years-expert-opinion-903949/

Rasak, M. J. (2021). Event barraging and the death of tactical level open-source intelligence. Military Review, 101(1), 48–57.

Royal United Services Institute (RUSI). (2025, October). Russian small-group infiltration tactics in Ukraine. https://www.rusi.org

Ryan, M. (2026). Ukraine is mastering 21st-century warfare. Engelsberg Ideas. https://engelsbergideas.com/essays/ukraine-is-mastering-21st-century-warfare/

Samus, M. (2026). Russia's war in Ukraine: Drone-centric warfare. International Centre for Defence and Security (ICDS). https://icds.ee/en/russias-war-in-ukraine-drone-centric-warfare/

Sedlak, M. (2026). Ukrainian battlefield gains expose Russia's communications problems. Atlantic Council. UkraineAlert. https://www.atlanticcouncil.org/blogs/ukrainealert/ukrainian-battlefield-gains-expose-russias-communications-problems/

Small Wars Journal. (2026, March 31). Drone swarms: The potential AI future of drone warfare. https://smallwarsjournal.com/2026/03/31/drone-warfare-ukraine-ai-swarms/

UK Ministry of Defence. (2022, November 29). Defence intelligence update on Russian battalion tactical groups [as reported by Newsweek]. https://www.newsweek.com/intelligence-report-reveals-3-intrinsic-russian-tactical-unit-weaknesses-1763215

van Beek, B., & Rietjens, S. (2024). Open-source intelligence in the Russia-Ukraine war. https://www.jstor.org/content/oa_chapter_edited/jj.13760045.7?seq=1

Lyseiuk, A. (2026). Artificial intelligence in intelligence and security services: Regulatory and ethical challenges of balancing operational efficiency with democratic oversight. Politics & Security, 16(2), 22–32.
https://doi.org/10.54658/ps.28153324.2026.16.2.pp.22-32

# ARTIFICIAL INTELLIGENCE IN INTELLIGENCE AND SECURITY SERVICES: REGULATORY AND ETHICAL CHALLENGES OF BALANCING OPERATIONAL EFFICIENCY WITH DEMOCRATIC OVERSIGHT

Andrii Lyseiuk
National Academy of the Security Service of Ukraine
Kyiv, Ukraine
https://orcid.org/0000-0002-9026-1188
andrii_lyseiuk@sci-univ.com

**Abstract.** *Purpose. The article examines how democratic states can govern the use of artificial intelligence in intelligence and security services without undermining operational effectiveness. It addresses the tension between AI-enabled speed, scale, and pattern detection, on the one hand, and legality, accountability, privacy, and democratic oversight, on the other. Methods. The study applies qualitative comparative legal and policy analysis. It combines review of regulatory instruments, intelligence oversight models, and AI ethics literature with a structured comparison of the European Union, the United States, the United Kingdom, and Israel. The article also develops an original analytical model, the Security–Oversight Balance framework. Findings. AI is already reshaping intelligence work through open-source intelligence analysis, signals intelligence triage, biometric identification, predictive threat analytics, cyber intelligence, and decision-support tools. Existing governance regimes are uneven. The EU has adopted a rights-based risk model through the AI Act, but national security exemptions remain significant. The United States relies more heavily on executive policy, agency guidance, and national security memoranda. The United Kingdom has a mature investigatory powers regime but lacks a dedicated AI-specific intelligence statute. Israel demonstrates a security-driven and innovation-oriented model with more limited public transparency. Across all cases, the central risks are algorithmic bias, opacity, mission creep, weak auditability, and the displacement of responsibility from human decision-makers to technical systems. Conclusions. Democratic oversight of AI in intelligence should not be treated as an obstacle to security capacity. It is a condition of legitimate and sustainable security governance. The proposed Security–Oversight Balance framework recommends four linked safeguards: legal authorization, technical auditability, managerial accountability, and ethical proportionality. The article argues for classified but reviewable AI registers, mandatory human accountability for consequential decisions, independent technical audit capacity, and international minimum standards for AI use in security services.*

**Keywords:** artificial intelligence in security; intelligence services regulation; democratic oversight; algorithmic surveillance; AI ethics in public security; national security governance.

## 1. INTRODUCTION

Artificial intelligence has become a strategic technology for intelligence and security services. Machine learning systems can process satellite imagery, intercepted communications, financial flows, social media

content, cyber telemetry, biometric records, and multilingual open-source materials at a speed and scale unavailable to human analysts. In operational terms, this creates clear advantages: AI can detect patterns, prioritize weak signals, support early warning, reduce analytic overload, and accelerate decision cycles in counterterrorism, cyber defence, border security, and military intelligence. Intelligence services have always depended on information asymmetry, but AI changes both the volume of available information and the institutional capacity to convert data into actionable assessments.

This transformation creates a democratic dilemma. The same systems that improve intelligence capacity may also expand state surveillance, normalize predictive suspicion, and weaken traditional safeguards. AI-based systems are not neutral instruments. They are trained on historical data, embedded in institutional cultures, shaped by procurement choices, and often protected by secrecy, intellectual property claims, and national security classifications. In intelligence contexts, these features are intensified. A person affected by an AI-generated risk score, watchlist nomination, biometric match, or targeting recommendation may never know that such a system was used. Courts, parliaments, inspectors general, and data protection authorities may also lack the technical expertise or access needed to evaluate the system properly.

The core problem is therefore not whether intelligence services should use AI. Democratic states cannot ignore technologies that adversaries, criminal networks, and authoritarian regimes already exploit. The real question is how AI can be integrated into intelligence operations while preserving democratic legitimacy. As Gill and Phythian (2018) argue, intelligence in democratic societies requires both effectiveness and control. Security services must be capable enough to protect the state, but constrained enough not to become a threat to the constitutional order they are meant to defend.

This article addresses the following research question: how can democratic states operationalize effective and legitimate control over the use of AI in intelligence operations without undermining security capacity? The article proceeds in nine steps. First, it explains the methodology. Second, it develops a typology of AI applications in intelligence and security operations. Third, it analyses the regulatory landscape in the EU, the United States, the United Kingdom, and Israel. Fourth, it identifies the main ethical challenges. Fifth, it compares democratic oversight mechanisms. Sixth, it proposes the Security–Oversight Balance framework. Seventh, it offers policy recommendations. The conclusion argues that the future of democratic intelligence governance depends on transforming oversight from a reactive legal check into a continuous socio-technical process.

## 2. METHODOLOGY

The article uses qualitative comparative analysis of legal, policy, and institutional materials. The research design combines three methods: normative document analysis, comparative institutional analysis, and conceptual framework development. Normative document analysis is applied to binding and non-binding instruments regulating AI, surveillance, data protection, and intelligence oversight. These include Regulation (EU) 2024/1689, the General Data Protection Regulation, the UK Investigatory Powers Act 2016, U.S. intelligence community AI principles, U.S. federal AI policy documents, the Council of Europe Framework Convention on Artificial Intelligence, the UNESCO Recommendation on the Ethics of Artificial Intelligence, NATO AI strategies, and the NIST AI Risk Management Framework.

The comparative component focuses on four democratic or democratic-allied jurisdictions: the European Union, the United States, the United Kingdom, and Israel. These cases were selected because each combines advanced security capacity with distinct legal and institutional approaches to AI governance. The EU represents a rights-based and risk-based regulatory model. The United States represents an executive-policy and agency-guidance model, complicated by changes across administrations. The United Kingdom represents a mature surveillance-law model structured around warrants, commissioners, and parliamentary review. Israel represents a security-intensive innovation model in which AI policy has developed alongside strong national security imperatives.

The article does not conduct empirical testing of classified AI systems. That limitation is unavoidable because intelligence AI deployments are often not publicly disclosed. Instead, the article evaluates governance design: how legal rules, oversight institutions, technical safeguards, and ethical principles could be combined to control high-risk AI uses. The proposed Security–Oversight Balance framework is therefore conceptual and prescriptive. It is intended as a tool for lawmakers, oversight bodies, and security institutions rather than as an empirical measurement instrument.

## 3. AI IN INTELLIGENCE OPERATIONS: A TYPOLOGY

AI in intelligence services should not be treated as a single technology. It is better understood as a family of systems embedded across the intelligence cycle: collection, processing, analysis, dissemination, operational planning, and post-operation review. The governance problem differs depending on whether AI merely filters large datasets, identifies persons, predicts conduct, recommends operational action, or autonomously triggers consequences.

A first major field is open-source intelligence. OSINT now includes social media posts, geolocation data, commercial satellite imagery, leaked databases, public procurement records, videos, messaging platforms, and digital traces from conflict zones. AI tools support entity recognition, translation, sentiment analysis, image classification, geospatial matching, network analysis, and disinformation detection. Recent OSINT research shows that AI can improve the speed of extracting signals from public data, but it also increases the risk of misinterpretation, source contamination, and overconfidence in pattern recognition (Browne et al., 2024). In conflicts such as Russia's war against Ukraine, OSINT has become operationally relevant, but the boundary between intelligence, journalism, activism, and information warfare has become blurred.

A second field is signals intelligence and communications analysis. Intelligence agencies collect and process vast volumes of metadata and content. AI can support language identification, voice recognition, anomaly detection, clustering of communication patterns, and prioritization of intercepts. These systems may reduce analytic overload, but they also create significant proportionality problems. The more automated the filtering process becomes, the more difficult it is to determine whether collection remains targeted or becomes functionally indiscriminate.

A third field is biometric intelligence. Facial recognition, gait analysis, voice identification, iris recognition, and other biometric tools allow security services to identify persons across physical and digital environments. Biometric systems can be valuable for identifying terrorism suspects, locating missing persons, or verifying identities at borders. Yet biometric AI is among the most rights-sensitive applications because it links bodies to state databases. Studies of commercial facial analysis have shown intersectional accuracy disparities, especially for darker-skinned women (Buolamwini & Gebru, 2018). In security contexts, such error disparities can produce wrongful suspicion, discriminatory targeting, or unlawful watchlisting.

A fourth field is predictive threat analytics. These systems seek to forecast possible threats by analysing behavioural, geographic, social, or transactional data. They may be used to prioritize investigations, identify radicalization risks, allocate patrols, detect insider threats, or predict cyberattacks. Predictive systems are attractive because they promise anticipation rather than reaction. However, predictive policing literature warns that such models may reproduce historical enforcement patterns and create feedback loops: areas or communities previously subject to more policing generate more recorded data, which then justifies further policing (Brayne, 2017; Ferguson, 2017).

A fifth field is cyber intelligence. AI can detect malware patterns, classify phishing campaigns, identify anomalies in network traffic, map adversary infrastructure, and support automated response to cyber incidents. Compared with biometric or predictive policing systems, cyber AI may seem less directly intrusive. Nevertheless, cyber intelligence often involves large-scale monitoring, cross-border data flows,

and cooperation with private infrastructure providers. It therefore raises oversight questions about authorization, necessity, and collateral access to personal or commercial data.

A sixth emerging field is AI-assisted decision support. Generative and agentic systems can summarize intelligence reports, generate hypotheses, simulate adversary behaviour, draft threat assessments, or recommend operational options. These tools may improve productivity, but they also introduce risks of hallucination, automation bias, and hidden dependence on systems that cannot reliably explain their outputs. In intelligence work, a plausible but false AI-generated synthesis can be more dangerous than an obviously incomplete report because it may appear authoritative.

Table 1. Artificial intelligence applications in intelligence and security services: operational benefits and main oversight risks

| AI application | Operational benefit | Main oversight risk |
|---|---|---|
| OSINT analysis | Rapid processing of public and semi-public data | Misclassification, source contamination, weak verification |
| Signals intelligence triage | Prioritization of large intercept datasets | Expansion of bulk collection and opaque filtering |
| Biometric identification | Faster person identification and identity verification | Discrimination, false matches, continuous public surveillance |
| Predictive threat analytics | Early warning and resource allocation | Feedback loops, profiling, predictive suspicion |
| Cyber intelligence | Faster anomaly detection and threat attribution | Overbroad monitoring and unclear authorization |
| AI decision support | Faster synthesis and scenario generation | Automation bias, hallucination, diluted responsibility |

This typology shows that governance cannot rely on a generic statement that "AI is supervised by humans." Oversight must be matched to function. A language translation model used for OSINT triage does not require the same control as a biometric watchlist system or a predictive threat model. The democratic challenge is to classify AI uses by operational intensity and rights intrusiveness, then attach appropriate safeguards.

## 4. THE REGULATORY LANDSCAPE

The regulatory landscape is fragmented. No major democracy has yet adopted a complete AI-specific intelligence statute. Instead, AI in intelligence is governed through overlapping layers: AI regulation, data protection law, surveillance law, constitutional rights, procurement rules, classified directives, and internal agency policies.

The European Union has adopted the most comprehensive horizontal AI regulation. Regulation (EU) 2024/1689 establishes a risk-based model, including prohibited practices, obligations for high-risk systems, transparency duties, and rules for general-purpose AI. Law enforcement and biometric systems appear in high-risk categories, and certain forms of real-time remote biometric identification in publicly accessible spaces are restricted. However, the AI Act also contains exclusions for military, defence, and national security purposes. This creates a central tension: the EU has a strong rights-based AI framework, but some of the most security-sensitive AI uses may fall partly outside its scope.

The GDPR remains relevant because AI systems often process personal data. Article 23 allows restrictions on certain rights and obligations when necessary and proportionate for national security, defence, public security, or criminal law purposes. This means that data protection rights may be limited in intelligence contexts, but not eliminated. The key legal test is necessity and proportionality. For AI-enabled intelligence, this implies that secrecy cannot become a blanket justification. Even where individual notification is impossible, independent bodies must be able to examine whether data processing is lawful, limited, and auditable.

The United States follows a more fragmented model. The Office of the Director of National Intelligence adopted Principles of Artificial Intelligence Ethics for the Intelligence Community and an AI Ethics Framework in 2020. These documents emphasize lawfulness, accountability, transparency, reliability, security, and human judgment. The NIST AI Risk Management Framework provides voluntary, rights-preserving guidance for identifying and managing AI risks. U.S. policy has also changed significantly since the 2023 Executive Order 14110. That order was rescinded in January 2025 and replaced by a more innovation- and competitiveness-oriented policy direction under Executive Order 14179. The 2025 America's AI Action Plan and OMB Memorandum M-25-21 emphasize accelerated federal AI adoption, governance, and public trust, while the 2026 National Security Presidential Memorandum on AI in the National Security Enterprise focuses directly on military and intelligence adoption.

The U.S. model therefore combines strong technical capacity with executive volatility. Agency-level AI safeguards may be sophisticated, but many are policy-based rather than statutory. Oversight occurs through congressional intelligence committees, inspectors general, the Foreign Intelligence Surveillance Court, privacy and civil liberties offices, and internal compliance mechanisms. However, classified AI systems may remain difficult for external actors to evaluate, especially when model performance, training data, or vendor contracts are not transparent.

The United Kingdom has a more consolidated surveillance-law regime. The Investigatory Powers Act 2016 governs interception, equipment interference, communications data acquisition, bulk powers, and oversight mechanisms. It introduced safeguards such as the "double lock" model, involving ministerial authorization and approval by a Judicial Commissioner for certain warrants. The Investigatory Powers Commissioner's Office oversees the use of investigatory powers, while the Intelligence and Security Committee of Parliament scrutinizes intelligence agencies. This structure is valuable for AI governance because it already contains mechanisms for classified review. However, the UK still lacks a comprehensive AI-specific framework for intelligence systems. Existing warrant and oversight models must therefore be adapted to evaluate algorithmic tools, not only human decisions to collect or intercept data.

Israel represents a different model. It is a technologically advanced security state with strong AI innovation capacity and high exposure to terrorism, cyber threats, and regional military conflict. Israel's 2023 AI regulation and ethics policy emphasizes responsible innovation, sectoral regulation, and risk management. However, the public legal framework for intelligence AI remains less transparent than in the EU or UK. This is partly a function of Israel's security environment and partly a feature of institutional design. The Israeli case illustrates a broader challenge: democracies facing acute security threats may prioritize operational flexibility, but this makes independent oversight even more important.

Table 2. Comparative regulatory approaches to AI in intelligence and security services: the European Union, the United States, the United Kingdom, and Israel

| Jurisdiction | Regulatory model | Strength | Weakness |
|---|---|---|---|
| EU | Horizontal AI Act plus data protection law | Strong rights-based framework | National security exclusions and enforcement complexity |
| United States | Executive policy, agency guidance, courts, congressional oversight | Technical sophistication and agency frameworks | Policy volatility and fragmented statutory basis |
| United Kingdom | Surveillance statute with commissioners and parliamentary oversight | Mature warrant and review architecture | Limited AI-specific legal standards |
| Israel | Sectoral AI policy and security-driven governance | Innovation capacity and operational integration | Lower public transparency in intelligence AI |

Across these models, the central regulatory gap is not the absence of principles. Lawfulness, accountability, transparency, fairness, reliability, and human oversight appear repeatedly in AI governance instruments. The gap is operationalization. Intelligence agencies need procedures that translate principles

into authorization thresholds, logs, audit trails, bias testing, red-team evaluations, procurement conditions, and reviewable records.

## 5. ETHICAL CHALLENGES

The first ethical challenge is bias and discrimination. AI systems learn from data generated by unequal societies and institutions. In policing and intelligence, historical data often reflect enforcement priorities, surveillance patterns, reporting biases, and political decisions. If such data are used to train predictive models, the system may treat past suspicion as evidence of future risk. Barocas and Selbst (2016) describe how data-driven systems can produce disparate impact even without explicit discriminatory intent. Selbst et al. (2019) further argue that fairness cannot be solved by technical metrics alone because AI systems operate within socio-technical contexts.

The second challenge is accountability. Intelligence work already involves secrecy and compartmentalization. AI can multiply this opacity. When an analyst acts on a model output, responsibility may be distributed among software developers, data engineers, procurement officers, commanders, analysts, and legal advisers. Kroll et al. (2017) argue that algorithmic accountability requires mechanisms beyond simple transparency, including technical design choices that allow systems to be tested and governed. In intelligence, this means that every consequential AI output should be traceable to a system version, dataset, operational purpose, authorization, and human decision-maker.

The third challenge is privacy. AI makes it possible to infer sensitive facts from apparently ordinary data. Location patterns, online behaviour, metadata, and social networks can reveal religion, political views, health conditions, intimate relationships, or professional associations. The OHCHR has warned that AI-enabled profiling and automated decision-making can seriously affect the right to privacy and associated rights. For intelligence services, the ethical issue is not only whether data were lawfully obtained, but whether AI use changes the nature of the intrusion. A dataset collected for one purpose may become far more intrusive when combined with other datasets and analysed by machine learning systems.

The fourth challenge is mission creep. Security tools introduced for exceptional threats often migrate into ordinary governance. Facial recognition deployed for counterterrorism may later be used for public order, immigration enforcement, or minor criminal investigations. Predictive analytics designed for national security may be repurposed for welfare fraud detection or protest monitoring. Lyon (2018) describes surveillance as a cultural and institutional process, not merely a set of devices. AI intensifies this process because the marginal cost of reusing models and datasets is low.

The fifth challenge is explainability. Some AI models produce outputs that cannot be easily explained in legal or operational terms. Intelligence agencies may not need full public transparency, but they do need reviewability. An oversight body should be able to ask why a person was flagged, what variables mattered, whether protected characteristics were directly or indirectly used, what error rates apply, and whether the model was valid for the relevant population. Wachter et al. (2017) argue that explanations must be meaningful to affected persons and institutions, not merely technical descriptions of code.

The sixth challenge is automation bias. Analysts and commanders may over-trust AI outputs, especially when systems are presented as objective or statistically advanced. In high-pressure security environments, speed can become a substitute for judgment. AI should support human reasoning, not replace it in decisions that affect liberty, life, reputation, or political rights. Human-in-the-loop governance is insufficient if the human merely rubber-stamps machine output. The relevant standard should be meaningful human responsibility.

## 6. DEMOCRATIC OVERSIGHT MECHANISMS

Democratic oversight of intelligence traditionally combines parliamentary, judicial, executive, and independent review. AI does not replace these mechanisms, but it requires them to evolve.

Parliamentary oversight provides democratic legitimacy. Committees can review budgets, mandates, legal authorities, strategic priorities, and major failures. The UK Intelligence and Security Committee and U.S. congressional intelligence committees illustrate this function. However, parliamentary bodies often lack technical capacity and depend on information supplied by the agencies they oversee. For AI governance, parliamentary oversight should include access to independent technical advisers, classified AI inventories, procurement contracts, and aggregate performance metrics.

Judicial oversight is essential where surveillance interferes with rights. Courts or judicial commissioners can authorize intrusive powers, assess necessity and proportionality, and review complaints. The U.S. Foreign Intelligence Surveillance Court and the UK double-lock warrant system provide examples of judicialized intelligence control. Yet AI creates new questions for judicial review. A judge may authorize interception, but not know that AI tools will later search, score, or correlate the collected data in ways that expand the intrusion. Warrants should therefore specify not only collection powers but also AI-enabled processing when such processing materially changes the risk to rights.

Independent oversight bodies are especially important because they can combine continuity, expertise, and classified access. Inspectors general, data protection authorities, privacy commissioners, and investigatory powers commissioners can examine internal systems more deeply than parliaments or courts. The challenge is technical capacity. Oversight bodies need staff who understand model validation, dataset bias, cybersecurity, adversarial manipulation, and audit logs. Without this capacity, oversight risks becoming formal rather than substantive.

Internal agency governance also matters. Democratic control does not occur only outside security services. Intelligence agencies should maintain AI review boards, legal compliance units, model risk committees, red teams, and ethics officers. However, internal governance cannot substitute for external oversight. It should generate the records and technical evidence that external bodies can inspect.

Civil society and media oversight are limited in intelligence contexts because secrecy is unavoidable. Still, investigative journalism, academic research, strategic litigation, and NGO reports often reveal abuses or governance gaps. Privacy International, Amnesty International, and other organizations have played a significant role in identifying the risks of surveillance technologies. Democratic systems should protect responsible disclosure and avoid using secrecy to shield unlawful or unethical AI practices.

The most effective model is layered oversight. No single institution can govern AI in intelligence. Parliaments can authorize and scrutinize; courts can approve intrusive powers; independent bodies can audit; internal units can manage risk; civil society can challenge public failures. AI governance should connect these layers through documentation, reporting duties, and escalation procedures.

## 7. THE SECURITY–OVERSIGHT BALANCE FRAMEWORK

The Security–Oversight Balance framework is designed to help democratic states evaluate AI uses in intelligence and security services. It rests on a simple premise: the level of oversight should increase with both operational intensity and rights intrusiveness. A low-risk translation tool used by analysts does not require the same controls as a biometric identification system deployed in public space. A predictive model used for strategic assessment does not require the same controls as a model that nominates individuals for coercive action.

The framework has four dimensions.

The first dimension is legal authorization. Each AI use should have a clear legal basis, defined operational purpose, authorized user group, data source limits, retention rules, and review procedure. National security secrecy may justify withholding information from the public, but it should not justify legal ambiguity. If an AI system changes the practical scope of a surveillance power, the authorization should reflect that change.

The second dimension is technical auditability. AI systems used in intelligence should generate records that allow later review. These include model version, training and validation data summaries, known limitations, performance metrics, bias testing, prompts or queries where relevant, output logs, human interventions, and override decisions. Technical auditability does not require publishing classified models. It requires making systems inspectable by authorized oversight bodies.

The third dimension is managerial accountability. Every consequential AI use should have an accountable human owner. Agencies should define who approved the system, who validated it, who may use it, who monitors performance, and who is responsible when harm occurs. Calo and Citron (2021) warn that automation can undermine the legitimacy of administrative action when agencies outsource or obscure judgment. Intelligence agencies must therefore avoid "the model decided" reasoning. AI may inform decisions, but it should not become an institutional shield.

The fourth dimension is ethical proportionality. AI use should be evaluated by necessity, suitability, proportionality, discrimination risk, and reversibility. The more difficult it is for affected persons to know, challenge, or correct an AI-generated consequence, the stronger the ex ante safeguards must be. Ethical proportionality also requires attention to group harms. A community may be disproportionately surveilled even if no single individual can prove a rights violation.

Table 3. The Security–Oversight Balance framework: four oversight tiers for AI use.

| Tier | AI use | Required safeguards |
|---|---|---|
| Tier 1: Administrative support | Translation, summarization, document search | Internal validation, user training, data security |
| Tier 2: Analytic support | OSINT clustering, cyber anomaly detection, strategic forecasting | Model logs, analyst verification, periodic audit |
| Tier 3: Person-affecting support | Watchlist support, biometric search, risk scoring | Legal authorization, bias testing, independent review, human justification |
| Tier 4: Coercive or operational action support | Targeting, arrest prioritization, intrusive surveillance triggers | Prior authorization, strict necessity test, technical audit, post-operation review |

The value of the SOB framework is that it avoids two extremes. It does not prohibit all AI in intelligence, which would be unrealistic and potentially harmful to democratic security. It also rejects unrestricted technological adoption, which would erode legitimacy. The framework treats oversight as a design requirement. AI systems should be built from the beginning to be reviewable, contestable where possible, and accountable at institutional level.

## 8. POLICY RECOMMENDATIONS

First, legislatures should require classified AI registers for intelligence and security services. These registers should list AI systems, operational purposes, legal bases, data categories, vendors, risk tiers, and responsible officials. Public disclosure may be limited, but parliamentary and independent oversight bodies should have access to the full register.

Second, warrants and authorizations should address AI-enabled processing. If AI materially expands the ability to search, correlate, identify, or predict from collected data, this should be treated as a distinct rights-relevant step. Judicial or commissioner approval should not be limited to the initial act of collection.

Third, intelligence agencies should establish AI assurance units. These units should test models before deployment, monitor drift, conduct bias and robustness evaluations, review incidents, and maintain audit records. They should include legal, technical, operational, and ethics expertise.

Fourth, procurement contracts should include audit rights. Governments should not purchase black-box systems that cannot be inspected by authorized public bodies. Vendors should be required to provide

documentation, performance evidence, cybersecurity assurances, and information on training data limitations.

Fifth, human accountability should be mandatory for consequential decisions. AI outputs should not be sufficient grounds for watchlisting, arrest, targeting, intrusive surveillance, or adverse administrative action. Human decision-makers should record their reasoning when relying on AI outputs.

Sixth, NATO and the EU should develop minimum standards for AI in intelligence cooperation. Intelligence sharing increasingly involves shared platforms and interoperable systems. If one partner uses weakly governed AI outputs, the risk may spread across alliances. Minimum standards should include auditability, proportionality, reliability, and bias mitigation.

Seventh, oversight bodies need technical capacity. Parliamentary committees, courts, commissioners, and inspectors general should be supported by independent AI experts with security clearances. Without technical expertise, oversight cannot evaluate whether AI systems actually perform as claimed.

## 9. CONCLUSIONS

AI is transforming intelligence and security services by increasing the speed, scale, and predictive ambition of state security operations. These capabilities can strengthen democratic resilience against terrorism, cyberattacks, hostile intelligence activity, organized crime, and foreign interference. Yet they can also intensify surveillance, reproduce discrimination, obscure responsibility, and weaken the rule of law.

The answer to the research question is that democratic states can operationalize legitimate control over AI in intelligence only by making oversight continuous, technical, and risk-sensitive. Traditional legal authorization remains necessary, but it is no longer sufficient. Oversight must extend into datasets, models, procurement, validation, deployment, human-machine interaction, and post-operation review.

The proposed Security–Oversight Balance framework offers one way to structure this process. It links legal authorization, technical auditability, managerial accountability, and ethical proportionality. Its central principle is proportional governance: the more intrusive and operationally consequential the AI system, the stronger the oversight requirements must be.

The article has limitations. It relies on publicly available materials and cannot evaluate classified deployments directly. It also focuses on democratic and democratic-allied systems, leaving authoritarian AI surveillance for separate study. Future research should examine how oversight bodies actually evaluate AI systems in practice, how classified technical audits can be designed, and how international intelligence cooperation can prevent rights laundering through less regulated partners.

Democratic oversight should not be seen as a burden on intelligence effectiveness. In the long term, legitimacy is a security asset. AI systems that cannot be explained, audited, or controlled may produce short-term operational gains, but they create strategic risks: public distrust, legal challenge, diplomatic friction, and institutional overreach. The task for democratic states is not to choose between security and oversight, but to design intelligence AI so that security remains accountable to democracy.

**AI Use Declaration.** *This article was originally written by the author in Ukrainian. AI-based tools were used to assist in translating the manuscript into English, in language editing and proofreading of the translated text, and in restructuring and reorganizing the material to meet the journal's requirements. The author reviewed and revised the resulting text, verified all sources and citations against the original materials, and confirms that the research, analysis, and conclusions presented are entirely the author's own. The author takes full responsibility for the accuracy, originality, and integrity of the final text.*

# REFERENCES

Amoore, L. (2020). Cloud ethics: Algorithms and the attributes of ourselves and others. Duke University Press.

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. California Law Review, 104(3), 671–732.

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review, 82*(5), 977–1008. https://doi.org/10.1177/0003122417725865

Brayne, S. (2021). Predict and surveil: Data, discretion, and the future of policing. Oxford University Press.

Brayne, S., & Christin, A. (2021). Technologies of crime prediction: The reception of algorithms in policing and criminal courts. Social Problems, 68(3), 608–624.

Browne, T. O., Abedin, M., & Chowdhury, M. J. M. (2024). A systematic review on research utilising artificial intelligence for open source intelligence applications. *International Journal of Information Security*, 23(4), 2911–2938. https://doi.org/10.1007/s10207-024-00868-2

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 77–91.

Calo, R., & Citron, D. K. (2021). The automated administrative state: A crisis of legitimacy. Emory Law Journal, 70(4), 797–846.

Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. Washington Law Review, 89(1), 1–34.

Council of Europe. (2018). Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Council of Europe.

Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. Council of Europe.

Deibert, R. J. (2023). Subversion Inc.: The age of private spycraft. MIT Press.

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union.

European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. Official Journal of the European Union.

Feldstein, S. (2021). The rise of digital repression: How technology is reshaping power, politics, and resistance. Oxford University Press.

Ferguson, A. G. (2017). The rise of big data policing: Surveillance, race, and the future of law enforcement. New York University Press.

Gill, P., & Phythian, M. (2018). Intelligence in an insecure world (3rd ed.). Polity Press.

Hildebrandt, M. (2015). Smart technologies and the end(s) of law: Novel entanglements of law and technology. Edward Elgar.

Investigatory Powers Act 2016, c. 25. (UK).

Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. University of Pennsylvania Law Review, 165(3), 633–705.

Leslie, D., Burr, C., Aitken, M., Katell, M., Briggs, M., & Rincon, C. (2022). Human rights, democracy, and the rule of law assurance framework for AI systems: A proposal. The Alan Turing Institute.

Lyon, D. (2018). The culture of surveillance: Watching as a way of life. Polity Press.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society, 3*(2), 1–21. https://doi.org/10.1177/2053951716679679

National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

North Atlantic Treaty Organization. (2021). Summary of the NATO Artificial Intelligence Strategy. NATO.

North Atlantic Treaty Organization. (2024). Summary of NATO's revised Artificial Intelligence Strategy. NATO.

Office of the Director of National Intelligence. (2020a). Principles of artificial intelligence ethics for the intelligence community. ODNI.

Office of the Director of National Intelligence. (2020b). Artificial intelligence ethics framework for the intelligence community. ODNI.

Office of Management and Budget. (2025). Memorandum M-25-21: Accelerating federal use of AI through innovation, governance, and public trust. Executive Office of the President.

O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown.

Organisation for Economic Co-operation and Development. (2024). OECD AI principles. OECD.

Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.

Privacy International. (2014). Who's watching the watchers? A comparative study of intelligence organisations oversight mechanisms. Privacy International.

President of the United States. (2025). Executive Order 14179: Removing barriers to American leadership in artificial intelligence. The White House.

President of the United States. (2026). National Security Presidential Memorandum/NSPM-11: Artificial intelligence in the national security enterprise. The White House.

Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 59–68. https://doi.org/10.1145/3287560.3287598

Slobogin, C., & Brayne, S. (2023). Surveillance technologies and constitutional law. Annual Review of Criminology, 6, 219–240.

UNESCO. (2021). Recommendation on the ethics of artificial intelligence. UNESCO.

United Nations High Commissioner for Human Rights. (2021). The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights (A/HRC/48/31). United Nations.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law, 7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005

White House. (2025). America's AI Action Plan. Executive Office of the President.

**POLITICS & SECURITY**
ISSN 2815-3324 Online, ISSN 2535-0358 Print

# PARLIAMENTARY INTELLIGENCE OVERSIGHT AND THE CHALLENGES OF ENHANCED EU INFORMATION SHARING: THE CASE OF BULGARIA

Nelly Bencheva
Department of Economic Security and Management
Academy of National and Information Security
Plovdiv, Bulgaria
https://orcid.org/0000-0001-7579-7323
n.bencheva@anis.bg

**Abstract.** *Global trends and the ongoing dynamic processes of trans-border security threats necessitate an unprecedented intensification of intelligence sharing among European Union (EU) Member States, which also reflects on the strengthening of parliamentary oversight of intelligence services. These changes require the application of an integral approach to understanding potential risks and threats, in order to increase awareness and the effectiveness of parliamentary control over intelligence agencies. On one hand, enhanced cooperation in information exchange within the EU strengthens collective security, but simultaneously creates significant difficulties regarding the control and accountability of national intelligence services and institutions. This study demonstrates that overcoming these gaps can largely be achieved by increasing their effective monitoring and parliamentary oversight. This article aims to explore the models of parliamentary intelligence oversight and reveal the challenges they face under the conditions of intensive information exchange within the EU. A special focus is placed on Bulgarian parliamentary practice and its institutional framework. Through the case of Bulgaria, the article examines and reveals the paradoxes of parliamentary control in light of international obligations and requirements for democratic transparency. The research results indicate that current oversight models lag behind the networked nature of contemporary intelligence cooperation. Proposals are made to strengthen inter-parliamentary cooperation within the EU through information-sharing agreements.*

**Keywords:** parliamentary control, intelligence oversight, national security, information sharing, democratic accountability European Union, Bulgaria.

## 1. INTRODUCTION

Over the past decade, security and intelligence cooperation within the EU has undergone a fundamental transformation. European security and intelligence are facing serious challenges from emerging risks and threats. These ongoing changes require the application of an integral approach to understanding potential risks and threats, increasing the effectiveness of oversight, and strengthening the exchange of intelligence information.

The issue of intensive intelligence sharing and parliamentary oversight of intelligence has become exceptionally topical due to several key reasons:

The rise of hybrid threats, transnational terrorism, and complex cyberattacks has forced EU member states to shift from "traditional isolationism" toward a model of "intelligence pluralism". This transformation in information sharing has outpaced the legal and institutional frameworks designed to ensure democratic accountability. Within the EU, the process of networking intelligence operations is increasingly accelerating, yet at the national level, their oversight remains fragmented. This has led to the emergence of a so-called "accountability gap". Consequently, shared intelligence often remains beyond the reach of national parliamentary committees, largely due to strict protocols regarding secrecy.

Accelerated technological progress and expanded capabilities for surveillance and control. Digital and information technologies provide intelligence services with vast opportunities for obtaining, processing, analyzing, and transmitting information (Stankov, V. H. 2025a, p. 161-180). The introduction of artificial intelligence allows for the rapid processing and analysis of large databases while ensuring more secure protection.

Democracy, transparency, and the protection of civil rights and liberties. Security in contemporary society is predicated upon democratic values, fundamental rights and freedoms, and equal opportunities for personal development (Updated National Security Strategy of the Republic of Bulgaria, 2018). There is an increasing demand for transparency and accountability across all state institutions within the national security sector. The activities of intelligence services must comply with legal frameworks and constitutional principles (Stankov, V. H. 2024, p. 110-114). Democratic societies increasingly call for security sector reforms that ensure greater transparency, accountability, and the effective operation of intelligence agencies.

International cooperation and interaction within the EU, along with the necessity of intelligence sharing, are increasing (Georgiev, V. 2025, p. 58-63). The escalation of global threats objectively necessitates closer international cooperation and synergy between intelligence services, as well as an intensified exchange of intelligence information. This places new demands on national legislatures for the oversight and accountability of intelligence agencies and institutions.

In this context, Bulgaria presents a compelling case study. As an EU frontier state and a relatively new member of the Schengen Area, the country is integrated into European standards and the EU security architecture. Nevertheless, the Bulgarian Parliament faces significant structural and political challenges in overseeing the manner in which national agencies process and protect shared intelligence.

This article aims to examine the model of parliamentary intelligence oversight by identifying the fundamental challenges arising from the intensification of information exchange within the EU, with a specific focus on Bulgarian parliamentary practice. The research thesis posits that the effectiveness of parliamentary control and intelligence accountability is of key importance for strengthening the role of intelligence sharing in the EU, as well as for modernizing the mechanisms of parliamentary oversight and the democratic accountability of intelligence services.

## 2. MATERIALS AND METHODS

The research methodology is aligned with its objective and the supported research thesis. In the course of the study, an interdisciplinary approach is applied, combining the legal framework with institutional analysis.

The methodology is structured around three primary pillars:

- Comparative Analysis: An examination of the EU legal framework (specifically the Treaty on European Union and relevant regulations, such as Regulation (EU) 2022/991 of the European Parliament and of the Council regarding Europol (Regulation (EU) 2022/991 of the European Parliament and of the Council, 2022 ) cooperation, the European Security Strategy (European Security Strategy, 2009) and the NATO Strategic Concept (NATO Strategic Concept, 2022)), alongside Bulgarian national legislation (the Constitution, statutes, the Law on the Management and Functioning of the National Security System (Management and Functioning of the National Security Protection System Act, 2015), sub-legislative acts, the Rules of Organization and Procedure of the National Assembly (Rules of Organization and Procedure of the National Assembly, 2017), parliamentary documents, minutes, resolutions, strategic, and international documents); comparative analysis (comparison of intelligence oversight models within the EU); legal analysis (normative analysis of legislation, analysis of case law, and comparative legal research); systems analysis (revealing the links, relations, and interactions between the elements of the legislative and intelligence systems).

- Case Study Analysis: A focused study of the Bulgarian parliamentary committee for the oversight of security services. This includes a review of public annual reports on the state of national security, legislative debates, and institutional interactions, aimed at identifying practical difficulties and barriers to parliamentary oversight, as well as obstacles to the international exchange of intelligence.
- Qualitative Analysis: An evaluation of the "third-party rule" and its application within EU intelligence-sharing networks. The study assesses the relationship between the "need-to-know" principle (operational effectiveness) and the "need-to-control" principle (democratic accountability).

The application of these research methods and approaches allows for an examination of the systemic gaps in parliamentary oversight, enabling the identification of key challenges within the EU information exchange process and the formulation of evidence-based recommendations for reform.

## 3. LEGISLATIVE OVERSIGHT OF INTELLIGENCE IN THE EUROPEAN UNION

Legislative oversight of intelligence within the EU does not adhere to a single, unified model. Each Member State maintains its own distinct system (Bakalov Y.I., Bahchevanov G. 2025, p. 37-50), the architecture of which is built upon the national Constitution, legal system, and political culture. Despite the absence of a uniform model, there are common principles and approaches within the EU, which include:

National Responsibility: The primary responsibility for overseeing national intelligence services lies with the parliaments of the respective Member States. In most EU countries, specialized parliamentary committees are established for intelligence oversight. Generally, these committees possess mandates in three key areas: legislative (defining the mandate and legal framework of the services); budgetary (approving and monitoring funding); and oversight (reviewing reports and investigating instances of violations of fundamental rights and duties).

Shared Responsibility: There exists an effective mechanism for democratic oversight based on the principle of shared responsibility among the legislative, judicial, and executive branches.

Legal Framework: Each Member State establishes a clear and comprehensive legal framework that defines the mandate and powers of the intelligence services while guaranteeing the fundamental rights of citizens.

International Parliamentary Cooperation and Oversight within the EU (Wills, A., & Vermeulen, M. 2011, p. 64-67): There is an intensifying cooperation between national services and EU bodies, aimed at establishing more effective oversight at the European level and coordination among individual services. Due to growing asymmetric threats, the radicalization of terrorist activities, organized crime, and the potential use of nuclear weapons, special attention must be paid to strengthening cooperation and oversight of information exchange among the intelligence services and institutions of Southeast European countries (Bakalov, Y. I. 2022, p. 10-41). In this regard, analysis indicates that countries in this region, which have recently transitioned from totalitarian regimes to democracy, require a reformation of their intelligence oversight models. Of particular importance is the necessity to implement contemporary parliamentary control mechanisms and instruments equivalent to those applied in EU member states with established democratic systems. This facilitates the creation of a legal framework that allows intelligence services to evolve into modern structures for policy implementation and intelligence sharing, thereby strengthening security and the protection of civil society.

Diversity of Approaches: The European Union Agency for Fundamental Rights (FRA) (European Union Agency for Fundamental Rights, 2024) distinguishes five different models of oversight frameworks across the Member States, reflecting a wide variety of approaches. These diverse models include specialized parliamentary committees composed of members from different parliamentary groups. For instance, such committees are established within the Parliaments of Bulgaria and Germany. Some models incorporate expert bodies appointed by Parliament, which may include external experts or members of

the judiciary. Belgium and the Netherlands serve as prominent examples of this approach. Furthermore, hybrid models exist, representing a combination of parliamentarians and independent experts.

Specialized Bodies: Within national parliaments, specialized parliamentary committees are established for the purpose of oversight. These committees include experts who are granted the requisite authorization for access to classified information.

Although the European Parliament lacks direct powers to oversee national intelligence services, it exercises oversight over EU agencies with intelligence-related functions, such as Europol, Frontex, and EU INTCEN. The Committee on Civil Liberties, Justice and Home Affairs (LIBE) (Activity report, 2019-2024) operates within the European Parliament, primarily monitoring the protection of citizens' fundamental rights and data privacy. Intelligence agencies are mandated to provide information to Members of the European Parliament (MEPs) through briefings and various hearing formats, subject to appropriate security clearances.

Horizontal and technological oversight is expected to be strengthened, with the legislative framework focusing on emerging threats. The Artificial Intelligence Act (AI Act) is slated to become operational starting in 2026. This is necessitated by the fact that AI systems are increasingly categorized as high-risk. Consequently, there are growing requirements for transparency regarding the utilization of these systems by public authorities.

With respect to data protection, EU legislation imposes specific directives on law enforcement authorities to ensure rigorous oversight of the manner in which agencies process personal data. Furthermore, the establishment of a European Intelligence Unit, to be led by the European Commission, is currently under discussion. The objective is to achieve enhanced coordination and a more robust analysis of threats.

In international intelligence cooperation within the EU, the "third-party rule" (European Union Agency for Fundamental Rights, 2017) is established as a fundamental principle. According to this rule, intelligence information received from a partner country cannot be shared with a third party without prior negotiation and the explicit consent of the original source. From the perspective of democratic oversight, this rule limits the ability of parliamentary committees to verify information obtained from foreign services (Born, H. and Leigh, I., 2005). To overcome these constraints, international intelligence cooperation is most frequently based on agreements that focus on thematic data and specific techniques. This primarily pertains to operational cooperation, the exchange of classified information, and coordinated actions in the fight against terrorism, among others.

Information exchange and cooperation are becoming increasingly imperative in the field of cybersecurity (FRA, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, 2017). For this reason, EU Member States are paying special attention to cybersecurity and defense. Legislative priorities in these areas focus on strengthening European defense and security through closer cooperation and new legislative measures and initiatives.

With a view to achieving a higher level of cybersecurity within the EU, Bulgaria has undertaken legislative measures in alignment with the European NIS 2 Directive (Directive (EU) 2022/2555) (Directive (EU) 2022/2555 of the European Parliament,2022). These measures are being implemented through extensive amendments to the Cybersecurity Act (Cybersecurity Act, 2026). New standards are being introduced in four primary areas: risk management, whereby business organizations are mandated to develop programs featuring specific organizational and technical measures and oversight policies; incident reporting, involving rigorous control through a three-stage model for notifying authorities in the event of cyber threats and incidents; and corporate accountability, where the management of business entities bears personal responsibility for the adoption and monitoring of measures aimed at achieving cyber resilience. These legislative changes aim to ensure Bulgaria’s sustainable integration into the pan-European framework for information exchange and the protection of network and information environments.

ISSN 2815-3324 Online, ISSN 2535-0358 Print

## 4. PARLIAMENTARY OVERSIGHT OF INTELLIGENCE IN BULGARIA

An integral part of the national security and intelligence system in Bulgaria is the question of the current model of oversight and accountability. Figure 1 presents a graphical model of the system for the control and protection of national security and intelligence. Each of the elements within the system possesses its own legally defined powers, activities, and accountability mechanisms, which ensures the fulfillment of national security and intelligence protection functions. In view of achieving the research objective, we provide a more detailed analysis of the mechanisms and instruments for intelligence oversight exercised by the legislative branch.

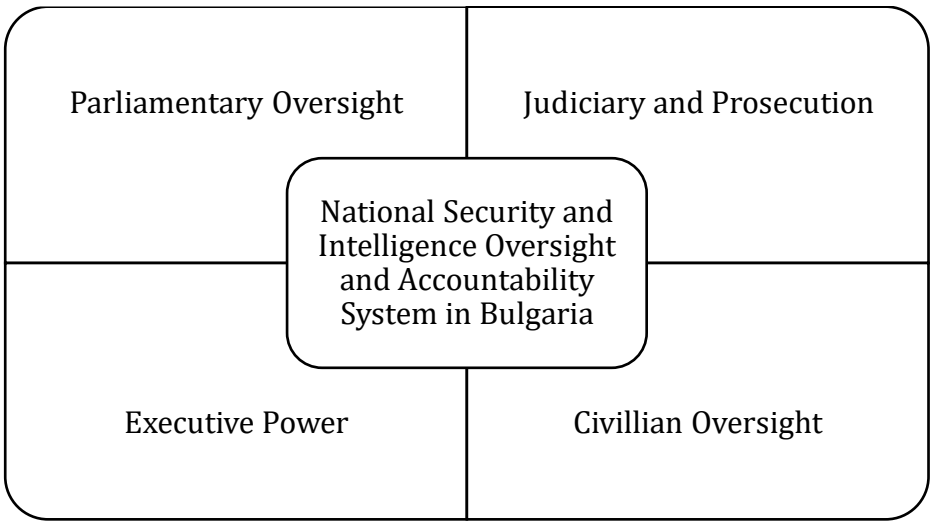



Figure 1. The national security and intelligence oversight and accountability system in Bulgaria

The legislative power in the Republic of Bulgaria is vested in the National Assembly. The National Assembly also exercises parliamentary oversight (Art. 62. (1) Constitution of the Republic of Bulgaria, 1991). The parliamentary oversight of intelligence services and structures constitutes a vital component of the democratic system of control and accountability. This oversight is conducted by Parliament through specialized mechanisms and instruments, the primary aim and objective of which are to regulate the legality of the activities and functions of intelligence services in carrying out the intelligence process, while strictly adhering to the principles of national security.

Legislative authority and the oversight of intelligence services are exercised on the basis of constitutional principles, the separation of powers, and parliamentary democracy.

Article 105 of the Constitution stipulates the powers of the Council of Ministers in the field of national security and subjects it to parliamentary oversight (Art. 105. (1) Constitution of the Republic of Bulgaria, 1991).

The oversight of intelligence services is of pivotal importance for maintaining a balance between conducting effective intelligence operations and ensuring the protection of democratic principles, as well as the rights and freedoms of civil society (Stankov, V. H. 2025b, p. 13-18).

In the sphere of security and intelligence, democratic oversight serves as a fundamental principle of the rule of law. It acts as a reliable guarantee that national security and intelligence agencies operate within legally established regulations, rules, and procedures.

For Bulgaria, amid escalating threats from military conflicts, terrorism, extremism, migratory pressure, and instability, legislative oversight of the intelligence services acquires particular significance for building public trust and confidence within civil society.

The model of parliamentary oversight mechanisms includes a specialized standing Committee on Oversight of the Security Services, the Application and Use of Special Intelligence Means, and the Access to Data under the Electronic Communications Act.

The activities of the Committee are conducted in accordance with the Constitution, the Rules of Organization and Procedure of the National Assembly, and the prevailing legislation (Committee on Oversight of the Security Services, 2017). The Committee exercises parliamentary oversight over the operations of the security services. This oversight pertains to the protection of classified information, the safeguarding of citizens' rights and freedoms, and the prevention of the unlawful use of special intelligence means and unauthorized access to data under the Electronic Communications Act. The Committee drafts reports, proposals, and opinions, and adopts positions regarding the annual reports and budgets of the security services.

Parliamentary oversight in Bulgaria encompasses several key institutions. The State Agency for National Security (SANS) conducts intelligence activities aimed at preventing, intercepting, and neutralizing threats and risks to national security. It provides the necessary intelligence information to support executive decision-making within the scope of national security.

The State Intelligence Agency (SIA) is directly subordinated to the Council of Ministers. This agency acquires, analyzes, and provides intelligence to the highest state authorities, as well as to government bodies with the relevant competence regarding the identification and prevention of risks and threats to national security.

Parliamentary oversight of the SIA's activities is exercised by the National Assembly through the standing Committee on Security, by means of monitoring and controlling its operations. However, the Committee does not have access to information regarding specific intelligence operations, nor to data concerning the Agency's employees or cooperating individuals. Furthermore, access to classified information is restricted during the performance of oversight activities concerning the Agency’s operations.

The specialized body for military intelligence in Bulgaria is the Military Intelligence Service. The Service organizes and conducts effective tactical and strategic intelligence, utilizing both technical and human resources to provide information support for the activities of state institutions in the field of national security and defense. Additionally, there are five other structures within the Ministry of Interior that acquire and utilize intelligence information to ensure public order and internal security.

The analysis of the model of legislative oversight and accountability of intelligence in Bulgaria indicates that there are untapped opportunities for its development and refinement. This includes moving toward closer cooperation and interaction among all institutions, bodies, and structures involved in the acquisition and use of intelligence, with the aim of increasing the efficiency and coordination of the intelligence process in Bulgaria.

The consolidation of the intelligence community, along with the legal regulation of the legislative oversight and accountability model over the intelligence process and the activities of intelligence services, is fundamental to the implementation of effective and efficient control over intelligence information for the protection of the national security system.

## 5. CHALLENGES TO PARLIAMENTARY OVERSIGHT ARISING FROM THE INTENSIFICATION OF INTELLIGENCE SHARING

The model of the parliamentary oversight and accountability system should reflect the fundamental values and legal principles inherent to intelligence and security. This is where one of the primary paradoxes of the legislative oversight model emerges: how to effectively oversee intelligence services and institutions whose efficacy is intrinsically linked to intelligence information that is, to a large extent, strictly confidential or classified (Annex No. 1 to Art. 25 of the Protection of Classified Information Act, 2002). In the context of escalating threats from military conflicts and terrorism, it becomes increasingly important to reconceptualize and refine the notion of security and the accessibility of intelligence, viewed through the prism of effective parliamentary control and accountability.

There is a growing critical importance in seeking and developing new opportunities for greater transparency, oversight, and accountability. Insufficient transparency and weak oversight may signal a lowering of requirements for the efficient utilization of the intelligence services' limited resources or indicate an increase in excessive political or economic influence over them. A risk exists regarding the curtailment of democratic oversight and accountability, particularly within the current rapidly changing security environment.

The dynamic shifts within the security environment pose a significant challenge to effective parliamentary oversight. The vast array of emerging issues and problems within the intelligence system—and their resolution through reliance on the regulatory framework, ordinances, rules, and practices of secrecy and information classification—impedes the work of members of parliament. In this regard, it is necessary to increase the utilization of research, specialized expertise, and scientific findings, as well as to engage legal experts and strengthen international cooperation in the field of intelligence and security.

The analysis established that there is no single model of parliamentary oversight that is universally functional and applicable to all EU Member States. Significant diversity exists in the rules, practices, and mandates of national parliaments. The challenge of strengthening parliamentary oversight over the intelligence and security sector serves as a catalyst for seeking greater alignment between the role of Parliament and national security policy, ensuring it meets the needs of civil society and the protection of national sovereignty.

A major challenge to achieving effective parliamentary oversight is the issue of "information asymmetry ". This can be defined as a classic paradox: while intelligence services acquire and possess comprehensive intelligence, members of parliament have access only to information provided to them in compliance with classified information protection requirements.

The established mechanisms for the application and use of special intelligence means, the acquisition of intelligence, and related violations by security services represent another significant challenge within the current model of legislative intelligence oversight. In this regard, a necessary balance must be sought to overcome the "secrecy-conflict "paradox. This paradox most frequently manifests during the processing and utilization of intelligence information. By definition, the legislative branch is public and transparent, whereas security services operate with both secret and classified information.

It is necessary to develop and implement effective mechanisms and instruments aimed at preventing information leaks. A particularly significant risk involves members of parliament, who are public figures working closely with journalists and representatives of the electronic media. In their interactions with the media, parliamentarians may be tempted to gain political dividends by sharing highly specialized information. Upon the identification of such violations, the application of appropriate legal sanctions is essential.

The contemporary, unprecedented challenges associated with hybrid threats, cyberattacks, and the use of artificial intelligence necessitate fundamental changes to the model of legislative intelligence oversight and accountability. Amendments to existing legislation should focus on the refinement and enhancement of administrative capacity.

Increasing the effectiveness of legislative oversight mechanisms and control entails a series of improvements, including new rules for the access and utilization of intelligence information, enhanced accountability and coordination, and the introduction of more effective sanctions.

## 6. CONCLUSION

A comparative analysis of the oversight and accountability models in the EU and Bulgaria demonstrates that the mechanisms and instruments for parliamentary intelligence oversight are an essential component of the broader process of European integration and cooperation among intelligence services. This aligns with best practices in the fields of democratic governance, control, and accountability.

The model of parliamentary intelligence oversight within the EU is diverse and characterized as decentralized. While each Member State maintains its own distinct system, they share a common commitment to ensuring oversight and democratic accountability in compliance with the rule of law.

The globalization of threats necessitates increasingly closer cooperation and the intensification of information exchange among the intelligence services of EU Member States. Consequently, this presents national parliaments with new challenges to strengthen and seek innovative forms of collective security and defense.

Within the framework of the legislative oversight model, security sector reforms are required to ensure a more comprehensive application of the principles of transparency, accountability, and efficiency of intelligence services, while simultaneously preserving their operational capabilities.

The European model of legislative intelligence oversight and accountability demands highly profound and precise work in the acquisition and utilization of intelligence information for the development of effective national security policies.

The applied European model is hybrid in nature, representing a synthesis of a direct democratic model at the national level and normative/budgetary oversight at the EU level over security and intelligence structures. This European model of legislative intelligence oversight facilitates a more efficient allocation of resources and improved management, enabling a swifter response to the dynamics of both internal and external threats.

The primary strengths of European intelligence oversight are manifested in the strong dominance of parliamentary control, robust judicial guarantees for order and legality, specialized institutions for security and the protection of civil society, as well as European integration, the harmonization of various security-related laws, and supranational oversight.

The model of oversight and accountability of the intelligence services in Bulgaria is a complex system of institutions, laws, regulatory acts, procedures, and mechanisms based on democratic principles and aligned with European security standards. A central role within this model is occupied by the specialized parliamentary Committee on Oversight of the Security Services, the Application and Use of Special Intelligence Means, and the Access to Data under the Electronic Communications Act. This parliamentary committee possesses clearly defined mandates and functions.

Despite the significant progress achieved in legislative oversight and accountability in Bulgaria, the analysis indicates that there remain untapped opportunities for more effective implementation of control within intelligence structures and institutions. Additional efforts are imperative to refine the oversight and accountability system in accordance with European standards and international best legislative practices.

The primary directions for the development and refinement of the legislative intelligence oversight and accountability system do not aim to diminish its strength or capabilities. Rather, they serve as a practical prerequisite for enhancing the democratic nature of oversight and accountability, as well as for the improved legitimation and representation of intelligence services' activities before civil society.

Within a democratic state governed by the rule of law, the strength of intelligence services does not imply opacity or a lack of accountability. The implementation of various instruments and mechanisms for the advancement of legislative oversight and accountability must contribute to the strengthening of institutional trust in the interest of civil society.

**AI Use Declaration.** *AI-based tools were used to assist with the translation and language editing of this article from the author's original Bulgarian manuscript into English. The author reviewed and revised the translated text, verified all sources and references against the primary materials, and confirms that the substantive content, analysis, and conclusions are the author's own. The author takes full responsibility for the accuracy, originality, and integrity of the final text.*

## REFERENCES

Activity report (2019-2024), LIBE, Committee on Civil Liberties, Justice and Home Affairs, https://www.europarl.europa.eu/cmsdata/285271/2019-2024%20LIBE%20Activity%20Report.pdf

Annex No. 1 to Art. 25 of the Protection of Classified Information Act (2002), lex.bg, https://www.lex.bg/laws/ldoc/2135448577

Bakalov, Y. I. (2022). Geopolitical Risks to the Security of Southeast Europe. Plovdiv: Publishing House VUSI, p. 58-72.

Bakalov, Y. I., & Bahchevanov, G. (2025). Yearbook (Vol. XXII, pp. 37–50). Academic Publishing House ANIS. https://www.anis.bg/wp-content/uploads/2026/04/Годишник-АНИС-2025.pdf

Born H., Leigh I. (2005). Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies. Oslo edition from http://www.procon.bg/node/3930

Committee on Oversight of Security Services, Special Intelligence Means and Access to Data under the Electronic Communications Act (2017), National Assembly of the Republic of Bulgaria, https://www.parliament.bg/bg/parliamentarycommittees/2596

Constitution of the Republic of Bulgaria (1991), Art. 105(1), https://www.parliament.bg/bg/const

Constitution of the Republic of Bulgaria (1991), Art. 62, https://www.parliament.bg/bg/const

Cybersecurity Act (2026). State Gazette, issue No. 17

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022, EUR-lex, https://eur-lex.europa.eu/eli/dir/2022/2555

European Security Strategy, (2009) https://www.consilium.europa.eu/media/30803/qc7809568bgc.pdf

European Union Agency for Fundamental Rights (2024), https://fra.europa.eu/en/publication/2025/consolidated-annual-activity-report-european-union-agency-fundamental-rights-2024

European Union Agency for Fundamental Rights. (2017). Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update. Publications Office of the European Union. https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu

Ivanov, M.M. (2020). Intelligence Infrastructure. Pleven: Publishing House "Nima ", 282 p.

Management and Functioning of the National Security Protection System Act (2015), lex.bg, https://www.lex.bg/bg/laws/ldoc/2136588572

NATO Strategic Concept (2022), https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf

Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices (2003), Inter-Parliamentary Union, Geneva Centre for the Democratic Control of Armed Forces. Geneva, https://www.files.ethz.ch/isn/129147/ipu_hb_bulgarian.pdf

Regulation (EU) 2022/991 of the European Parliament and of the Council (2022), EUR-lex, https://eur-lex.europa.eu/eli/reg/2022/991/oj

Rules of Organization and Procedure of the National Assembly (2017), National Assembly of the Republic of Bulgaria, https://www.parliament.bg/bg/rulesoftheorganisations

Stankov, V. H. (2024). Intelligence in the Security System. Plovdiv: Publishing Complex of VUSI, 110-114 p.

Stankov, V. H. (2025a). Intelligence through Technical Means. Plovdiv: Publishing Complex of VUSI, 161-180 p.

Stankov, V. H. (2025b). Control and Accountability in Intelligence. Plovdiv: Publishing Complex of VUSI, 204 p.

Updated National Security Strategy of the Republic of Bulgaria, Adopted by a Decision of the National Assembly on 14.03.2018, publ. State Gazette, issue 26 of 23.03.2018

Wills, A., & Vermeulen, M. (2011). Parliamentary Oversight of Security and Intelligence Agencies in the European Union. European Parliament, Directorate-General for Internal Policies, (64-67). https://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf

**POLITICS & SECURITY**
ISSN 2815-3324 Online, ISSN 2535-0358 Print

# STRATEGIC COMMUNICATIONS IN THE ARMED FORCES: CHALLENGES AND DEVELOPMENT PERSPECTIVES

Kateryna Tiazhkorob
Department of Publishing and Editing
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Kyiv, Ukraine
https://orcid.org/0009-0001-7215-0951
katushkajordison98@gmail.com

**Abstract.** *This article examines the theoretical and practical dimensions of strategic communications as an essential component of contemporary military operations. It explores the concept of strategic communications within the context of the armed forces, tracing its evolution and examining its role in strengthening national security. The study analyzes the core components of military strategic communications, including information and psychological influence, public affairs, civil-military cooperation, and operations in the information environment. It identifies the principal challenges to the effective implementation of strategic communications in the armed forces, including the absence of a unified doctrinal framework, insufficient personnel training, and the lack of a systematic approach to communication planning. Drawing upon the experience of NATO member states and the current practices of the Armed Forces of Ukraine, the article proposes key directions for improving the strategic communications system. Particular attention is devoted to the role of strategic communications in the context of hybrid warfare and information confrontation. The findings may serve as a basis for further reform of military communication structures, the development of doctrinal and policy documents, and the professional training of military communication specialists.*

**Keywords:** strategic communications; armed forces; hybrid warfare; information environment; national security.

## 1. INTRODUCTION

The transformation in the character of contemporary armed conflicts driven by the rapid development of digital technologies, the globalization of the information space, and the spread of network communications has led to a substantial revision of traditional approaches to ensuring a state's military security. In the twenty-first century, the achievement of military-political objectives increasingly depends not only on the application of military force but also on the ability to manage information flows effectively, shape favorable narratives, and counter destructive information influence (Gorbulin, 2017). Under these conditions, the information space is becoming a distinct theater of military operations, in which the struggle over the perception of events is often no less significant than direct armed confrontation. Against this background, strategic communication is acquiring particular importance as a comprehensive system for planning, coordinating, and implementing communicative activity aimed at achieving the strategic objectives of the state and its armed forces. Unlike traditional information measures, strategic communication entails the coordinated use of all available communication capabilities from public relations and civil-military cooperation to information and psychological operations in order to shape the necessary information environment and support military-political decision-making (Hallahan & Zerfass, 2015).

The relevance of research into strategic communication has grown substantially as a result of the spread of hybrid forms of warfare, in which information-psychological influence serves as one of the key instruments for achieving strategic advantage. The events connected with Russian aggression against Ukraine (beginning in 2014 and especially after the start of the full-scale invasion in 2022) have

demonstrated that the effectiveness of military action depends to a significant degree on a state's ability to defend its own information space, maintain public trust in state institutions, sustain the moral and psychological resilience of the population and military personnel, and shape favorable international perceptions of events.

The concept of strategic communication underwent systematic development in the doctrinal documents of NATO member states and the United States at the beginning of the twenty-first century. It rests on the understanding that any action taken by a state and its military structures has a communicative effect and influences the perceptions of target audiences. Accordingly, the effectiveness of contemporary military operations is determined to a considerable extent by the degree to which the communicative component is integrated into strategic and operational planning processes. The problematics of strategic communication remain at the center of attention among foreign and domestic researchers. The theoretical foundations of strategic communication have been examined in the work of Hallahan et al (2007), Holtzhausen and Zerfass (2015), Paul (2011), and other scholars, who treat it as an instrument for achieving organizational and political goals through the coordinated management of communication processes. A significant contribution to the development of domestic scholarly discourse has been made by Pocheptsov (2015), Lipkan (2015), Barovska (2015), and other researchers, who analyze strategic communication through the lens of national security and the state's information policy.

At the same time, a review of the scholarly literature reveals a number of unresolved issues. Above all, there is no unified understanding of the essence and structure of strategic communication in the military sphere, and questions concerning its institutional support and its integration into the system of military command remain insufficiently developed. Moreover, the body of research devoted to the practical problems of strategic communication functioning within the Armed Forces of Ukraine under conditions of prolonged armed conflict and adaptation to NATO standards remains limited. Particular attention is warranted by the problem of evaluating the effectiveness of strategic communication and defining criteria for assessing its results under conditions of contemporary information confrontation.

Thus, there is an objective need for a comprehensive study of the theoretical foundations, structural components, and current problems in the organization of strategic communication in military service. Resolving these issues is of considerable importance both for the development of military science and for the practical improvement of the communication support system for the activities of the Armed Forces of Ukraine.

The purpose of the article is a comprehensive analysis of the theoretical foundations and problems of strategic communication functioning in military service, together with the substantiation of directions for improving its organization under conditions of current security challenges and Ukraine's Euro-Atlantic integration.

Achieving this purpose requires resolving the following tasks:

- to clarify the essence and content of the concept of "strategic communication" in the context of the armed forces and to distinguish it from adjacent concepts;
- to characterize the structural components and mechanisms for implementing strategic communication in contemporary military operations;
- to systematize the key problems of implementing effective strategic communication in the Armed Forces of Ukraine on the basis of an analysis of domestic and foreign experience;
- to develop proposals for improving the system of strategic communication in the Armed Forces of Ukraine, taking into account the doctrinal approaches of NATO countries.

The article is grounded in the following hypothesis: the effectiveness of strategic communication in the armed forces is determined not so much by the presence of individual communicative tools or units, as by the degree of systemic integration of strategic communication into operational planning processes and the level of institutional maturity of the corresponding organizational structures. If this hypothesis is confirmed, it will make it possible to substantiate the claim that reforming the system of strategic

communication in the Armed Forces of Ukraine requires not isolated measures but systemic institutional changes — from the revision of doctrinal documents to the restructuring of officer training curricula.

## 2. MATERIALS AND METHODS

The methodological basis of the research comprises a set of general scientific and specialized scientific methods, the application of which is conditioned by the interdisciplinary character of the problematics of strategic communication in the military sphere. The theoretical foundation of the work is formed by the tenets of communication theory, security studies, military science, and public administration, as well as contemporary concepts of information confrontation and hybrid warfare.

The dialectical method was used to investigate the regularities in the development of strategic communication under the influence of the transformation of the security environment, the digitalization of society, and the growing role of the information factor in contemporary armed conflicts. This made it possible to examine strategic communication as a dynamic system that evolves in accordance with changes in the nature of threats and military operations.

The historical method was applied to analyze the genesis of the concept of strategic communication in NATO member states and to trace the process of its establishment in Ukraine. Within the framework of this method, the preconditions for the formation of strategic communication policy following the terrorist attacks of September 11, 2001, the development of the corresponding NATO doctrines between 2009 and 2025, and the impact of Russian aggression against Ukraine on the institutionalization of strategic communication within the state's security and defense sector were examined.

The formal-legal method was used to analyze the regulatory and legal foundations of the functioning of strategic communication in Ukraine. In particular, the provisions of the Law of Ukraine "On National Security of Ukraine," Decree of the President of Ukraine No. 392/2020 "On the Decision of the National Security and Defense Council of Ukraine of September 14, 2020, 'On the National Security Strategy of Ukraine,'" Decree of the President of Ukraine No. 121/2021 "On the Decision of the National Security and Defense Council of Ukraine of March 25, 2021, 'On the Military Security Strategy of Ukraine,'" as well as the Strategic Communications Doctrine of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine, were examined. Analysis of these documents made it possible to identify the regulatory foundations for the organization of strategic communication, its place within the national security system, and the principal directions of its further development.

The comparative-legal method was applied to compare the Ukrainian regulatory framework with NATO doctrinal documents, in particular the NATO Strategic Communications Policy (PO (2009)0141), the NATO Military Concept for Strategic Communications (MCM-0085-2010), the NATO Strategic Communications Handbook, and the recommendations of the NATO Strategic Communications Centre of Excellence. This made it possible to assess the level of implementation of Alliance standards in the activities of the Armed Forces of Ukraine and to identify directions for the further adaptation of the national strategic communication system to Euro-Atlantic requirements.

The method of analysis and synthesis was used to process scholarly sources devoted to the problematics of strategic communication. The works of K. Hallahan, D. Holtzhausen, C. Paul, H. Pocheptsov, V. Lipkan, A. Barovska, and other researchers were analyzed. This made it possible to distinguish the principal theoretical approaches to defining the concept of "strategic communication," to clarify its relationship to the categories of "information operations," "psychological operations," and "public diplomacy," and to form the conceptual basis of the study.

The systems method served as the key instrument for investigating strategic communication as an integral, multi-level system. Within this approach, the interaction among public relations structures, civil-military cooperation (CIMIC), information operations (Info Ops), psychological operations (PSYOPS), and military command bodies was analyzed. This made it possible to determine the place of strategic communication within the overall system of defense force management.

The structural-functional method was used to investigate the functional purpose of individual components of strategic communication. On this basis, the role of public communications in building trust in the Armed Forces of Ukraine, the significance of civil-military cooperation for interaction with the population in areas of combat operations, and the contribution of information and psychological operations to achieving strategic effects in the cognitive space were determined.

Content analysis was applied to Ukrainian regulatory acts, NATO doctrinal documents, analytical materials of the NATO Strategic Communications Centre of Excellence, and official communications of the Ministry of Defense of Ukraine, the General Staff of the Armed Forces of Ukraine, and the Center for Strategic Communications and Information Security. In the course of this analysis, the key categories, principles, and mechanisms for the implementation of strategic communication were identified, and the principal problems of their implementation in the military sphere were systematized.

The method of generalization was used to systematize the research findings, to formulate conclusions regarding the current state of strategic communication in the Armed Forces of Ukraine, and to develop proposals for its improvement with due regard to the practices of NATO member states.

The empirical basis of the research consists of Ukraine's regulatory and legal acts in the field of security and defense, in particular the Law of Ukraine "On National Security of Ukraine," the National Security Strategy of Ukraine (2020), the Military Security Strategy of Ukraine (2021), and the Strategic Communications Doctrine of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine, as well as NATO documents — the NATO Strategic Communications Policy, the NATO Military Concept for Strategic Communications, the NATO Strategic Communications Handbook — and analytical materials of the NATO Strategic Communications Centre of Excellence.

# 3. RESULTS

## 3.1. Theoretical foundations of strategic communication in the military sphere: Essence, evolution, and place in the national security system

Strategic communication in the military sphere is one of the key elements in the transformation of the contemporary approach to conducting armed conflicts, in which the information space has become an autonomous sphere of confrontation. Whereas the traditional model of military command was predominantly concentrated on the physical destruction of adversary forces, contemporary conflicts are characterized by a struggle over perception, the shaping of public sentiment, the legitimization of one's own actions, and the erosion of the opponent's informational advantages. It is precisely for this reason that strategic communication is today regarded not as an auxiliary function of military structures but as an integrated mechanism for achieving political and military objectives.

In both scholarly and practical terms, the concept of "strategic communication" lacks a fully unified definition. This is due to the fact that the concept was formed at the intersection of several fields: military command, public diplomacy, information operations, crisis communication, and strategic management (Hallahan et al., 2007).

One of the most widespread approaches is that proposed in NATO documents, according to which strategic communication is regarded as the integrated and coordinated use of communication capabilities to support the political and military objectives of the Alliance. In its contemporary understanding, NATO Strategic Communications encompasses not merely the transmission of messages but also the alignment between the organization's actions, its words, and the perception of those actions by target audiences. This approach is reflected in the Alliance's strategic documents, in particular the NATO Strategic Concept (2022), which emphasizes the need to strengthen societal resilience, counter disinformation, and develop capabilities in the field of strategic communication (NATO 2022 Strategic Concept, 2022).

In Paul's view, strategic communication in the military context should be understood as the process of synchronizing various communication instruments and activities in order to achieve strategic effects.

This approach focuses attention not merely on the informational product but, above all, on coordination among political leadership, military command, and communication structures (Paul, 2011). At the same time, contemporary research emphasizes that the effectiveness of strategic communication is determined not by the number of informational messages but by an organization's capacity to construct durable frameworks of meaning and to influence the behavior of defined audiences. Ukrainian researchers predominantly examine strategic communication through the lens of national security and information sovereignty. Thus, Syvak (2018) defines it as the management of meaning under conditions of a competitive information environment, in which the key resource is not merely information as such but the capacity to shape the necessary interpretation of events. In the context of the Russo-Ukrainian war, strategic communication has acquired particular importance as an instrument for ensuring state resilience, sustaining the international coalition, and countering hostile information-psychological operations.

Important to distinguish strategic communication from other types of communicative activity in the military sphere. Strategic Communications is the broadest concept, uniting all the communication capabilities of a state or military organization in pursuit of strategic objectives. Its principal characteristic is integrativeness: strategic communication encompasses both informational measures and direct actions, since any action taken by the state has a communicative effect. Public Affairs constitutes a separate component of strategic communication and is directed toward ensuring open interaction between the military organization and the mass media, the public, and other external audiences (Storozhenko & Petkun, 2021). The principal function of Public Affairs is to inform, to ensure transparency of activity, and to build trust in military structures. Unlike strategic communication, Public Affairs does not encompass the full spectrum of informational influence but is concentrated predominantly on the public dimension of communication. Information Operations represent the coordinated use of informational capabilities to influence the decision-making processes of an adversary, neutral parties, or other defined audiences. In military practice, Info Ops encompass such areas as cyber operations, electronic warfare, psychological influence, and the management of the information environment. Psychological Operations constitute a narrower instrument, directed toward influencing the perception, persuasion, and behavior of specific audiences through the use of psychological mechanisms (Karpchuk et al., 2023). Unlike StratCom, psychological operations are predominantly operational in character and are applied to achieve specific military effects.

Thus, the relationship among these concepts can be represented as a hierarchical model: strategic communication forms the overarching framework, within which Public Affairs, Information Operations, and Psychological Operations perform discrete functions in accordance with defined strategic tasks.

The evolution of the concept of strategic communication is linked to the transformation in the character of contemporary conflicts. In the United States, the active development of this approach began after the operations in Afghanistan and Iraq, when it became evident that military superiority does not guarantee political success without the support of the information environment. In response, the U.S. Department of Defense began to form a systematic approach to strategic communication that entailed the integration of informational capabilities into military planning processes. Within NATO, the concept of strategic communication received institutional formalization in 2009–2010 and continued to develop under the influence of the Alliance's operational experience, in particular in Afghanistan. The contemporary NATO approach holds that strategic communication must be integrated at all levels of command — from the political to the tactical. An important role in the development of this field is played by the NATO Strategic Communications Centre of Excellence (2023), which conducts research into the information environment, develops methodologies for narrative analysis, and supports the development of communication capabilities among member states and partners (Ministry of Defence, 2020).

In Ukraine, the development of strategic communication accelerated after 2014 in response to Russian aggression and the adversary's large-scale application of information-psychological operations. A regulatory and organizational foundation for strategic communication in the security and defense sector was gradually established. Important milestones included the adoption of the Law of Ukraine "On National

Security of Ukraine," the National Security Strategy of Ukraine (2020), the Military Security Strategy of Ukraine (2021), as well as the establishment of dedicated strategic communication units within the Ministry of Defence of Ukraine and other security-sector bodies. Today, the Strategic Communications Department of the Ministry of Defence of Ukraine coordinates the development of the strategic communication system in the defense sphere, the formation of communication strategies, and the strengthening of the defense sector's resilience. Within the national security system, strategic communication performs several key functions. First, it ensures the legitimation of state defense policy by building the trust of citizens and international partners. Second, it contributes to strengthening society's resilience to informational threats and disinformation. Third, it ensures coordination among the various actors of the security and defense sector in responding to hybrid threats.

Strategic communication in the military sphere should therefore be regarded as a systemic component of national security provision, one that unites informational, organizational, and managerial mechanisms of influence. Its significance extends far beyond traditional public communication, since in contemporary conflicts victory is determined not only by control over territory but also by the capacity to shape the perception of events, sustain trust, and secure strategic advantage within the information environment.

### 3.2. Structure and functional components of strategic communication in contemporary military operations

Under present-day conditions, strategic communication is regarded as an integrated system for managing the information environment, one that ensures the alignment of political, military, and communicative measures in order to achieve defined strategic effects. Unlike the traditional model of communication, oriented predominantly toward the transmission of information, the contemporary concept of strategic communication entails the comprehensive management of the processes by which perception, the interpretation of events, and the behavioral responses of target audiences are shaped.

In the military sphere, strategic communication is not a discrete type of activity or the function of a single unit. It constitutes a cross-functional system that integrates various communicative capabilities and ensures their synchronization with operational planning processes. Bjola and Pamment (2019), for instance, in analyzing the transformation of public diplomacy amid the spread of digital propaganda, emphasize that the effectiveness of strategic communication in the digital age is determined not by isolated informational products but by an organization's capacity to align actions, messages, and channels into a single system for responding to threats within the information environment. In accordance with the NATO approach, strategic communication must be incorporated into every stage of the planning and conduct of military operations, since every action taken by a military organization produces an informational effect and influences how the operation is perceived by different audiences (NATO StratCom COE, 2023).

The integrated character of strategic communication lies in the fact that it brings together several interrelated lines of activity: public affairs, cooperation between military and civilian actors, information operations, operations aimed at shaping psychological effects, and digital communication and social media engagement. Rid (2020), in examining the evolution of disinformation campaigns over the past century, demonstrates that it is precisely the integration of technical, psychological, and organizational instruments of influence — rather than isolated propagandistic messages — that determines the effectiveness of information confrontation in the digital era; this conclusion applies directly to the logic underlying the construction of a contemporary strategic communication system. Each of these components has its own functional purpose, yet their effectiveness is determined not by autonomous application but by their capacity to operate within a single, unified strategic logic.

Public affairs is one of the central components of the strategic communication system, ensuring open interaction between military structures and society, the mass media, state institutions, and other external audiences. Its principal task is to ensure the transparency of a military organization's activity, to build trust in the security and defense sector, and to explain the objectives and consequences of military decisions. In

contemporary NATO doctrine, public affairs is treated not merely as an informing function but as an instrument for shaping the information environment that supports the strategic objectives of an operation (NATO Strategic Communications Handbook, 2023). At the same time, public affairs is fundamentally distinct from information operations: its activity is grounded in the principles of accuracy, openness, and engagement with the public, whereas information operations may include measures deliberately intended to influence the adversary's information environment. Public affairs thus functions as the "outward-facing communicative dimension" of strategic communication, securing the legitimacy of military action and sustaining the connection between the armed forces and society.

Cooperation between military and civilian actors — commonly referred to by its NATO abbreviation, CIMIC — is a component of strategic communication that ensures interaction among military structures, government authorities, international organizations, humanitarian bodies, and the civilian population in areas where operations are conducted. Its principal function is to create the conditions for the effective execution of military tasks by managing the interface between the military and civilian environments. In contemporary conflicts, this form of cooperation acquires particular significance, since the support of the local population, the maintenance of humanitarian stability, and the building of trust in military structures directly affect the success of operations. Within the framework of strategic communication, this cooperation serves to ensure consistency between the practical actions of military units and their strategic messaging: humanitarian measures, assistance to the civilian population, or the restoration of critical infrastructure all generate a communicative effect irrespective of whether they are accompanied by explicit informational messaging. It is for this reason that the contemporary concept of strategic communication rests on the principle that actions communicate in themselves: if the actual conduct of a military organization contradicts its stated values, even an effective information campaign will fail to produce the necessary strategic effect.

Information operations constitute one of the most important components of strategic communication in the military sphere. They are directed toward coordinating the use of informational capabilities in order to influence the adversary's decision-making processes, to protect one's own information resources, and to shape a favorable information environment. Under contemporary NATO approaches, information operations are not equated with the dissemination of information or with propaganda as such; their essence lies in the planning and coordination of measures that make it possible to achieve defined military effects through influence on informational processes. Such operations may encompass the analysis of the information environment, countering hostile disinformation, cyber operations, electronic warfare, the management of information flows, and support for operations aimed at shaping psychological effects. In the Russo-Ukrainian war, information operations have become one of the key axes of confrontation: Russia actively employs them to construct alternative narratives, discredit Ukraine, and influence international audiences, while Ukraine, for its part, is building its own information-defense capabilities and integrating them into its strategic communication system.

Operations aimed at shaping psychological effects — known in doctrine as psychological operations — represent a specialized component of military communication directed toward influencing the perception, motivation, and behavior of defined audiences through the use of psychological mechanisms (Karpchuk et al., 2023). Unlike strategic communication, which is comprehensive in character and oriented toward the broader information environment, such operations have a narrower, more operational purpose: their objective is to achieve a specific psychological effect — for example, lowering the adversary's morale, sustaining the morale of one's own forces, or influencing the behavior of particular groups. In contemporary conflicts, these operations increasingly rely on digital platforms, social networks, and large-scale data analytics, which allow for more precise audience segmentation and the formulation of tailored communicative messages.

Digital communication and social media have fundamentally reshaped the structure of strategic communication. Social media have become not merely a channel for transmitting information but an environment in which public sentiment is formed, narratives compete, and support is mobilized. In contemporary military conflicts, digital platforms perform several functions: providing timely information

to the population, countering disinformation, shaping strategic narratives, supporting international communication, and analyzing informational trends. Ukraine's experience since 2022 demonstrates the significance of digital communication in securing international support and shaping global perceptions of the war: the use of social networks has made it possible to establish direct contact with international audiences without the mediation of traditional media (Storozhenko & Petkun, 2021).

On the basis of a synthesis of NATO's doctrinal approaches, an analysis of how the strategic communication system functions within the Armed Forces of Ukraine, and the current characteristics of information confrontation, the author proposes an Integrated Military Strategic Communications Model (IMSCM) — an integrated model of strategic communication for a military organization. Unlike the conventional approach, which treats public affairs, information operations, psychologically oriented operations, and cooperation with civilian actors as separate functional strands, the proposed model rests on the principle of their continuous integration into a single cycle of military command and control. The model's key distinguishing feature is that strategic communication does not merely accompany a military operation but forms an integral part of every stage of its planning, execution, and evaluation. This ensures the synchronization of command decisions, informational influence, and the practical actions of forces, thereby making it possible to produce durable cognitive effects among defined target audiences (Figure 1).

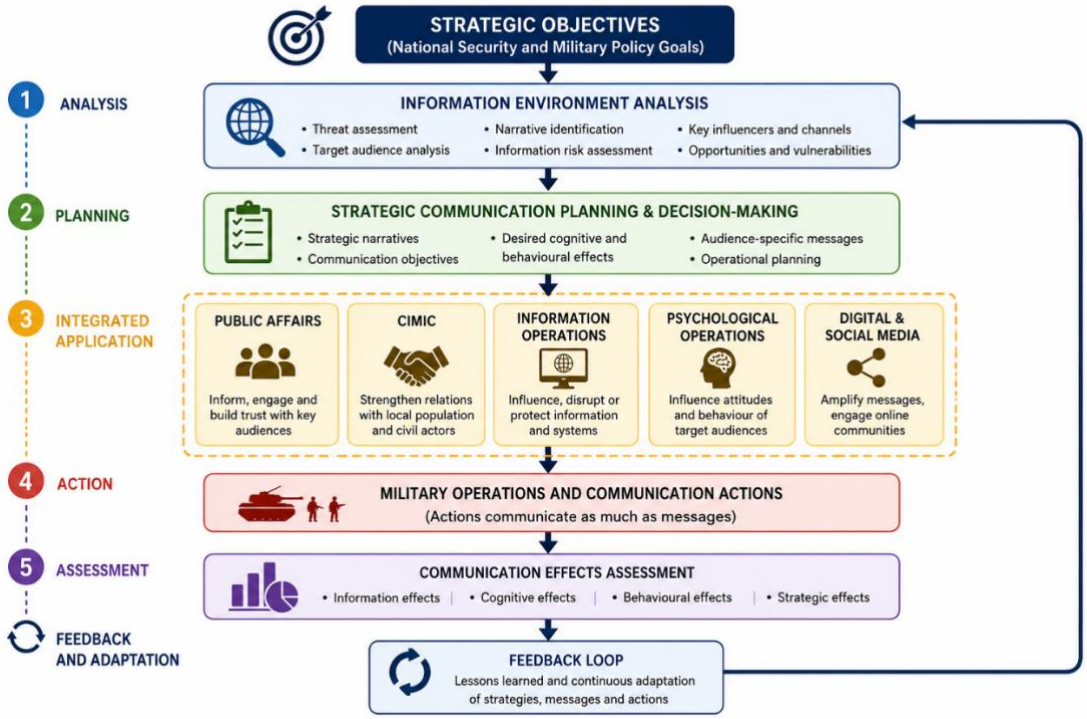



Figure 1. Integrated military strategic communications model

*Source: developed by the author*

The proposed model demonstrates the cyclical character of strategic communication. In the first stage, the information environment is analyzed, encompassing the identification of informational threats, key audiences, dominant narratives, and the forecasting of potential communicative risks. The results obtained form the basis for constructing strategic messages and defining the communicative effects to be achieved during the military operation. This is followed by the integrated application of all functional components. The final stage consists of evaluating the informational, cognitive, and behavioral effects achieved, the results of which are used to adjust the next cycle of strategic planning. The model thus embodies the principle of continuous feedback, in line with contemporary NATO doctrinal approaches, and ensures the adaptability of the strategic communication system to changes in the information environment.

ISSN 2815-3324 Online, ISSN 2535-0358 Print

The model comprises five sequential stages, joined by a feedback loop, and unfolds beneath the strategic objectives of the operation (national security and the state's military-political goals):

Analysis of the information environment — assessment of informational threats, identification of dominant narratives, analysis of target audiences, key influential actors and communication channels, and identification of informational risks, opportunities, and vulnerabilities.

Strategic planning and decision-making — formulation of strategic narratives, definition of communicative objectives, desired cognitive and behavioral effects, audience-specific messages, and operational planning of the communicative dimension of the operation.

Integrated application of components — the simultaneous and coordinated implementation of public affairs, cooperation with civilian actors, information operations, operations aimed at shaping psychological effects, and digital and social media activity, all within a single managerial logic rather than as isolated functions.

Action — direct military operations and communicative actions that give effect to the principle that "actions communicate no less than words."

Assessment — the measurement of the informational, cognitive, behavioral, and strategic effects achieved.

The results of this assessment form a feedback and adaptation loop that ensures the adjustment of narratives, messages, and actions in the subsequent planning cycle. The model thus embodies the principle of continuous feedback, consistent with contemporary NATO doctrinal approaches (NATO Strategic Communications Handbook, 2023), and ensures the adaptability of the strategic communication system to changes in the information environment.

Unlike the classical decision-cycle model (the OODA loop) or the standard strategic communication planning process set out in the NATO Strategic Communications Handbook, the key distinguishing feature of the IMSCM is that its third stage — integrated application — brings all five functional components together into a single parallel phase of the cycle, rather than treating them as separate, accompanying processes that unfold outside the main operational planning cycle. This makes it possible to avoid the fragmentation that arises, for example, when operations aimed at shaping psychological effects or information operations are planned separately from public affairs — a practice that in practice often results in contradictory messaging and the erosion of target audiences' trust.

In sum, public affairs ensures engagement with external audiences, cooperation with civilian actors builds the connection between military and civilian environments, information operations ensure the management of informational processes, operations aimed at shaping psychological effects are directed toward achieving specific psychological outcomes, and digital communication ensures the speed and scale of strategic message dissemination. The integration of these components within the single managerial cycle of the IMSCM makes it possible to move from fragmented communicative activity to the systemic management of the information environment a necessary condition for achieving strategic objectives in contemporary military operations.

### 3.3. The role of strategic communication in hybrid warfare and information confrontation

The transformation in the character of contemporary armed conflicts has led to a substantial expansion of the space of confrontation, in which — alongside traditional military operations — the informational, cognitive, and psychological dimensions are acquiring ever greater significance. Hybrid warfare entails the combined application of military, political, economic, diplomatic, informational, and cyber instruments in pursuit of strategic objectives, without necessarily escalating to the classical model of full-scale armed confrontation. Under such conditions, the information space becomes a distinct theater of confrontation, in which states compete for control over the perception of events, the shaping of public sentiment, and the determination of the dominant interpretation of reality (Paul and Matthews, 2018).

A distinguishing feature of the informational dimension of contemporary conflicts is that the object of influence is not merely information infrastructure or data-transmission channels but, above all, the consciousness of individuals, social groups, and the international community. Unlike the traditional propaganda of the past, contemporary information-psychological operations employ digital platforms, social networks, content-personalization algorithms, and automated tools for disseminating information, which makes it possible to exert large-scale, rapid influence on diverse audiences (Ecker et al., 2026). Under these conditions, strategic communication acquires significance as a mechanism for managing the information environment, since it ensures not merely the dissemination of messages but also the construction of a system of meanings, values, and strategic narratives necessary for achieving political and military objectives.

The experience of the Russo-Ukrainian war is one of the most illustrative examples of the role of strategic communication in a contemporary conflict. Beginning in 2014, the Russian Federation actively employed a complex of hybrid instruments in which informational influence became one of the central elements of its aggression. Its information operations were directed toward legitimizing the unlawful annexation of Crimea, constructing a distorted image of Ukraine on the international stage, demoralizing Ukrainian society, and diminishing the level of support for Ukraine among its foreign partners (Mammadov, 2026). A distinguishing feature of the Russian approach was the systematic use of disinformation, manipulative narratives, and pseudo-news, together with the use of social networks and controlled media resources to construct an alternative picture of reality.

Following the start of Russia's full-scale invasion in 2022, the significance of strategic communication for Ukraine grew substantially. The war demonstrated that informational superiority can directly affect military and political outcomes. Ukraine's system of strategic communication became one of the key instruments for securing international support, mobilizing domestic resources, and building societal resilience (Pynnöniemi and Tolvin, 2025). An important factor in this success was the combination of official communication by state bodies, the activity of military structures, digital diplomacy, and the engagement of civil society.

The experience of the Russo-Ukrainian war merits examination not merely in descriptive terms but also through the lens of the Integrated Military Strategic Communications Model, which makes it possible to explain why informational advantage or defeat on either side is determined not by the presence of individual communicative instruments but by the degree of their systemic integration into a single management cycle. The Russian side, for instance, has since 2014 demonstrated a high level of coordination among individual components (information operations, psychologically oriented operations, and controlled digital media) corresponding to the third stage of the model. Yet this coordination has not been accompanied by a stage analogous to "action" within the IMSCM: Russia's practical conduct (the occupation of territory, war crimes) systematically contradicts its own stated strategic narratives even a highly effective information campaign loses its strategic effect if it is not reinforced by consistent action. Ukraine's system of strategic communication after 2022, by contrast, more closely approximates the full IMSCM cycle: the analysis of the information environment (monitoring hostile narratives), strategic planning (the formation of a unified communicative position among state bodies), integrated application (the combination of public affairs, digital diplomacy, and civil-society engagement), and the assessment of effects (adjusting communicative strategy in response to shifts in international perceptions of the war) can be traced with reasonable consistency across the activity of Ukrainian institutions, although the institutional maturity of individual components of the cycle remains uneven — a matter examined in greater detail in the section devoted to the problems of implementing strategic communication within the Armed Forces of Ukraine. The comparison of the two approaches thus substantiates the central hypothesis of the study: advantage in information confrontation is determined not by the instruments themselves but by the degree of their integration into a unified management cycle.

One of the key areas of application of strategic communication in the context of hybrid warfare is countering the adversary's disinformation and information-psychological operations (Ehrl, 2023). Such counteraction cannot be confined to the refutation of individual false claims, since contemporary

ISSN 2815-3324 Online, ISSN 2535-0358 Print

information campaigns are directed not so much at disseminating isolated falsehoods as at constructing durable patterns of perception. For this reason, an effective system of strategic communication must include the monitoring of the information environment, the analysis of hostile narratives, the forecasting of informational threats, timely response, and the formulation of persuasive messages of its own.

In this context, it is important to shift from a reactive to a proactive model of communication, under which the state not merely responds to the adversary's informational attacks but independently sets the agenda and shapes strategic meanings. Such an approach entails the construction of coherent strategic narratives that explain the objectives of state policy, strengthen citizens' trust in institutions, and secure the support of international partners. A illustrative example of this proactive approach is the work of Ukraine's Center for Strategic Communications and Information Security (SPRAVDI), established in March 2021 under the Ministry of Culture and Information Policy. In particular, the Center's information campaign explaining the ideological doctrine of the "Russian World" was directed not at refuting individual Russian claims but at constructing a durable counter-narrative addressing the origins and dangers of this ideology; according to the Center's own leadership, the campaign's findings were partly reflected in the subsequent resolution of the European Parliament condemning the "Russian World" ideology (Center for Strategic Communications and Information Security of Ukraine, 2025). This example illustrates the key distinguishing feature of the proactive model: a state institution does not respond to disinformation already in circulation but instead sets the agenda itself, preempting the adversary's potential manipulative narratives. In the military context, a strategic narrative functions not merely as an informational message but as a comprehensive system explaining the causes of the conflict, the objectives of the struggle, and the desired future outcome. This is consistent with N. Bolt's definition, which treats strategic narrative as a projection of a state's foreign and security policy, directed toward changing the attitudes and behavior of target audiences in order to achieve strategic effects through words, images, actions, and even inaction employed in the state's interest (Bolt, 2011). In this sense, strategic narrative performs not only an informational but also an explanatory and legitimizing function, uniting the past (the causes of the conflict), the present (the objectives of the struggle), and the future (the desired outcome) into a single construct of meaning.

Strategic narratives are of particular importance for sustaining societal resilience. The conditions of a prolonged armed conflict impose a considerable psychological burden on the population and contribute to the spread of war fatigue, distrust, and social tension. At the same time, empirical evidence indicates that effective communicative work can sustain a high level of trust in security-sector institutions even amid a protracted conflict: according to a survey by the Kyiv International Institute of Sociology, trust in Ukraine's Defense Forces stood at 94 percent as of December 2025, remaining consistently high (92–94 percent) throughout 2024–2025, whereas trust in other state institutions — the courts, the prosecutor's office — did not exceed 15 percent (KIIS, 2025). This gap in trust indirectly confirms the role of strategic communication in the defense sector as a factor sustaining societal resilience even against a backdrop of broader institutional distrust. Under these conditions, strategic communication performs the function of sustaining moral and psychological resilience by explaining the rationale behind decisions taken, demonstrating the results of the security and defense sector's activity, and fostering a sense of shared purpose.

Beyond its domestic dimension, strategic communication plays an important role in the international environment. In contemporary wars, victory depends to a considerable degree on a state's ability to shape favorable international perceptions of the conflict, to secure the political support of its allies, and to counter the adversary's attempts to impose its own interpretation of events. Ukraine's experience demonstrates that effective strategic communication can become an important factor in building an international coalition and sustaining a state's defense efforts.

The empirical material examined here provides grounds for testing the study's central hypothesis directly against the case of the Russo-Ukrainian war: whether the effectiveness of strategic communication is determined by the presence of individual instruments or by the degree of their institutional integration. The analysis supports the latter proposition. Ukraine's system of strategic communication possesses a

broad and functionally complete set of instruments — the Center for Strategic Communications and Information Security, dedicated units within the Ministry of Defence, the Strategic Communications Department of the General Staff, the Center for Countering Disinformation, as well as a developed sector of digital diplomacy and civic initiative. Yet the effectiveness of this system over the period 2022–2025 was constrained to a considerable degree not by a shortage of instruments but by the insufficient institutional stability of its coordinating center. Tellingly, the ministry responsible for strategic communication changed its name and mandate three times within three years: the Ministry of Culture and Information Policy (until September 2024) was renamed the Ministry of Culture and Strategic Communications, only to be reverted in October 2025 to its previous name and scope of authority — the Ministry of Culture (Cabinet of Ministers of Ukraine, 2024; 2025). At the same time, the Center for Strategic Communications and Information Security itself was compelled during 2025 to change its organizational and legal form from a state institution to a non-governmental organization, retaining its practical cooperation with state bodies while losing part of its institutional standing (Detector Media, 2026). Such organizational fluctuations illustrate a situation in which individual functional components of strategic communication — public affairs, information operations, digital communication — continue to operate and develop, while the degree of their systemic integration into a unified command vertical remains unstable — a pattern that directly bears out the study's hypothesis: it is not the array of instruments but the institutional maturity of the coordinating structure that constitutes the decisive factor in effectiveness. By contrast, the high and stable level of public trust in the Defense Forces (92–94 percent throughout 2024–2025, according to KIIS data), set against considerably lower trust in other state institutions, indirectly confirms that where the integration of the communicative function within the military command system is more consistent above all at the level of the Armed Forces themselves rather than civilian coordinating bodies strategic communication produces a more durable result.

Strategic communication under conditions of hybrid warfare thus performs a comprehensive function in securing a state's informational, political, and societal resilience. It brings together the instruments of communication, the analysis of the information environment, the countering of disinformation, and the construction of strategic narratives. The experience of the Russo-Ukrainian war confirms that informational superiority is an integral component of contemporary military advantage, and that an effective system of strategic communication must be regarded as one of the key elements in securing national security and defense. The empirical material drawn from the hybrid war waged by Russia against Ukraine confirms the practical applicability of the proposed IMSCM: it is the cyclical integration of analysis, planning, action, and assessment that determines the strategic effectiveness of countering information aggression.

### 3.4. Challenges in implementing strategic communication in the armed forces of Ukraine

Despite significant progress in developing the system of strategic communication within Ukraine's security and defense sector, its practical implementation in the Armed Forces of Ukraine remains a process accompanied by a range of doctrinal, organizational, personnel-related, technological, and methodological problems. The formation of a fully-fledged system of strategic communication is taking place under conditions of ongoing armed aggression by the Russian Federation, requiring the simultaneous conduct of combat operations and institutional adaptation to NATO standards. This produces a certain asymmetry in development: on the one hand, Ukraine has established the basic elements of the regulatory and organizational framework for strategic communication; on the other, individual mechanisms of its functioning have not yet attained a sufficient level of systemic coherence and integration.

One of the key problems remains doctrinal ambiguity and insufficient conceptual coherence with respect to strategic communication in the military sphere. Despite the codification of the concept of strategic communication in the regulatory documents of the security and defense sector, practical activity still exhibits a certain conflation of the concepts of strategic communication, public affairs, information operations, and psychological operations. Such terminological ambiguity can lead to the duplication of functions among structural units, divergent understandings of tasks among relevant officials, and

ISSN 2815-3324 Online, ISSN 2535-0358 Print

insufficient coordination of communicative activity. In particular, strategic communication is not infrequently equated exclusively with the work of press services or with the informational support of military command bodies' activities, although under NATO standards it is considerably broader in character and entails the integration of communicative capabilities into planning and decision-making processes.

The doctrinal problem is also linked to the need for the further development of a national model of strategic communication that takes into account the specific character of the Russo-Ukrainian war. The mechanical transfer of NATO approaches does not always account for the particularities of Ukraine's security environment, in particular the scale of the adversary's information-psychological operations, the substantial role of digital platforms, and the need to secure both domestic and international support simultaneously. The task of adapting allied doctrinal approaches to the conditions of a prolonged armed conflict, and of formulating an indigenous practice of strategic communication, therefore remains an urgent one.

A further set of problems concerns organizational and institutional challenges. The effectiveness of strategic communication depends on the extent to which it is integrated into the structure of military command. In practice, strategic communication often remains the function of individual units rather than a cross-cutting process that must be taken into account throughout strategic, operational, and tactical planning. In many instances, the communicative component is incorporated into the command process only after the relevant decisions have already been taken, which limits its capacity to shape strategic effects.

A further problem is the insufficiently clear delineation of authority among the various actors involved in strategic communication within the security and defense sector. The Ministry of Defence of Ukraine, the General Staff of the Armed Forces of Ukraine, military command bodies, public affairs units, and structures responsible for information operations, psychological operations, and cooperation with civilian actors are all simultaneously engaged in shaping the information environment. The absence of a fully integrated coordination mechanism among these actors can create risks of unsynchronized messaging, duplication of functions, or delayed response to informational threats.

A separate problem is the inadequacy of the regulatory framework for strategic communication. Ukraine has established a basic regulatory foundation through the provisions of the Law of Ukraine "On National Security of Ukraine," the National Security Strategy of Ukraine (2020), the Military Security Strategy of Ukraine (2021), and the Strategic Communications Doctrine of the Ministry of Defence of Ukraine and the Armed Forces of Ukraine. At the same time, these regulatory documents predominantly define general principles and directions for the development of strategic communication, whereas questions concerning the system's practical functioning — planning procedures, the allocation of responsibility, mechanisms for evaluating effectiveness, and interaction among its components — require further elaboration.

An important challenge remains the staffing of strategic communication functions. The contemporary strategic communication model requires specialists who combine knowledge of military command, communication, informational analysis, psychology, digital technologies, and international relations. However, the traditional system of military personnel training was for a long time oriented predominantly toward classical military specializations, whereas competencies in the field of strategic communication have only begun to be actively developed in recent years.

An insufficient number of specialized training programs, the absence of unified standards for the preparation of specialists, and limited practical experience in dealing with contemporary informational threats are factors affecting the effectiveness of the strategic communication system's functioning. Particular attention is required not only for the training of narrowly specialized communicators but also for command personnel, who must understand the role of the informational component in the process of military decision-making.

Technological problems are linked to the need for constant adaptation to rapid changes in the information environment. The Russo-Ukrainian war has demonstrated the significance of social networks, digital platforms, artificial intelligence, and automated information analysis in contemporary confrontation. At the same time, the development of Ukraine's own technological capabilities for monitoring the information space, analyzing narratives, and forecasting informational threats requires substantial resources and a systematic approach.

One of the most complex issues remains the assessment of the effectiveness of strategic communication. Unlike traditional military indicators, communicative effects are often long-term and indirect in character, which complicates their quantitative measurement. For example, an increase in public trust in the Armed Forces, a shift in international perceptions of the state, or a reduction in the influence of hostile narratives cannot be assessed solely through standard statistical indicators.

In NATO's strategic communication practice, increasing attention is being paid not only to the results of informational activity but also to the achievement of desired behavioral and cognitive effects. For Ukraine, an urgent task is the development of its own evaluation system that would make it possible to determine the extent to which communicative measures contribute to the achievement of military-political objectives.

The problems of implementing strategic communication in the Armed Forces of Ukraine are thus comprehensive in character, spanning doctrinal, organizational, personnel-related, technological, and methodological dimensions. The principal challenge remains the transition from an understanding of strategic communication as a discrete informational domain to its recognition as an integrated command function. The further development of the strategic communication system requires not only the improvement of the regulatory framework and organizational structures but also the cultivation of a corresponding culture of communication within the military environment, in which every decision and action is regarded as an element of strategic informational influence.

To synthesize the results of the analysis conducted, it is appropriate to systematize the principal problems affecting the functioning of the strategic communication system in the Armed Forces of Ukraine according to their underlying causes, potential consequences, and possible directions for resolution (Table 1). This approach makes it possible to assess comprehensively the interrelationship among organizational, regulatory, personnel-related, and technological factors, and to outline priority directions for the further reform of the strategic communication system.

Table 1. Matrix of key challenges in implementing strategic communications in the Armed Forces of Ukraine (developed by the author)

| Problem | Underlying cause | Potential consequences | Recommended solution |
|---|---|---|---|
| Fragmented coordination between StratCom actors | Absence of an integrated coordination mechanism and unified management procedures | Inconsistent messaging, duplication of functions, reduced operational effectiveness | Establish a unified strategic communications coordination system integrated into operational planning |
| Insufficient integration with military decision-making | StratCom is often regarded as a supporting rather than operational capability | Communication activities are disconnected from operational objectives | Integrate strategic communications into all stages of military planning and command processes |
| Limited institutional capacity | Shortage of qualified personnel, insufficient training programmes and lack of specialised education | Reduced ability to counter information threats and conduct influence activities | Develop professional education programmes, specialised training and NATO-oriented capacity building |
| Incomplete regulatory framework | Fragmented legal regulation and absence of unified doctrinal documents | Different approaches among military units and institutions | Harmonise national doctrine with NATO standards and adopt comprehensive regulatory documents |

| | | | |
|---|---|---|---|
| Technological limitations | Limited use of AI, OSINT, big data analytics and digital monitoring systems | Slow identification of threats and ineffective assessment of information operations | Introduce advanced analytical technologies and decision-support systems |
| Weak interagency cooperation | Insufficient information exchange between defence, intelligence and civilian institutions | Delayed response to hybrid threats | Strengthen institutional cooperation through permanent coordination mechanisms |
| Insufficient assessment of communication effectiveness | Lack of unified indicators for evaluating information influence | Difficulties in measuring operational success and adapting communication campaigns | Introduce a comprehensive system of strategic communication performance indicators |

The synthesis of these problems indicates that most of them are systemic in character and cannot be resolved through localized organizational changes alone. Effective reform of the strategic communication system requires a comprehensive approach that combines institutional, regulatory, personnel-related, and technological measures. It is for this reason that the subsequent analysis is appropriately focused on identifying promising directions for improving the strategic communication system, taking into account the practical experience of NATO member states and the current requirements of information confrontation.

### 3.5. Directions for Improving the System of Strategic Communication in the Armed Forces of Ukraine: NATO Experience and Prospects for Adaptation

The further development of the system of strategic communication in the Armed Forces of Ukraine should proceed with due regard to the experience of NATO member states, which over recent decades have developed comprehensive models for managing the information environment. Analysis of the Alliance's practices indicates that the effectiveness of strategic communication is determined not merely by the presence of specialized units but, above all, by the degree to which the communicative function is integrated into the system of strategic and operational command. It is precisely this approach that makes it possible to move from a reactive model of responding to informational challenges toward the proactive shaping of the information environment in accordance with defined political and military objectives.

The problems systematized in Table 1 give rise to the need for a set of interrelated solutions. These solutions are best regarded not as a discrete list of measures but as a coherent model of reform grounded in the experience of NATO member states, which over recent decades have developed comprehensive approaches to managing the information environment. One of the most developed of these is the NATO approach, codified in the Alliance's key doctrinal document — the Allied Joint Doctrine for Strategic Communications (AJP-10) — which rests on the principle of synchronizing all communicative capabilities: public affairs, information operations, psychological operations, and cooperation with civilian actors (NATO Standardization Office, 2023a). A more detailed treatment of the approach to information operations is provided in AJP-10.1, the Allied Joint Doctrine for Information Operations (January 2023), which introduces the so-called behaviour-centric approach — an orientation not toward the dissemination of messages but toward the achievement of defined behavioral effects among target audiences (NATO Standardization Office, 2023b). Matters concerning the public communication of military structures are addressed separately in AJP-10.3, the Allied Joint Doctrine for Military Public Affairs, which defines the role of public affairs at the strategic, operational, and tactical levels (NATO Standardization Office, 2022).

Within NATO member states, strategic communication is treated as a function of command rather than merely a task assigned to discrete informational units: communication advisers are embedded within military command structures at every level — from the strategic to the tactical — and their task consists not only in preparing informational materials but also in ensuring that the informational dimension is taken into account throughout the planning of military operations. A distinguishing feature of this approach is the consistent application of a principle already articulated in Section 2 of this article: every military action produces a communicative effect, and strategic communication must therefore begin not

after a decision has been taken but already at the stage of situational analysis, the definition of operational objectives, and the assessment of an operation's possible consequences for different audiences.

It is important to distinguish the functional purpose of the two models presented in this article. The Integrated Military Strategic Communications Model (IMSCM) proposed in Section 2 is an operational model: it describes the cycle of planning, execution, and assessment for specific communicative measures within an individual operation. The five-level model set out below, by contrast, is institutional in character — it outlines the directions for the systemic reform of strategic communication at the national level of command, thereby addressing not the question of "how to plan a specific campaign" but rather "how to restructure the institutional architecture so that the IMSCM cycle can be consistently implemented in practice."

An important direction for improvement is the further development of the regulatory and doctrinal framework for strategic communication. Ukraine currently possesses a set of basic regulatory documents that define the significance of information security and strategic communication, in particular the Law of Ukraine "On National Security of Ukraine," the National Security Strategy of Ukraine (2020), the Military Security Strategy of Ukraine (2021), and the Strategic Communications Doctrine of the Ministry of Defence of Ukraine and the Armed Forces of Ukraine (2020) (see Table 1, row "Incomplete regulatory framework"). It would be advisable to develop an updated strategic communications doctrine for the Armed Forces of Ukraine, one that clearly defines the conceptual apparatus of strategic communication; the relationship among strategic communication, public affairs, information operations, and psychological operations; the procedures for interaction among the relevant units; and the processes for planning, executing, and evaluating communicative measures. Such a document should be aligned with the provisions of AJP-10, AJP-10.1, and AJP-10.3.

The effectiveness of strategic communication depends on the degree to which it is integrated into the structure of military command. An improved model should provide for the participation of strategic communication representatives in the work of staffs and command groups from the moment an operation's concept is first formulated, rather than at the stage of providing informational support for decisions already taken.

A further direction concerns the integration of strategic communication into the operational planning processes of the Armed Forces of Ukraine. At present, the communicative component is often treated as an element of informational support for decisions that have already been made, whereas NATO standards call for the inclusion of strategic communication at every stage of operational planning. An improved model should provide for the participation of strategic communication representatives in the work of staffs and command groups from the moment an operation's concept is first formulated. Within this approach, the process of operational planning should include the mandatory analysis of the information environment, the identification of key audiences, the assessment of potential informational risks, the formulation of desired communicative effects, and the development of corresponding messages. Strategic communication must be linked not merely to the dissemination of information but to the decision-making process itself, since any military action must take into account its possible impact on public perception, international support, and the state's informational resilience.

A separate priority direction concerns the development of a system for the professional training of strategic communication specialists. NATO's experience demonstrates that the effectiveness of strategic communication depends to a considerable degree on the availability of trained personnel possessing interdisciplinary competencies in military command, communication, informational analysis, psychology, digital technologies, and international relations. For the Armed Forces of Ukraine, it is necessary to establish a multi-tiered system of personnel training. At the basic level, all officers and commanders should acquire knowledge of the role of the information environment in contemporary warfare and of the principles of strategic communication. At the specialized level, it is necessary to ensure the training of strategic communication officers, public affairs specialists, analysts of the information environment, and specialists in countering information-psychological operations. Also important is the development of joint

ISSN 2815-3324 Online, ISSN 2535-0358 Print

training programs with NATO member states and the use of the experience accumulated by the Alliance's relevant training centers.

One of the most complex issues remains the assessment of the effectiveness of strategic communication, since communicative effects are often long-term and indirect in character. One of the principal problems of strategic communication is the difficulty of determining its effects, since the results of communicative activity frequently emerge only over the long term and are predominantly qualitative in nature. Assessment should not, therefore, be confined to the number of publications, views, or informational messages. In NATO practice, increasing attention is being devoted to a three-tiered system of assessment: (1) informational activity (the quantity and quality of measures undertaken, audience reach, speed of response); (2) perception (the level of trust, shifts in public opinion, the dynamics of narratives); and (3) behavioral effects (changes in the behavior of target audiences, support for state policy, and a reduction in the effectiveness of hostile information operations) — an approach consistent with the logic of the behaviour-centric approach embedded in AJP-10.1. For Ukraine, an urgent task is the development of its own evaluation system based on this logic, supplemented by technological tools for monitoring the media space, analyzing social networks, and forecasting informational threats, including through the use of big-data analytics and artificial intelligence.

The implementation of this five-level institutional model creates the conditions under which the operational model can be consistently applied in practice: doctrinal clarity removes terminological confusion; organizational integration ensures unity of coordination; the operational inclusion of strategic communication in planning makes it possible to realize the principle that "actions communicate no less than words"; personnel training supplies the human resources needed to execute the cycle; and the assessment system closes the feedback loop. The transition from the fragmented use of individual communicative instruments to a fully-fledged, institutionally integrated system of strategic communication thus corresponds to the contemporary requirements of hybrid warfare and creates the preconditions for strengthening Ukraine's informational resilience under conditions of prolonged security confrontation.

## 4. CONCLUSIONS

Under present-day conditions of transformation in the character of armed conflicts, in which the information space has become one of the key domains of confrontation, strategic communication has acquired the status of a critically important element in ensuring a state's national security and defense capability. The present study was directed toward a comprehensive analysis of the theoretical foundations, structural components, functional problems, and prospects for the development of strategic communication in the military sphere. The results obtained confirm that contemporary war is waged not only over territory and resources but also over perception, trust, public support, and a state's capacity to construct and defend its own strategic narratives.

The study established that strategic communication in the military context must be understood as a systemic managerial function that ensures alignment among a state's actions, its military decisions, and its communicative processes. Unlike the traditional model of informational activity, oriented predominantly toward the dissemination of messages, strategic communication entails the comprehensive management of the information environment, the construction of targeted meanings, and the achievement of defined cognitive and behavioral effects among relevant audiences.The theoretical analysis made it possible to clarify the relationship between strategic communication and adjacent concepts — public affairs, information operations, and psychological operations. It was established that public affairs ensures open communication between military structures and society and the media; information operations are directed toward coordinating influence on the information environment; and psychological operations are employed to achieve specific psychological effects among defined audiences. At the same time, it is strategic communication that functions as the integrating mechanism, ensuring the coordination of these lines of activity in accordance with the strategic objectives of the state and its armed forces. To operationalize this integrative logic at the level of a specific operation, the study proposed an original

analytical instrument which represents strategic communication as a continuous five-stage cycle (analysis, planning, integrated application, action, and assessment) rather than as a set of parallel, loosely connected functions.

Analysis of the experience of the United States, NATO member states, and Ukraine demonstrated that the development of strategic communication constitutes a direct response to the changing nature of contemporary conflict. NATO practice shows that the effectiveness of strategic communication is determined not by the presence of discrete communicative units but by the degree of their integration into the system of military command. At the same time, the experience of the Russo-Ukrainian war confirmed that informational superiority, the capacity to counter disinformation, and the ability to construct persuasive strategic narratives can directly affect the course and outcomes of armed confrontation. The examination of the functional components of strategic communication showed that their effectiveness is secured through the interaction of public affairs, cooperation with civilian actors, information and psychological operations, and digital communication. In contemporary military operations, these components cannot be treated in isolation, since only their synchronized application makes it possible to ensure consistency among military actions, official messaging, and the intended strategic effects.

The analysis of the problems involved in implementing strategic communication in the Armed Forces of Ukraine identified the principal groups of challenges — doctrinal, organizational, personnel-related, technological, and methodological — and systematized them according to their underlying causes, potential consequences, and recommended solutions (Table 1). Among the most significant of these problems are the insufficient integration of strategic communication into operational planning processes, the need for further improvement of the regulatory framework, the absence of a fully developed system for training specialized personnel, and the difficulty of assessing the effectiveness of communicative activity, given that its results cannot be reduced solely to quantitative indicators.

The results of the study confirm the hypothesis advanced at the outset: that the effectiveness of strategic communication in the armed forces is determined above all by the degree of its institutional integration into command processes, rather than merely by the presence of individual informational instruments or specialized units. This conclusion is substantiated not only theoretically but also empirically: the comparative analysis of the Russian and Ukrainian approaches to strategic communication during the ongoing war (Section 3.3) showed that Russia's high level of coordination among individual instruments has not translated into strategic effectiveness, since its practical conduct systematically contradicts its own narratives, whereas Ukraine's comparatively more consistent — albeit institutionally uneven — implementation of the full communicative cycle has been accompanied by a sustained high level of public trust in the Defense Forces (92–94 percent in 2024–2025, according to KIIS data), even as recurrent institutional restructuring at the level of the coordinating ministry indicates that this institutional integration remains incomplete. This implies that the further development of the strategic communication system of the Armed Forces of Ukraine must entail a comprehensive institutional transformation — from the improvement of doctrinal documents and organizational procedures to the cultivation of a new culture of military command in which the informational dimension is taken into account in every strategic decision.

Taking into account the experience of NATO member states and the particularities of Ukraine's security environment, the study proposed the principal directions for improving the strategic communication system of the Armed Forces of Ukraine. These include: adapting the regulatory and doctrinal framework to Alliance standards; incorporating strategic communication into the operational planning cycle; establishing a multi-tiered system for the training and professional development of specialists; developing technological capabilities for analyzing the information environment; and constructing a system for assessing communicative effects based on cognitive, behavioral, and strategic indicators.

The proposed model for improving strategic communication in the Armed Forces of Ukraine entails a transition from the fragmented use of individual communicative measures to a comprehensive system for managing the information environment, integrated into the processes of military planning and

decision-making. The implementation of such a model would contribute to strengthening the state's informational resilience, deepening public trust in the security and defense sector, reinforcing international support for Ukraine, and building the capacity to counter contemporary hybrid threats effectively.

The study is subject to certain limitations that warrant acknowledgment. The empirical analysis relies substantially on open-source materials, doctrinal documents, and publicly available sociological data, rather than on internal institutional data regarding the actual planning and coordination procedures of the Armed Forces of Ukraine, access to which is restricted for reasons of operational security. The proposed IMSCM and the five-level institutional model should accordingly be regarded as analytical frameworks derived from the synthesis of doctrinal sources and open empirical material, the practical validation of which would require further field-based or institutional research.

Promising directions for further research include the development of practical methodologies for assessing the effectiveness of strategic communication in the military sphere, the study of the influence of digital technologies and artificial intelligence on the transformation of information confrontation, and the formulation of models for adapting NATO experience to the specific characteristics of Ukraine's defense system.

**AI Use Declaration.** *This article was originally written by the author in Ukrainian. AI-based tools were used to assist in translating the manuscript into English. The author reviewed and edited the resulting translation for accuracy, terminology, and academic style, verified all sources and citations against the original materials, and confirms that the research, analysis, and conclusions presented are entirely the author's own. The author takes full responsibility for the accuracy, originality, and integrity of the final text.*

## REFERENCES

Barovska, A. V. (2015). Strategic communications: NATO experience. Strategic Priorities, (1), 147–152.

Bjola, C., & Pamment, J. (Eds.). (2019). Countering online propaganda and extremism: The dark side of digital diplomacy. Routledge.

Bolt, N. (2011). The violent image: Insurgent propaganda and the new revolutionaries. Columbia University Press.

Cabinet of Ministers of Ukraine, National Security and Defense Council. (2020). Указ Президента України № 392/2020 «Про Стратегію національної безпеки України» [Decree of the President of Ukraine No. 392/2020, "On the National Security Strategy of Ukraine"].

Cabinet of Ministers of Ukraine, National Security and Defense Council. (2021). Указ Президента України № 121/2021 «Про Стратегію воєнної безпеки України» [Decree of the President of Ukraine No. 121/2021, "On the Military Security Strategy of Ukraine"].

Cabinet of Ministers of Ukraine, National Security and Defense Council. (2021). *Указ Президента України № 685/2021 «Про Стратегію інформаційної безпеки України»* [Decree of the President of Ukraine No. 685/2021, "On the Information Security Strategy of Ukraine"]. https://www.president.gov.ua/documents/6852021-41069

Cabinet of Ministers of Ukraine. (2024). Постанова № 1028 від 6 вересня 2024 р. «Про перейменування Міністерства культури та інформаційної політики України» [Resolution No. 1028 of September 6, 2024, "On renaming the Ministry of Culture and Information Policy of Ukraine"].

Cabinet of Ministers of Ukraine. (2025). Постанова № 1396 від 29 жовтня 2025 р. «Про перейменування Міністерства культури та стратегічних комунікацій України» [Resolution No. 1396 of October 29, 2025, "On renaming the Ministry of Culture and Strategic Communications of Ukraine"].

Center for Strategic Communications and Information Security of Ukraine (SPRAVDI). (n.d.). *Універсальний інструмент: посібник з розробки комунікаційних кампаній* [Universal tool: A guide

to developing communication campaigns]. https://spravdi.gov.ua/universalnyj-instrument-czentr-strategichnyh-komunikaczij-vypustyv-posibnyk-z-rozrobky-komunikaczijnyh-kampanij/

Detector Media. (2026). *Центру стратегічних комунікацій та інформаційної безпеки 5 років* [The Center for Strategic Communications and Information Security turns 5]. https://detector.media/infospace/article/248734/

Ecker, U.K.H., Spearing E.R., DiResta R., & Lewandowsky, S. (2026). Misinformation as strategy: Epistemic consequences and the undermining of shared truth. Trends in Cognitive Sciences. https://doi.org/10.1016/j.tics.2026.06.009

Ehrl, M. (2023). Understanding Russia's Disinformation Narratives about Ukraine: A Ratio-Oriented Approach to Strategic Crisis Narratives. *ESSACHESS*. https://doi.org/10.21409/QW1H-BD11

Gorbulin, V. P. (2017). World hybrid war: Ukrainian front [Monograph]. National Institute for Strategic Studies.

Hallahan, K., Holtzhausen, D., van Ruler, B., Verčič, D., & Sriramesh, K. (2007). Defining strategic communication. *International Journal of Strategic Communication, 1*(1), 3–35. https://doi.org/10.1080/15531180701285244

Holtzhausen, D. R., & Zerfass, A. (Eds.). (2015). *The Routledge handbook of strategic communication*. Routledge. https://doi.org/10.4324/9780203094440

Karpchuk, N., Yuskiv, B., Shuliak, A., & Fedoniuk, S. (2023). Стратегічні комунікації ЄС [EU strategic communications]. Vezha-Druk.

Kyiv International Institute of Sociology. (2025). Омнібус, листопад–грудень 2025 р. [Omnibus survey, November–December 2025] [Data set].

Law of Ukraine. (2018). Про національну безпеку України [On national security of Ukraine] (with amendments).

Mammadov, R. (2026). Sincere or Strategic: Probing Russian Journalists' True Convictions Behind Ukraine War Coverage. Journalism & Mass Communication Quarterly, 0(0).

Ministry of Defence of Ukraine. (2020). *Strategic Communications Doctrine of the Ministry of Defence of Ukraine and the Armed Forces of Ukraine*. https://mod.gov.ua/en/about-us/ministry-staff-en/department-of-strategic-communications

National Academy of the Security Service of Ukraine. (2024). *Стратегічні комунікації в умовах війни: погляд від волонтера до науковця* [Strategic communications in wartime: A view from volunteer to scholar] [Collective monograph]. https://msj.ukma.edu.ua/wp-content/uploads/2024/01/Stratehichni_komunikatsii_v_umovakh_hibrydnoi_viiny_-_pohliad_vid_volontera_do_naukovtsia.pdf

NATO Standardization Office. (2022). AJP-10.3, Allied joint doctrine for military public affairs (Edition A, Version 1).

NATO Standardization Office. (2023a). AJP-10, Allied joint doctrine for strategic communications (Edition A, Version 1).

NATO Standardization Office. (2023b). AJP-10.1, Allied joint doctrine for information operations (Edition A, Version 1).

NATO Strategic Communications Centre of Excellence. (2020–2024). *Annual reports and research papers on strategic communications*. https://www.act.nato.int/article/nato-stratcom-coe/

NATO. (2021). NATO warfighting capstone concept. NATO.

NATO. (2022). *NATO 2022 strategic concept*. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2023/03/03/nato-2022-strategic-concept

NATO. (2023). A comprehensive and coordinated approach to strategic messaging. NATO Review.

Nye, J. S. (2011). The future of power. PublicAffairs.

Paul, C. (2011). Strategic communication: Origins, concepts, and current debates. Praeger.

Paul, C., & Matthews, M. (2016). *The Russian "firehose of falsehood" propaganda model: Why it might work and options to counter it*. RAND Corporation. https://www.rand.org/pubs/perspectives/PE198.html

Pocheptsov, G. G. (2008). Strategic communications: strategic communications in politics, business, and public administration. Alterpres.

Pocheptsov, G. G. (2015). Contemporary information wars. Kyiv-Mohyla Academy.

Popova, T. V., & Lipkan, V. A. (2016). Strategic communications: A dictionary (V. A. Lipkan, Ed.). FOP O. S. Lipkan.

Pynnöniemi, K., & Tolvin, A. (2025). Reconstructing Kremlin strategic deception: the logic of disinformation narratives during the first phase of the full-scale invasion of Ukraine. *The Journal of Slavic Military Studies*, *38*(3), 299–320. https://doi.org/10.1080/13518046.2025.2548727

Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.

Salnikova, O. F., Izhutova, I. V., & Kushnir, V. O. (2020). Fundamentals of strategic communications in national security and defense [Textbook].

Storozhenko, L., & Petkun, S. (2021). Strategic communications: Conceptual approaches and basic principles. *Society. Document. Communication*, (11), 386–403. https://doi.org/10.31470/2518-7600-2021-11-386-403

Syvak, T. (2018). Theoretical analysis of the concept of "strategic communications" in public administration. Теорія та історія державного управління.

Syvak, T. V. (2019). Strategic communications in the system of public administration of Ukraine [Monograph]. NAPU.

Georgiev, V. (2026). Unity under pressure: The European Union's foreign policy after 24 February 2022. Politics & Security, 16(2), 64–75. https://doi.org/10.54658/ps.28153324.2026.16.2.pp.64-75

# UNITY UNDER PRESSURE: THE EUROPEAN UNION'S FOREIGN POLICY AFTER 24 FEBRUARY 2022

Vasil Georgiev
Department of Global and National Security
Academy of National and Information Security
Plovdiv, Bulgaria
https://orcid.org/0000-0003-4246-0622
v.georgiev@anis.bg

**Abstract.** *This article examines the dynamics of European foreign policy unity after February 24, 2022. The main question is whether the unity demonstrated after the Russian aggression against Ukraine represents a sustainable institutional consolidation or a temporary mobilization under the pressure of a crisis. The study uses a legal-institutional and political-analytical approach, examining the Common Foreign and Security Policy through five tests: aid to Ukraine, the trade pressure of the Donald Trump administration, the Israel-Gaza conflict, the crisis around Iran, and the Greenland case. The analysis shows that the EU can formulate a common position when external pressure is strong enough, but it has difficulty turning this position into an independent strategic capability. The main conclusion is that future European foreign policy should seek a model of interaction between willing states that overcome the paralyzing effect of unanimity without destroying the institutional architecture of the Union.*

**Keywords:** CFSP; European Union; strategic autonomy; foreign policy; European security; veto power, variable geometry.

## 1. INTRODUCTION

This article examines the dynamics of cooperation within the EU in the international environment that was formed after 2022. It is characterized by an initial crisis consolidation caused by Russian aggression, but subsequently transformed into a more difficult - procedural and political - maintenance of a common position regarding security issues in the Middle East and the policy of Donald Trump.

The purpose of the analysis is to analyze the evolution of the existing institutional framework of cooperation and to outline the characteristics of possible models of future development of this cooperation.

The CFSP has an intergovernmental character; that is, each state can "press the brake" and thereby oppose the adoption of a particular decision. If, when this policy was created in the early 1990s, the Member States numbered 12, today they are 27, which means 27 potential brakes on any given decision. Among the interested public, as well as among some scholars, there are serious doubts about the potential of this policy, including its effectiveness vis-à-vis Russia (Thaler, 2020, p. 4).

The most significant circumstances that hinder the establishment of an integrated EU foreign policy can be summarised as follows:

a) The EU is a union of states which, especially after the enlargements following the 1990s, are located in different regions. This predetermines different—whether significant or less significant—foreign-policy priorities and different approaches to security (Lonardo, 2023a, p. 33).
b) Even when there are no substantial differences among the Member States on a specific foreign-policy issue, foreign policy and defense remain areas closely linked to state sovereignty (from the perspective of the external autonomy of the state). Therefore, the

transfer of competences to the EU is perceived as a potential limitation of that sovereignty—something that states are not readily prepared to accept.

c) The EU cannot independently guarantee its defense security and relies to a significant extent on NATO and the United States.
d) The EU's energy dependence and the differences in the energy needs and vulnerabilities of the Member States create divergent political incentives and hinder the formation of a unified foreign-policy position.

Therefore, the willingness of all Member States to be part of one union does not mean that there is consensus as to what the foreign policy of that union should be.

## 2. MATERIALS AND METHODS

The study uses a qualitative legal-institutional and political-analytical approach. The analysis is based on the provisions of EU primary law on the CFSP, on acts and public positions of the EU institutions, as well as on relevant scientific literature on European foreign policy, strategic autonomy and transatlantic relations.

The method is comparative and case-oriented: by sequentially examining several foreign policy crises after 2022, recurring limitations in the EU's ability to act as a single strategic actor are deduced.

## 3. THE WAR IN UKRAINE AS A MOMENT OF CRISIS UNITY

In 1996, Schmitter pointed out that the way the EU functions is different from that of the member states, in that the EU, although it has no strategic plan, its actions emerge in an improvised manner from tactical responses to concrete and immediate problems (Schmitter, 1996, p. 2).

This characteristic is particularly visible after February 24, 2022, when Russia's attack on Ukraine placed European countries in a completely different security environment. And despite the lack of a coherent policy and strategic approach of the EU in its relations with Russia. (Lonardo, 2023b, pp. 39 ff.), the EU's response was unified (including Hungary).

This unity was the result not of a common strategic, well-thought-out idea of the EU, but of a combination of various factors that determined the political moment at the beginning of 2022:

1. The war in Ukraine was a shocking and indisputable moral case, in which the aggressor and the victim were clearly defined. This left no room for disagreement among European countries in their response.
2. A unifying factor was the common understanding by Member States of the risk posed by a Russian invasion, reinforced by fears of territorial aggression in Europe - especially for the Baltic states, Sweden, Finland, Romania, Poland.
3. Unity was not only at the EU level, but also at the transatlantic allies – the US, the UK, Turkey, Norway, etc. Thus, the transatlantic framework acted as an additional stabilizing factor for unity.
4. Last but not least, the determination of this unity, motivation and joint action would have remained at a lower level if the Ukrainian resistance had not proved so determined. The transformation of Ukraine from a victim to a defender of the European order was an additional incentive for the united position of the EU Member States.

The war in Ukraine demonstrated the need for a unified policy towards Russia, placing this security issue at the forefront, ahead of all other priorities. However, the change in the factors mentioned above also affected the initial unity.

Russia launched its military invasion of Ukraine on the assumption that the EU was a weak and dependent foreign policy actor whose unity could easily be paralyzed. This proved to be a miscalculation. The war led to the consolidation of the EU and an increase in its role in European security.

The initial manifestations of this unity are remarkable.

The EU has adopted economic, financial and trade restrictive measures, which constitute the most severe sanctions ever taken by the EU against a third country. (Council of the European Union, 2026) The EU and its Member States have also provided significant economic, humanitarian and military assistance, as well as assistance to support refugees in the EU. (European Council, 2026).

The EU's decision to use the European Peace Facility – a fund to support and finance EU and partner operations – to supply military equipment, including lethal weapons, to Ukraine represents one of the most significant changes in EU foreign policy. (Lonardo, 2023b, p. 1) The EU's supply of lethal weapons to a third country was unprecedented in EU history.

The war in Ukraine has led to greater coherence on other related issues – the energy transition, refugee policy, criminal law, relations with China, relations with African countries. Global challenges are harbingers of a conceptual shift in the understanding of the essence and character of European foreign policy, and the war in Ukraine is the tectonic event that has led to the realization of changed priorities for the future.

The main effect of the war in Ukraine in terms of energy was a sharp reduction in the EU's energy dependence on Russia. By 2022, the Russian Federation was a significant supplier of solid fossil fuels and the largest importer of oil and natural gas to the European Union. The German government's decision to halt the Nord Stream 2 project and the drastic reduction in the volume of fossil fuels imported from Russia are a harbinger of a new geopolitical relationship between the EU and Russia.

In the area of military cooperation, changes are the most difficult to come by. The positive thing about solving the problems with the EU's defense vision is that the processes have already begun – they began after the adoption of the Global Strategy in 2016, the problems with the Strategic Compass were identified, and initiatives related to the Common Security and Defense Policy have been launched. (Scazzieri, 2020, p. 2).

The 2023 ASAP Regulation, aimed at accelerating the production of ammunition and missiles in the EU, in relation to the needs of Ukraine and the depletion of European stocks, also fits into this process. In 2025, this logic was expanded through SAFE, a loan instrument of up to €150 billion for common defense procurement, and through the ReArm Europe/Readiness 2030 plan, which aims to mobilise over €800 billion to increase Europe's defense readiness.

These initiatives show that the EU is gradually building an industrial-financial framework for defense, but they do not yet create an independent European military capability. Progress cannot be rapid, as it concerns joint planning, development and acquisition of military capabilities, as well as actions to create military mobility within the EU. The EU can mainly provide the framework for cooperation in the defense industry – for example, by creating a common market and by limited funding of certain projects. However, the contracting authorities are national governments and it is they, along with the military and industry, who determine the intensity of this cooperation.

## 4. FROM CRISIS TO DIFFICULT UNITY

European unity after 2022, however, is unity produced by the weight of the crisis; it is not the result of strategic maturity. Therefore, changes in the factors identified above also affected the initial unity, and after the first shock it became clear that the factors limiting the CFSP—national priorities, limitations in military capabilities and energy differences—continued to exert influence.

Thus, European unity after 2022 placed old contradictions under new pressure. They are clearly visible in five cases: assistance to Ukraine, Trump's trade pressure, Israel–Gaza, the United States–Iran crisis, and Greenland.

The first test was Hungary. Then Hungarian Prime Minister Viktor Orbán turned the right of veto into a systematic instrument of pressure. He did not block bilateral assistance from Germany, France or Poland

ISSN 2815-3324 Online, ISSN 2535-0358 Print

to Ukraine, but rather the common decision without which the EUR 90 billion loan could not be issued. The veto thus ceased to be only a guarantee of national sovereignty and became a bargaining tool.

The second test was Donald Trump's trade policy. His administration confronted the EU with a choice between accommodation and reciprocity in trade relations. The trade agreement reached in July 2025 was blocked months later after new tariff threats. France insisted on a tougher response; Germany was more cautious because of the dependence of its exports on the American market; Italian Prime Minister Giorgia Meloni described the tariffs as a "mistake", but avoided open confrontation. There was unity, but it was reactive—it appeared when external pressure from the United States required it.

The third test was Israel–Gaza. Here the rupture was within the EU itself. The European Commission found grounds to consider that Israel had violated its obligations under Article 2 of the Association Agreement and proposed a partial suspension of trade preferences. The Council, however, did not reach unanimity on a full suspension. Spain, Ireland, Belgium and Slovenia insisted on tougher measures; Germany and Italy remained more cautious. Thus the EU formulated a position that exceeded its actual capacity for action.

The fourth test was the United States–Iran war of 2026. In this crisis, the EU turned from a participant into an observer of a crisis that directly affected European security but developed beyond its control.

The background—the Iranian nuclear deal—illustrates the diplomatic weight of the EU, insofar as the EU, through the High Representative, France, Germany and the United Kingdom, participated in the elaboration of this arrangement for the non-proliferation of nuclear weapons. After the United States withdrew from the deal in 2018, the EU position remained formally united but practically indefensible, since the US withdrawal also meant the imposition of secondary sanctions on European companies trading with Iran—something the EU could not prevent. This in practice rendered the agreements reached largely meaningless.

During the crisis of 2025–2026, the foreign ministers of France, Germany and the United Kingdom, together with the EU High Representative, called for restraint, a return to diplomacy and a solution that would ensure that Iran did not acquire nuclear weapons. In March 2026 there was already a position on behalf of the EU condemning Iranian attacks and insisting on de-escalation, international law, the protection of civilians and freedom of navigation, including through the Strait of Hormuz. Taken by itself, however, this position cannot be described as complete—there was no unified position on the US intervention—or as strategic, since the EU had limited influence over the development of the crisis. The opposite, however, is not true: the crisis had a major impact on the EU, since the EU would be a serious loser from the closure of the Strait of Hormuz.

The fifth test was Donald Trump's claims to Greenland. It was particularly revealing because it concerned the relations of the EU and the Member States with the United States—the traditional guarantor of European security. When the American president linked his claims to Greenland with tariff pressure on European exports, the EU reacted in a more consolidated manner: the European Parliament postponed the ratification of the trade agreement, and European leaders spoke of unity. Yet here, too, it was clear that the EU's capabilities lay in the field of soft power—statements, the delaying of agreements and countermeasures—without capabilities that could prevent unilateral action by Donald Trump.

All five cases confirm the thesis that European unity after 2022 is activated under pressure and fades when that pressure diminishes. None of the cases demonstrates proactive, institutionally sustainable consolidation; each reveals at least one of the old structural limitations: the veto of a small state (Slovakia or Hungary), trade asymmetry (the United States), historical and value-based cleavages (Israel), energy dependence (Iran) or military helplessness (Greenland).

The absence of a strategic orientation on the main security problems—Russia, the Middle East, Greenland and relations with the United States—cannot be compensated for solely by unity among European states in crisis situations. Policy must be consistent in crisis, post-crisis and non-crisis environments alike. In this sense, a strategy must include reflection not only on actions aimed at ending a

crisis, but also on actions after it has ended: what Europe's strategic objectives are towards Russia, the Middle East and the United States; what place these actors will have in a possibly transformed security environment; and how Europe will protect its interests in that environment. At present, these questions do not have a unified European answer.

## 5. TRUMP 2.0 AND THE PROBLEM OF EUROPEAN DEFENSE

The disagreements between the EU and the US regarding NATO are another problematic node in the EU's foreign policy that deserves special attention. They directly affect the need for a unified foreign and security policy of the Union, since an effective foreign policy implies a combination of soft and hard power. It is the latter that remains the EU's weakest point: the Union has significant regulatory, economic and diplomatic weight, but does not possess an independent military capability commensurate with its foreign policy ambitions and potential.

In these relations, there is a lasting contradiction that has been evident since the 1950s.

On the one hand, the majority of EU member states want more autonomy for European defense, both politically and militarily. Such autonomy can be achieved through more investment, which would lead to a strengthening of the European pillar of NATO.

In practice, however, the idea of European autonomy is supported by the US with the formula "yes, but" — yes, Europe should have strategic independence and take more responsibility for its defense, but this carries the risk of duplication, competition, and ultimately weakening of NATO structures (Howorth, 2007, p. 237).

Thus, the conundrum of European defense can be summarized as follows: how can more EU not mean less NATO and how can more NATO not mean less EU?

Donald Trump's victory in the 2024 presidential election, while confirming the need for independent development of European defense, has added further conceptual ambiguity to this conundrum. This ambiguity relates to the different understanding of the role of NATO — whether the Alliance is primarily a defense alliance for collective defense, or a military alliance in which partners should support the leading ally in its foreign policy and military initiatives. This conceptual difference defines the Euro-Atlantic relationship in two very different ways.

Donald Trump's understanding is closer to the idea that NATO is not so much a defensive alliance for collective defense as a military alliance in which partners should support the leading member in its foreign policy and military initiatives - for example, in the case of Iran. It is significant, however, that Washington has not offered similar reciprocity regarding Ukraine, where it is precisely the European allies who have the most direct interest in support against Russian aggression.

From a formal point of view, the North Atlantic Treaty Organization is not a military alliance in the sense of an alliance of states directed against a specific third state or community. NATO is an organization for collective defense, established on the basis of Art. 51 of the UN Charter. In the literature, one can also find the understanding that the original construction of NATO was precisely a military alliance (Milward, 2009, p. 104; Kissinger, 2014, pp. 403 ff.; Kissinger, 2002, p. 300). Whatever the role of NATO at the beginning and during the Cold War, at present its function is primarily defensive.

The processes of understanding the need for Europe to take on a greater role in protecting its security began immediately after the end of the Cold War with the Maastricht Treaty of 1992. Achieving "strategic autonomy" has been an EU goal since the launch of the European Security and Defense Policy with the Saint-Malo Declaration of 1998 (Joint Declaration on European Defense, 1998). Strategic autonomy means that the EU should achieve the ability to take responsibility for its security and foreign policy by building the necessary organizational, military and operational capabilities.

At first glance, it seems that the EU has taken the necessary steps even before 2022. These include the Permanent Structured Cooperation, the European Defense Fund, the European Peace Facility, the Coordinated Annual Review on Defense, and others. In 2022, the Strategic Compass for Security and

Defense was adopted, in 2023 — the ASAP Regulation aimed at supporting the production of ammunition (Regulation (EU) 2023/1525, 2023), and in 2024 — a new strategy for the European defense industry (European Commission & High Representative, 2024). In connection with the Russian aggression in Ukraine, the Regulation establishing the Instrument for strengthening the European defense industry through joint procurement (Regulation (EU) 2023/2418, 2023) was also adopted. In 2024, the adoption of a European Defense Industrial Programme was also proposed (European Commission, 2024).

All these initiatives illustrate the high priority of defense on the European agenda. However, the fundamental problems associated with the configuration of European defense suggest that even if there is political will, these processes are likely to take more than a decade. The creation of a common defense market, joint acquisition of capabilities, interoperability and military mobility across the EU are essential prerequisites for building a common defense.

The rationale for EU defense policy is clear: more investment, joint projects and the creation of a common defense market (Varga, 2024, pp. 73–108). Positive developments in this direction are already underway, particularly in the areas of military mobility (Chihaia, 2024, p. 3) and joint acquisition of capabilities (Andersson, 2023, p. 2).

The lack of military capabilities, the impossibility of full military mobility, fragmented national defense markets, duplication of capabilities, insufficient cooperation in the defense industry, and the lack of interoperability are among the main problems that European defense must address. Paradoxically, the annexation of Crimea in 2014 did not act as a sufficient catalyst for political will (Varga, 2024, p. 82). Political decisions for additional investments were only taken under the pressure of the events of 2022.

NATO and the EU are communities of shared values (Sloan, 2016, p. 32). At the same time, it is fair to assess that they complement each other, since the EU does not have sufficient military capabilities and NATO does not have an independent strategic vision in the European sense (Duff, 2022, p. 98). To achieve this goal, Duff proposes the creation of an additional organization — the European Security Council — as an intergovernmental instrument that would connect the EU, NATO, and associated European countries, while keeping the United States involved in European security.

In summary, EU-NATO cooperation does not imply confrontation between the two organizations, but rather the building of a European defense capacity that strengthens, not weakens, Euro-Atlantic security. However, this capacity must also be able to act independently - as a separate but functionally linked structure to Euro-Atlantic security.

## 6. DISCUSSION: TOWARDS A NEW INSTITUTIONAL STRUCTURE

From the above, it can be concluded that after 2022, the CFSP not only does not contain a satisfactory mechanism for the successful implementation of foreign policy, but in certain cases it also becomes an obstacle to foreign policy action - both of the EU as a whole and of the Member States that wish to act faster and more decisively.

The reason for this is institutional, insofar as the competences in this area are located on the two-dimensional field of "integration – intergovernmentalism", without finding a sustainable formula between common action and national autonomy. A similar conclusion is reached by Andrew Duff (Duff, 2022, p. 95 et seq.), who sees the EU as an unfinished political construct between confederation and federation.

According to the author, foreign policy can neither be fully communitarianized nor purely national, although institutionally the CFSP tends more towards the latter. The EU's foreign policy is institutionally built on the national, with conceptual commonality also passing through the awareness of problems not only as national, but also as European. This allows in certain cases the member states to adopt the common European position, although it does not always fully coincide with their immediate national comfort. Therefore, the successful combination of "national – community" is the basis, on the one hand, of the awareness of the national interest as part of the European one, and on the other – of the possibility of independent protection of the national interest.

An essential condition for a successful foreign policy is that states have a wider range of options to resolve a specific foreign policy problem: not to be deprived of the right to act independently, but also not to be blocked when they wish to act collectively. In this sense, the EU should act as an amplifier of their strategic interests, and where unity is required, it should not undermine the very foundations of their national foreign policy.

The CFSP does not offer a clear institutional answer on how to achieve this balance. On the contrary, the current system is not only weak as a mechanism for joint foreign policy due to the veto power, but in certain cases it also weakens the individual foreign policy of the Member States.

The weaknesses to which the right of veto gives rise for collective foreign policy are widely known: delayed reactions, dilution of common positions, blocking of sanctions or assistance, the transformation of foreign policy into an instrument of domestic or bilateral pressure, and the creation of an impression of strategic indecision on the part of the EU.

Less obvious are the negative influences of the CFSP for national foreign policy.

When a timely decision must be taken on a particular problem, the EU's foreign-policy framework places states under pressure to wait for a common position rather than to develop their own policy or a coordinated position with a group of like-minded states in good time. A state may thus find itself in an uncomfortable intermediate position: it no longer acts entirely alone, yet it does not receive an effective common European framework that would amplify its action.

Another problem arises when a Member State uses its veto on one foreign policy issue to achieve entirely different political aims. This was the example of 21 September 2020, when the EU Foreign Affairs Council failed to reach a decision on imposing restrictive measures against Belarus because Cyprus blocked the sanctions, insisting that the EU simultaneously take measures against Türkiye because of its drilling activities in the Eastern Mediterranean.

A similar risk is the possibility that a third country may direct pressure at one or several Member States to prevent a common EU decision. Under the principle of unanimity, it is sufficient for that pressure to succeed vis-à-vis one state to block the entire common position. In this sense, the CFSP resembles a fortress with twenty-seven gates: not all gates need to be opened for the defense to be breached; one gate left unlocked is enough.

All this indicates that the most serious limitation to the operation of the CFSP remains the requirement for unanimity in decision-making.

The treaty mechanisms through which attempts have been made over the past thirty years to mitigate this restriction are cautious and difficult to implement. A partial exception is constructive abstention, which allows a member state to abstain from participating in a certain decision without blocking its adoption by the others. But in this case, the decision depends on the political willingness of the dissenting state to temporarily not interfere – for example, the dissenting leader deciding to leave the room, to "go for a coffee" so as not to block the general decision. This is more of a wishful rather than a legal guarantee.

Another substantial problem is the limited possibility for institutional upgrading of the system. Within the existing legal framework, the principle of unanimity can be overcome in two ways: through amendment of the founding treaties under Article 48 TEU, or through the use of the so-called passerelle clause under Article 31(3) TEU, which allows the European Council, acting unanimously, to determine areas of the CFSP in which the Council may adopt decisions by qualified majority.

In both cases, however, change is again premised on the unanimity of the Member States. Such unanimity is difficult to achieve, since several states oppose such reform. Even if some of them could be persuaded over time—or if governments more favourable to such change came to power in them—the political cycle in the EU constantly reproduces new sceptics.

ISSN 2815-3324 Online, ISSN 2535-0358 Print

For this reason, waiting for a pan-European "window of opportunity" for deep CFSP reform appears unrealistic. Moreover, reform is also a precondition for future enlargement, since the admission of new Member States would further aggravate the problem of achieving unanimity.

This opens the door to another alternative: new forms of interaction among willing European states outside or around the existing EU framework—a separate but functionally integrated structure (including institutions such as the Commission, the Parliament and the Court) that would allow faster political and defense action without formally destroying the institutional architecture of the Union.

Such a structure should be open both to non-EU European countries, such as the United Kingdom, Norway or Ukraine, and to member states that did not join initially but later wish to participate. It should also form the core of a global alliance of like-minded countries such as Canada, Australia, Japan, South Korea, etc.

The model should be the reverse of the CFSP model: instead of limited and blocking, it should be inclusive and non-blocking. The system should not exclude any EU Member State in advance, but the non-participation of an individual state should not become a veto over the actions of the others.

In order to be politically acceptable, such an organisation should be built on several safeguards.

First, it should have a clear organisational structure and a single representative—for example, a European foreign minister, as envisaged in the draft Constitution for Europe.

Second, participation by states should be voluntary, with the right to a limited opt-out from specific strategic initiatives. A limited opt-out does not mean that a state may at any moment freely withdraw from commitments undertaken, since this would lead to disengagement for reasons of saving money and effort. It should function as a safeguard clause for actions affecting essential national strategic interests, not as a general right of selective participation.

Third, to prevent the model from becoming an arbitrary "coalition of the willing", a threshold should be provided: if a significant share of states declare an opt-out, the decision should not be adopted.

Fourth, the actions of the organization should be linked to a pre-defined strategic framework, clear accountability and transparent financial commitments, so that flexibility does not become a cover for the domination of the largest states.

Thus, the model creates a tool for cases where some European countries already share a common strategic goal and are ready to act, without replacing national foreign policy. The main goal is to eliminate the possibility of those who are unwilling to paralyze those who are willing.

A key issue in such a model is the relationship between the "willing" and the "unwilling" and whether this could lead to a new division. The formation of groups of countries that choose to cooperate more intensively in certain areas has always been viewed with some suspicion, although the need for a "multi-speed Europe" was already mentioned in the Tindemans Report in 1975.

These concerns are not unfounded. Such a structure could create a sense of a "first" and "second" Europe, deepen mistrust between large and small states, duplicate existing EU and NATO formats, or produce decisions with unclear democratic accountability.

The proposed model differs from the concept of "multi-speed Europe", which belongs primarily to the integrational, rather than the intergovernmental, logic of the EU (Stubb, 1996, p. 288). This objection is justified if by different speeds one understands the classical model in which all countries move towards the same degree of integration, but at different paces.

In the field of foreign policy and security, however, it is not a question of different degrees of integration. It is a question of different capacities, readiness and agreement to act within the framework of an already accepted strategic goal. This idea is therefore closer to the model defined by Stubb as variable geometry than to the classic "multi-speed Europe".

In the field of foreign policy, it is not about gradually joining everyone into the same integration community. The guiding principle here is the common European strategic framework, in which a different circle of countries can participate in specific foreign policy and defense actions according to their capacity, interest, and political readiness.

On the other hand, the possibility of opt-out also gives the model certain characteristics of à la carte integration, insofar as individual countries can choose not to participate in specific actions or commitments. However, this does not make the model a purely à la carte solution, because participation or non-participation develops within the framework of a previously agreed common strategic objective, and not as a free choice of unrelated policies. It is therefore more accurate to define the model as a variable geometry with an opt-out possibility, rather than as a foreign policy "Europe à la carte".

That is, once European states have agreed on a "grand strategy"—for example, that Russian aggression is a threat to European security or that Europe must develop greater defense autonomy—it is not necessary that every subsequent operational decision be blockable by all. In this sense, the model represents a European system of differentiated strategic action: a common goal, but varying degrees of participation, commitment, and operational readiness.

The proposed system does not necessarily replace the CFSP. This is not necessary, because even now Europe's foreign policy action is not limited to the classic CFSP. Alongside it, there are several formats: the institutional format of the Council and the High Representative; the operational format of CSDP missions and operations; the flexible internal format of PESCO and Art. 44 TEU; the diplomatic format of E3/EU; ad hoc formats outside the EU, such as the Normandy Format and coalitions of the willing; and the broader political format of the European Political Community.

However, these formats are either too tied to unanimity or too weakly institutionalized. The creation of a new European organization would make sense precisely as a way to channel and institutionalize such practices. The existence of multiple unrelated formats is not evidence of flexibility in itself, but rather a symptom of a lack of a unified policy. and a factor in excluding countries from the decision-making process and acting.

If Europe continues to rely solely on unanimity, it risks preserving the architecture of a common voice but losing the capacity for common action. However, if it builds an institutionalized variable geometry of strategic action, it can both preserve the inclusive nature of the European project and restore its capacity for timely response.

However, the functionality of such a project is not the only criterion for assessing its feasibility. According to the constructivist reading of Leuffen, Rittberger and Schimmelfennig (Leuffen et al., 2013, pp. 198–206) of the failure of the creation of a European Defense Community in the 1950s, it stems from a clash between the European idea of supranational defense and the national understanding of the army as a symbol of independence.

The parallel with the current European dilemma is apt, as it, too, represents a clash between two visions — the "sovereignist" and the "community" one.

According to the constructivist explanation, the change in public opinion and political support for the European Defense Community cannot be understood solely through changes in national interests, the balance of power, or the positions of the industries concerned (arguments that are still debated today as central to the understanding of a unified foreign policy). These factors are important and correspond, respectively, to the intergovernmental, realist, and liberal-intergovernmental schools.

Constructivism, however, adds a deeper layer of explanation: the very understanding of national interest, of an acceptable balance of power, and of an acceptable price for integration is shaped through notions of identity. Therefore, the failure of the European Defense Community can be understood not simply as an institutional or strategic failure, but as a failure to legitimize European defense from the perspective of the identity of Western European societies. Societies create defensive structures to protect political communities with which they identify and which they perceive as "theirs."A constructivist reading

is important for understanding the future European foreign policy and security structure. If it is presented as a replacement for the nation-state or as a covert federalization of defense, it risks repeating the identity problem of the ill-fated European Defense Community.

Another, more recent example of a misconstrued European construction is the 2004 draft Treaty establishing a Constitution for Europe. It largely played out the conflict between the same two identity visions. In a significant part of the public debate, the draft was perceived as a symbolic step towards European statehood. The use of the term "constitution" activated identity fears — that the nation-state and sovereignty would be replaced by a supranational center. In this sense, the failure of the Constitutional Treaty was a result of the way it was politically narrated and socially perceived, rather than its content. Supporting this understanding is the fact that a significant part of this content was subsequently incorporated into the Lisbon Treaty. This happened much more unproblematically, when the most visible European identity markers in the terminology were replaced with more neutral terms.

Therefore, the new structure must satisfy two competing and intertwined identity visions - to be legitimized as part of the European project, but not as a renunciation of national sovereignty: linked to the EU and its institutions, open to European countries outside the EU, but structured in such a way that states retain the feeling that they are participating voluntarily in a common instrument to reinforce, rather than replace, their national foreign policy. Put simply, from a constructivist perspective, the success of such an organization will depend not only on whether it is functionally useful, but also on whether it is correctly narrated.

## 7. CONCLUSION

Foreign policy and security are areas where integration is difficult to achieve because the differences between member states go deeper than simple political preferences. They affect strategic culture, understanding of sovereignty, attitudes towards the use of force, the degree of dependence on the US, and different vulnerabilities to external crises.

The most significant obstacles to building an integrated EU foreign policy can be summarized in four groups: first, the different foreign policy priorities of the Member States; second, the sovereign nature of foreign policy and defense; third, the inability of the EU to independently guarantee its defense security; and fourth, the different degrees of energy dependence and energy vulnerability of individual Member States.

The five case studies examined confirm that European unity after 24 February 2022 is most activated under pressure and weakens when this pressure decreases or when the crisis affects the Member States in different ways. None of them shows a proactive and institutionally sustainable consolidation. Each reveal at least one of the old structural limitations of the CFSP – disagreements between states, fears of loss of sovereignty, dependence on the US, military inadequacy or energy vulnerability. This means that European unity, when it appears, often represents a temporary mobilization, not a completed strategic capability.

After February 24, 2022, the initial shock produced a strong consolidation around Ukraine and against Russia. Over time, however, this unity began to turn into a more difficult process of coordination between countries with different strategic cultures, different energy dependencies, different degrees of trust in the US, and different understandings of the EU's place in the security system.

The war in Ukraine, on the one hand, has established the CFSP as a forum and catalyst for a common response, but on the other hand, it has shown the limits of European unity. The main task facing European countries is no longer just to formulate common positions, but to find an institutional model that allows for timely common action, without erasing the differences between them and without turning the disagreement of one country into a veto on the actions of the others.

This future structure can hardly be built entirely within the framework of the CFSP, since it is based on the logic of the mandatory participation of all Member States and on the principle of unanimity. To a

large extent, Ralf Dahrendorf's definition that the European Union has been a «remarkable political success, but an equally remarkable institutional failure» can be applied to the institutional structure of the CFSP (Dahrendorf, 1979, p. 8).

Therefore, the understanding of the future European foreign policy must move beyond the two-dimensional opposition "integration – intergovernmentalism". Differentiation is not a deviation from the European project, but its inherent characteristic and it can be traced in the most diverse manifestations of exclusive, shared, coordinating, supporting and reserved for the Member States – both in individual integration regimes such as the euro area and Schengen, in the mechanisms of enhanced cooperation and in the Permanent Structured Cooperation in the field of defense. The question is therefore how to institutionalize foreign policy in such a way as to preserve the unity of the European project without paralyzing the capacity to act.

The main conclusion of the study is that Europe's future foreign policy should be built as an institutionalized variable geometry of strategic action: a common European strategic framework, voluntary participation of willing and able states, limited opt-out in case of essential national interests and the possibility of decision-making without the paralyzing effect of unanimity. Such a model would allow the EU to preserve the inclusive nature of the European project and at the same time - to restore its ability to act in a timely manner.

## REFERENCES

Andersson, J. (2023, April 3). Buying weapons together (or not): Joint defense acquisition and parallel arms procurement (Brief No. 7). European Union Institute for Security Studies. https://www.iss.europa.eu/content/buying-weapons-together-or-not

Chihaia, M. S. (2024, November 13). Military mobility 2.0 revisited: Lessons learned. European Policy Centre. https://www.epc.eu/publication/Military-mobility-20-revisited-Lessons-learnt-5f5640/

Council of the European Union. (2026). EU response to Russia's invasion of Ukraine. https://www.consilium.europa.eu/en/policies/eu-response-ukraine-invasion/timeline-eu-response-ukraine-invasion/

Dahrendorf, R. (1979). A third Europe? Third Jean Monnet Lecture, European University Institute, Florence, 26 November 1979. European University Institute

Duff, A. (2022). *Constitutional change in the European Union: Towards a federal Europe* . Palgrave Macmillan. https://doi.org/10.1007/978-3-031-10665-1

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2024). A new European defense industrial strategy: Achieving EU readiness through a responsive and resilient European defense industry (JOIN(2024) 10 final).

European Commission. (2026). European Defense Industry Program . https://defence-industry-space.ec.europa.eu/document/download/3864237c-ff5b-4f50-80e8-dd41a5b19426_en?filename=EDIP%20WP%20factsheet%20v4.pdf

European Council. (2026). EU solidarity with Ukraine. https://www.consilium.europa.eu

European Parliament and Council of the European Union. (2023). Regulation (EU) 2023/1525 of 20 July 2023 on supporting ammunition production (ASAP). Official Journal of the European Union, L 185, 1–12.

European Parliament and Council of the European Union. (2023). Regulation (EU) 2023/2418 of 18 October 2023 on establishing an instrument for the reinforcement of the European defense industry through common procurement. Official Journal of the European Union.

Howorth, J. (2007). Security and defense policy in the European Union. Palgrave Macmillan.

Joint Declaration on European Defense. (1998, December 3–4). Joint declaration issued at the British-French Summit, Saint-Malo.

Kissinger, H. (2002). Politikata: Kam diplomatsiyata na XXI vek [Politics: Towards the diplomacy of the 21st century]. Trud & Prozorets.

Kissinger, H. (2014). Diplomatsiyata [Diplomacy]. Trud.

Leuffen, D., Rittberger, B., & Schimmelfennig, F. (2013). Differentiated integration: Explaining variation in the European Union. Palgrave Macmillan.

Lonardo, L. (2023a). EU common foreign and security policy after Lisbon: Between law and geopolitics. Springer. https://doi.org/10.1007/978-3-031-19131-2

Lonardo, L. (2023b). Russia's 2022 war against Ukraine and the foreign policy reaction of the EU: Context, diplomacy, and law. Palgrave Macmillan.

Milward, A. S. (2009). The European rescue of the nation-state (2nd ed.). Routledge.

Scazzieri, L. (2020, October/November). Can the EU's Strategic Compass steer European defense? Center for European Reform Bulletin, 134.

Schmitter, P. C. (1996). Examining the present Euro-polity with the help of past theories. In G. Marks, F. W. Scharpf, P. C. Schmitter, & W. Streeck (Eds.), Governance in the European Union. SAGE Publications.

Sloan, S. (2016). Defense of the West: NATO, the European Union and the transatlantic bargain. Manchester University Press.

Stubb, A. C.-G. (1996). A categorization of differentiated integration. Journal of Common Market Studies, 34 (2), 283–295.

Thaler, P. (2020). Shaping EU foreign policy towards Russia: Improving coherence in external relations. Edward Elgar Publishing.

Varga, T. (2024). Reinforcing European defense industry for times of great power conflicts. In Shielding Europe with the Common Security and Defense Policy: The EU legal framework for the development of an innovative European defense industry in times of a changing global security environment (pp. 73–108). https://doi.org/10.54237/profnet.2024.zkjeszcodef_2

Jakimiec, D. (2026). Contemporary challenges for Japan's international policy in the context of security and defense. Politics & Security, 16(2), 76–81. https://doi.org/10.54658/ps.28153324.2026.16.2.pp.76-81

# CONTEMPORARY CHALLENGES FOR JAPAN'S INTERNATIONAL POLICY IN THE CONTEXT OF SECURITY AND DEFENSE

Dawid Jakimiec
Lublin Academy of Political Science and Engineering
Lublin, Poland
https://orcid.org/0000-0002-1310-3944

***Abstract.*** *This article examines the evolution and contemporary challenges of Japan's external security and defence policy. Setting the discussion in its historical context – from the more than two centuries of isolation under the Tokugawa shogunate, through the modernisation of the Meiji Restoration and the militarism that ended in defeat in the Second World War – the study traces how Japan's post-war security posture was shaped by the 1946 Constitution, the pacifist commitment of its Article 9, and the establishment of the Self-Defense Forces. It analyses the central role of the alliance with the United States, Japan's growing engagement in East and Southeast Asia, and the ongoing debate over constitutional revision in response to a changing regional environment. Particular attention is devoted to the contemporary threats confronting Japan – the rise of China, a nuclear-armed North Korea, and unresolved territorial disputes with Russia, China, and South Korea – and to Japan's efforts to strengthen its defence capabilities while balancing dependence on the United States against aspirations to regional leadership.*

**Keywords:** Japan; security policy; Self-Defense Forces; Article 9 of the Constitution; Japan–United States alliance; Indo-Pacific; territorial disputes.

## 1. INTRODUCTION

The subject of this article is the issue of security conditions in the face of a dynamically evolving list of threats and the many serious challenges facing contemporary Japan. Of particular importance in ensuring the level of security expected by Japanese society is the manner and direction of the Japanese government's external security policy and the building of international relations. The author also outlines and illuminates the historical context of the discussed issues, highlighting the most significant events in the history of the Land of the Rising Sun. The chronology of events spans from Japan's isolationist period, which lasted over two hundred years, through the colonial policy of the Meiji Restoration, armed conflicts, including the war with Russia and China, to the events of World War II. The article also provides an in-depth analysis of the fundamental directions of Japan's defense policy in the Land of the Rising Sun after the end of World War II. It also highlights the changes and ongoing evolution in the external security policy pursued by Japanese decision-makers. Considerable attention is paid to Japan's increased involvement in East and Southeast Asia, and existing disagreements and conflicts over disputed territories are outlined. These significantly impact Japan's relations with countries with which it has unresolved disputes. Furthermore, the article also presents the key elements of the Japan Self-Defense Forces' defense capabilities.

## 2. DIRECTIONS, GOALS, AND ASSUMPTIONS OF JAPAN'S SECURITY POLICY

Analyzing the long and rich history of the Land of the Rising Sun, we encounter a period of isolationism that lasted over 200 years and protected the country not only from the influence of other cultures but also served as a barrier ensuring the external security of the Empire of Japan (Meyer, 2009, pp. 127–129). In 1635, the shogun Tokugawa Iemitsu issued an edict that closed the country's borders to foreigners and

ISSN 2815-3324 Online, ISSN 2535-0358 Print

prohibited maritime trade with most countries. Only small trade was possible in the ports of Nagasaki and Kagoshima with a few countries, including China, Korea, the Netherlands, and the Ryukyu Kingdom (Henshall, 2012, pp. 75–107; Tashiro, 1982).

In 1854, the United States forced the opening and modernization of the country after Japan's isolation, which had lasted over 200 years. It must be admitted that the Japanese Empire was not only the first Asian industrial society but also soon began expanding its sphere of influence, primarily in the Pacific region. This expansion, as we know, ended with Japan's defeat in World War II and the American occupation. The creation of legal acts and political documents, ideologies, and doctrines of all kinds almost always contains references to more or less ancient history and the culture shaped by it. One of the researchers in the field of cultural sociology and political science is Ewa Skrabacz, who writes: "the nature of political actions is fundamentally future-oriented, but the construction of programs and the presentation of proposals naturally refers to the past: a summary, a prediction of continuation, a critique, a correction (Skrabacz, 2011, p. 24). It is important to consider the modifications and transformations taking place in the security environment, which result from changing geopolitical conditions. In this sense, taking into account immediate political needs, a sensibly crafted policy in international relations constitutes the binding agent and, at the same time, the material that can be used to justify specific actions expressed in dominance and defense potential, as well as subordination, as well as the legitimization of a specific system of building security and exercising power (Giddens, 2007, p. 49). As a supplement to the issue of Japan's isolation, it is worth emphasizing that it ended with the signing of the Treaty of Kanagawa, in which the Americans forced Japan to open up to trade with the United States and had to open two ports in Shimoda and Hakodate (Ladouce, 2010, pp. 157–184).

Following the overthrow of the last shogun, Tokugawa Yoshinobu, in 1868, a new era began in the Empire of Japan. Emperor Mutsuhito ascended the throne in 1867, and his reign is known as the Meiji Era, which lasted from 1868 to 1912. Japan's imperialist and militaristic ambitions intensified and were evident in its wars not only with China but also with Russia. The policies pursued by the Land of the Rising Sun briefly gave the Empire dominance in Asia. Only defeat in World War II halted the Japanese drive and efforts to subjugate other countries.

Due to Japan's geographical location, in order to prevent the islands from being occupied by a potential enemy attack, it is forced to defend the state in the surrounding waters. Therefore, the foreign policy pursued by the Land of the Rising Sun is largely determined by the desire to expand its geographical reach into deeper territories (Haliżak, 1999, pp. 150–166). For decades, Japanese decision-makers have been considering largely geopolitical conditions. The Japanese government remains undecided as to whether the foundation for Japan's development and power should be the resources, conditions, and socioeconomic characteristics of Asian countries, or whether, conversely, the importance and greatness of the Land of the Rising Sun should be built on the paradigms and patterns characteristic of Western civilization (Tow, 1983, pp. 51–83). It is worth noting the views of Fukuzawa Yukichi, who opposed the feudal system and promoted Western concepts of the state. He also opposed Japan's isolationism and criticized its lack of willingness to imitate more developed societies (being stuck in a state of stagnation). He believed that Western civilization was characterized by the intermingling of various social groups, which led to the development of democracy and their rapid economic and technological growth. Fukuzawa also touched on the topic of kokutai. He believed that national character was not solely a feature of Japanese society. According to this theory, each nation possesses a unique character, which is not immutable (unrelated to religion and language). It is subject to transformations that adapt to current social conditions. Fukuzawa also adapted the kokutai theory to his concept of national development and independence, identifying progress and independence with national character.

The strategic alliance with the United States is crucial for Japan in maintaining an appropriate level of external security. Other countries in the region are not interested in strengthening Japan's international position and would gladly form a bloc and form an alliance to block Japan's aspirations to become a regional hegemon (Bedeski, 1984, pp. 277–290).

Japan's devastating losses and defeat in World War II had a significant impact on the values and directions of the Japanese government's policies and international relations. Both the Japanese people and the ruling party advocated for the peaceful coexistence of states and nations and condemned militarism and expansionism (Niedziela, 2005). It is worth recalling the achievements and efforts of Shigeru Yoshida to establish new democratic principles and assumptions. His vision was based on, among other things:

− strategic cooperation with the United States, which was to be the primary guarantor of Japan's external security. Japan concluded a peace treaty with the United States in 1951, and a treaty of mutual cooperation and security was signed in 1960;

− abandoning the development of a military capability in the form of its own army. In return, the Japan Self-Defense Forces were established in 1954. These forces were to consist of naval, land, and air components. Article 9 of the 1947 Constitution imposed by the US stipulated that Japan renounce the use of war and embraced the principle of pacifism. Since the 1970s, Japan has been making efforts to strengthen political and economic cooperation with the countries of the Pacific region. In the history of relations between Japan and China, we can note a situation in which the Chinese government proposed to the Land of the Rising Sun a joint alliance against a possible military aggression by the Soviet Union.

In the area of security and defense, the Japanese government is revising its views, expressing the belief that Japan's external security should not be based solely on the alliance with the US and that it is necessary to expand and strengthen its own defense capabilities. The Japanese are considering the reliability of American allies in the event of a real threat (Yamada, 2010, pp. 137–155). In 1991, the Japanese government developed a concept for expanding Japan's international policy to include security issues in the Southeast Asian region (Haruki, 1999, pp. 222–223). Amendments to the Japanese constitution made in 1992 gave the Japan Self-Defense Forces the right to participate in international peacekeeping missions as part of the UN's statutory tasks. Japanese soldiers participated, among others, in participation in international peacekeeping operations in Mozambique, Cambodia and the Golan Heights.

The end of the Cold War and the collapse of the polarized world have redefined Japan's security policy. The Land of the Rising Sun is making diplomatic efforts aimed at building a system encompassing all countries in the Southeast Asian region. This arrangement would serve as a counterweight to the existing alliance and agreements with the United States. Recently, Japan has been significantly more active in building positive relations to strengthen and maintain an acceptable level of security both in the Indo-Pacific region and globally. The Japanese parliament passed a special law sanctioning the fight against terrorism, following the September 11, 2001, terrorist attacks in the United States. The Japan Self-Defense Forces have participated in missions in Turkey, Rwanda, Iran, India, Russia, and Indonesia.

It is worth noting that the regulations adopted in the Japanese Constitution of 1946 are not only principles for building a democratic state ruled by law, but also distinguish this supreme legal act from all the constitutions of democratic states. This includes the provision regarding pacifism and the renunciation of war as a means of resolving disputes. Furthermore, it includes a previously unknown concept of national sovereignty and a recognition of human rights. By adopting the Constitution, the Japanese nation not only adopted a democratic direction for its development but also completely renounced war. This resulted in the Land of the Rising Sun losing the right to build its own military force in the form of a classic army, which would safeguard state security and defend its independence and sovereignty. Article 9 of the Japanese Constitution contains a provision stating that the goal of the Japanese nation is to sincerely strive for world peace based on order and justice. The aforementioned text further states: The article contains a provision stating that the country must forever renounce war and the use or threat of war, and that this is the sovereign right of the nation (Suzuki & Winczorek, 1990, p. 35).

The constitutional regulations of 1946, imposed by the US, are incompatible with the current, changing international security conditions and the geopolitical and regional situation in the Indo-Pacific region. Shortly after the constitution was adopted, the United States needed Japan as an ally in the armed conflict with Korea, as well as to reinforce the threat posed by the USSR and China. The Japan Self-Defense

ISSN 2815-3324 Online, ISSN 2535-0358 Print
Forces, while not very numerous, are equipped with state-of-the-art weaponry. The lack of definition and precise definition of defense leads to endless debates regarding the validity of Article 9 regulations. Following the escalation of terrorist attacks, Japanese politicians are calling for a radicalization of defense regulations and are demanding a constitutional revision. The shifting priorities of the Japanese government in security and defense policy have led the Japan Self-Defense Forces to engage not only in peacekeeping missions conducted under the aegis of the UN but also in military operations conducted by NATO. By imposing Article 9 of the Japanese Constitution in 1946, the Americans sought to prevent the Japanese from pursuing any imperialist ideas or ambitions. However, in the current situation of growing threats and tensions in the Pacific region, the lack of an army is increasingly being questioned, not only by the Japanese people, politicians, and government elites, but also by international opinion. Independent military experts and observers believe that, given the current geopolitical security situation, a revision of the Japanese constitution is necessary, including amending Article 9. They believe these proposed changes will contribute to Japan's greater involvement in building stability in the Southeast Asian region and more effectively combating terrorism.

Currently, Japan's self-defense forces constitute the only support and potential adapted and equipped to conduct offensive operations, which is contrary to the current regulations contained in Article 9 of the Japanese Constitution. Japan compensates for the lack of a traditional army with self-defense forces that participate in international operations. The name of these forces in Japanese means "self," "defense," and "regiment." The origins of the Self-Defense Forces date back to World War II. As history records, the United States dropped atomic bombs on Hiroshima and Nagasaki on 6 and 9 August 1945, and in the post-war period sought to hold Japan accountable for war crimes. Japan is a technologically and economically well-developed country with a strong international position. However, the strengthening competitiveness, not only of China, forces it to constantly seek new markets for its goods. In choosing the direction of contemporary international and security policy, the Land of the Rising Sun faces a choice between two concepts: the first is based on continuing to maintain and celebrate its alliances with the United States, while the second path involves building regional economic power and a leading position in Southeast Asia within ASEAN. Furthermore, Japan is also considering establishing an enclave within the Sea of Japan and the Yellow Sea, whose primary goal would be to strengthen security, expand the sphere of prosperity, and enhance the development potential of the Land of the Rising Sun, where the country would play a key role in this region. The Japanese government is making visible efforts to lessen its external security umbrella's dependence on the United States. The Japanese are increasing their military spending, as such proximity justifies strengthening their military potential (Lorat, 2010). The Japanese security strategy establishes priorities and directions for security policy, with ensuring Japan's own security as its primary goal. However, Japan's ambitions are steadily growing toward building a strong economic, financial, and financial zone, of which it will be the leader and administrator (Niedziela, 2009).

Japan has unresolved territorial disputes with Korea, China, and the Russian Federation, which are a source of ongoing unrest and tension between these countries.

## 3. CONCLUSION

Japan, defeated in World War II, was forced by the United States to adopt a constitution in 1946 and build a new political system – democracy. We may wonder whether, after the horrors of war, the suffering it endured, and the murders perpetrated by the Japanese on the populations of conquered countries, it would have been able to voluntarily abandon its imperialist ambitions, aspirations, and ambitions without any pressure. It was under pressure from the United States that the process of building a different social and political order began in the Land of the Rising Sun. A new democratic system and security could be built primarily on the basis of agreements, alliances, and understandings with the United States.

Japan currently faces new difficulties and challenges in the context of China's strengthening hegemony, the security threat posed by nuclear-armed North Korea, the unresolved territorial dispute with the Russian Federation over the Kurils and Sakhalin Islands, and the revision of its alliance with the

United States. Japan strives to play an increasingly important role in building and strengthening security in the Asia-Pacific region.

The Japanese government believes that its importance in the region and internationally must be commensurate with its level of economic and technological development and proportionate to its economic potential. The dynamically evolving catalog of contemporary threats to the Land of the Rising Sun's security poses new requirements and goals for ensuring the country's security, which is a prerequisite for its existence and development.

Serious unrest and tensions in the region, which are the source of many significant threats to Japan's external security, have prompted ongoing internal transformations in the context of its international and security policy. Japan is strengthening, modernizing, and expanding its military capabilities. It is aggressively strengthening and modernizing its naval equipment and resources. It is building modern ships and helicopter destroyers designed to counter ballistic missiles. The alliances and agreements with the United States, in place since the end of World War II, continue to play a fundamental role in ensuring Japan's adequate security, simultaneously serving as an effective deterrent to potential aggressors and adventurous states in the region. Furthermore, existing mutual support and cooperation contribute to regional and supra-regional stability and significantly increase its active role in shaping Japan's foreign policy and international relations.

## REFERENCES

Bedeski, R. E. (1984). La politique étrangère japonaise sous Nakasone: Le dilemme d'une superpuissance économique [Japanese foreign policy under Nakasone: The dilemma of an economic superpower]. Études Internationales, 15(2).

Giddens, A. (2007). Socjologia [Sociology]. Wydawnictwo Naukowe PWN.

Haliżak, E. (1999). Stosunki międzynarodowe w regionie Azji i Pacyfiku [International relations in the Asia-Pacific region].

Haruki, W. (1999). Problèmes des Territoires du Nord: Histoire et avenir [Problems of the Northern Territories: History and future]. Asahi Shinbun.

Henshall, K. (2012). A history of Japan: From Stone Age to superpower. [Publisher].

Konstytucja Japonii [The Constitution of Japan] (T. Suzuki & P. Winczorek, Trans.). (1990). Zakład Narodowy im. Ossolińskich.

Ladouce, L. (2010). Le Japon et les travaux d'Hercule en Méditerranée d'Asie [Japan and the labours of Hercules in the Mediterranean of Asia]. Géostratégiques, (26).

Lorat, P. (2010, November 9). Géopolitique – un accord stratégique Inde-Japon pour contrer les ambitions chinoises [Geopolitics – A strategic India-Japan agreement to counter Chinese ambitions]. Le Nouvel Économiste.

Meyer, M. W. (2009). Japan: A concise history. [Publisher].

Niedziela, S. (2005). Dokąd zmierza Japonia? [Where is Japan going?]. Dziś. Przegląd Społeczny, (1).

Niedziela, S. (2009, June). Indie – nowe mocarstwo światowe [India – A new world power]. Przegląd Morski.

Skrabacz, E. (2011). Ogarnąć przeszłość – polityczność historii i pamięci w III RP [Grasping the past – The political dimension of history and memory in the Third Polish Republic]. In E. Nieroba (Ed.), Targowisko przeszłości: Społeczne konsekwencje popkulturowych sposobów opowiadania o świecie minionym [The marketplace of the past: Social consequences of pop-cultural ways of narrating the bygone world]. Internetowa Księgarnia Naukowa i Techniczna.

ISSN 2815-3324 Online, ISSN 2535-0358 Print

Tashiro, K. (1982). Foreign relations during the Edo period: Sakoku reexamined. Journal of Japanese Studies, 8(2).

Tow, W. T. (1983). Sino-Japanese security cooperation: Evolution and prospects. Pacific Affairs, 56(1).

Yamada, Y. (2010). Un conflit géopolitique persistant entre le Japon et la Russie: La question des Territoires du Nord [A persistent geopolitical conflict between Japan and Russia: The question of the Northern Territories]. Géostratégiques, (26).

Mihaylov, M., & Nikolova-Alexieva, V. (2026). Aspects of food security. Politics & Security, 16(2), 82–88.
https://doi.org/10.54658/ps.28153324.2026.16.2.pp.82-88

# ASPECTS OF FOOD SECURITY

Mihail Mihaylov
Academy of National and Information Security
Plovdiv, Bulgaria
https://orcid.org/0000-0003-2482-228X
m.mihaylov@anis.bg

Valentina Nikolova-Alexieva
Academy of National and Information Security
Plovdiv, Bulgaria
https://orcid.org/0000-0001-5384-1485
valentina_nikolova@abv.bg

**Abstract.** *The quest for security has accompanied humanity throughout its evolutionary development, from the Stone Age to the present day. Security is identified with a state of protection, with the physical and moral survival of the individual, with their freedom and rights, and with their spiritual and social development. This defines the multifaceted nature of the concept of "security," which centers on the individual and society. Human security has many dimensions, of which food security is vital. Given its significance, the management of food security is a matter of state policy and national security. This article traces the origins, evolution, and current state of food security on a global, European, and national scale.*

**Keywords:** Food security; FAO; IPC

## 1. INTRODUCTION

The pursuit of security has become a primary concern and goal. It has accompanied humanity throughout its evolutionary development, from the Stone Age to the present day. Security is identified with a state of protection, the physical and moral survival of the individual, their freedom and rights, and their spiritual and social development. This defines the complex nature of the category of "security," whose subjects are the individual and society. Human security has many dimensions, of which food security is vital, because without constant access to safe food and drinking water, human existence is unthinkable.

The diversity of human needs and their hierarchical arrangement are the subject of the scientific interests of the American psychologist Abraham Maslow (1908–1970). According to him, the needs at the lowest level (physiological needs—water, food, shelter) must be fully satisfied before moving on to the next levels. Food security ensures that the population has access to sufficient safe food and drinking water.

U.S. President Franklin Roosevelt played a significant role in food policy and security in the aftermath of the Great Depression. In his speech to Congress (1941), he articulated the principles of the Four Freedoms, which were subsequently adopted by the UN General Assembly (1948) in the Universal Declaration of Human Rights:

- freedom of speech;
- freedom of religion;
- freedom from want;
- freedom from fear. (Roosevelt, 1941)

## 2. THE EVOLUTION OF FOOD POLICY AND THE ROLE OF THE FAO

Following the Great Depression, Franklin Roosevelt launched the New Deal program, which included reforms related to food security and the country's economic development. The main priorities of this program were: support for the agricultural sector, agricultural subsidies, reducing unemployment, and social security. For President Roosevelt, food and economic security were the foundation of national security, without downplaying the role of military security.

ISSN 2815-3324 Online, ISSN 2535-0358 Print

In 1945, in Quebec City, Canada, a specialized agency for food and agriculture (FAO) was established under the United Nations, which launched a global campaign against hunger. Currently, the organization is headquartered in Rome and has 195 member states.

The main tasks of the FAO are as follows:

- leading the international fight against hunger;
- monitoring and improving international food security;
- analyzing, improving, and coordinating the development of sectors—land and water resources, agriculture, forestry, and fisheries.

The activities of the Food and Agriculture Organization are carried out through its departments (Table 1).

Table 1: FAO Divisions

| № | Department |
|---|---|
| 1. | Agriculture and Consumer Protection |
| 2. | Biodiversity |
| 3. | Land and Water |
| 4. | Climate |
| 5. | Fisheries and Aquaculture |
| 6. | Forestry |
| 7. | Economic and Social Development |
| 8. | Cooperation and Management of Programs for Sustainable Agricultural Development and Food Security |

*Compiled by: the authors*

## 3. MEASURING FOOD SECURITY: INDICATORS AND THE IPC CLASSIFICATION

The analysis of the state of the food crisis in a given region (country) uses the following indicators:

- Food Security Phase Classification (IPC);
- analysis of extreme food and water needs;
- capacity and response for humanitarian aid.

The UN's Integrated Food Security Phase Classification (IPC) includes five phases of food security (IPC Global Partnership, 2021) (Table 2)

Table 2: UN Classification of Food Security

| # | Phases | Description |
|---|---|---|
| 1. | Minimal | Households meet their basic food and non-food needs |
| 2. | "Stress" | Households have reduced food consumption but can still afford food |
| 3. | "Crisis" | Food shortages, reduced availability, and malnutrition |
| 4. | "Emergency" | Severe food and drinking water shortages, malnutrition, and disease |
| 5. | "Disaster" | Extreme lack of food, water, and social assistance. Death |

Adapted from IPC Global Partnership (2021) by the authors

## 4. FOOD SECURITY AS A HUMAN RIGHT AND INTERNATIONAL COMMITMENTS

Article 25 of the Universal Declaration of Human Rights, adopted by the United Nations General Assembly (1948), states:

"Article 25: Everyone has the right to a standard of living, including food, clothing, housing, medical care, and necessary social services, that is necessary to maintain his or her health and well-being and those of his or her family." (United Nations General Assembly, 1948, Art. 25)

To combat acute food crises, the Global Network Against Food Crises (GNAFC) was established to coordinate efforts to prevent and address them. It is an international organization whose members include the United Nations, the World Bank, governments, the European Union, and non-governmental organizations. Each year, the organization prepares reports on acute food crises caused by military conflicts, climate-related disasters, and economic crises. These reports serve as the basis for making urgent decisions and taking action in regions affected by food crises.

The international community has committed to ensuring an adequate standard of living for every citizen of the planet through the International Covenant on Economic, Social and Cultural Rights, adopted in 1966 by the UN General Assembly and entered into force in 1976. To date, this covenant has been ratified by 171 countries. Article 11, paragraph 1 of this covenant states: "the right to an adequate standard of living, including adequate food, clothing…, as well as the continuous improvement of living conditions." (United Nations General Assembly, 1966, Art. 11)

At the FAO World Food Summit (1996), food security was defined as "a state in which all people, at all times, have physical, economic, and social access to sufficient, safe, and nutritious food to meet their dietary needs and food preferences for an active and healthy life." This forum also established World Food Day, which is observed annually on October 16 and is dedicated to the fight against hunger worldwide. The United Nations World Food Programme (WFP) plays an active role in combating food crises in various regions and has therefore been awarded the Nobel Peace Prize.

In 2000, the United Nations, with the participation of 191 member states, adopted eight Millennium Development Goals. The main ones were to combat hunger, poverty, inequality, and disease by 2015. These goals became the basis for establishing 17 Sustainable Development Goals (SDGs) with a target date of 2030. The elimination of extreme poverty and hunger stand out as the leading sustainable development goals.

Food security is linked to access to sufficient safe food and drinking water, which are essential for human health. Access to water and nutritious food is a fundamental human right.

Food security has four main pillars:

- Physical availability.
- Economic accessibility.
- Biological accessibility.
- Stability and consistency in availability.

## 5. THE FOUR PILLARS OF FOOD SECURITY

Physical accessibility means access to sufficient quantities of food. The sufficiency and availability of a diverse food supply are linked to global climate change. Food must be accessible to everyone, regardless of whether it is sourced from the domestic market and/or imported.

Economic accessibility means that people must have the financial means to secure the necessary amount of nutritious food. Price fluctuations in global markets can threaten food security. A surge in food prices could push more than 1 billion people into malnutrition and extreme poverty.

Biological sufficiency refers to each person's need for an optimal amount of nutrients to sustain life, which includes an energy intake appropriate to their physiology and age. Biological access to food is also linked to food and water safety and all of the requirements listed above. Climate change increases the risk of gastrointestinal diseases, zoonoses, and food poisoning.

The fourth pillar of food security is the stability, consistency, and availability of food at all times, without the risk of shortages due to financial or political reasons. The stability of food supplies is influenced

ISSN 2815-3324 Online, ISSN 2535-0358 Print

by climate change and the seasonality of agricultural production. Threats to the stability and consistency of food availability will increase with population growth, and this could destabilize global food security. The struggle for drinking water and food, driven by climate change, has the potential to cause a serious collapse of the food system and to intensify the trend of migration of hungry and thirsty people from the impoverished South to the wealthier North.

The four pillars are interconnected, and their goal is to ensure that everyone on the planet has access to sufficient quantities of high-quality food.

According to the FAO, 60% of the population faces food insecurity for the following reasons:

- a mismatch between the increased natural population growth and the limited food resources;
- 3 billion people do not have access to a healthy diet;
- 40% of the population suffers from water scarcity;
- climate change;
- soil erosion.

Even Europe is threatened by a food crisis due to climate change, natural disasters, and strained relations between some countries. The Scandinavian countries rank among the world's leaders in food security. In these countries, only 15% of household income is spent on food, while at the other end of the spectrum are countries like Nigeria, where about 60% of family income goes toward food.

According to the FAO (2024), in 2024, approximately 1.7 billion people were affected by low crop yields due to soil degradation and ecosystem threats. Global food prices rose by an average of 4.3% in 2025 compared to 2024. Global prices for vegetable oils and dairy products have risen. The crisis in the dairy sector is caused by a 25% drop in production, while high energy costs are driving up vegetable prices.

The Food and Agriculture Organization (FAO), with its mission to ensure the sustainability of food and agricultural systems, has defined 10 elements of agroecology.

The first group consists of environmental measures and includes:

- diversification and variety of crops and livestock;
- knowledge creation, sharing, and innovation in agriculture;
- positive interactions (in crop and livestock farming);
- reducing dependence on external resources;
- circular economy (closing the cycle of food, materials, biomass, and water);
- resilience to pests and climate change.

The second group consists of socio-economic issues:

- a focus on the health and working conditions of farmers and rural communities;
- support for healthy eating, local foods, and traditions;
- the establishment of transparent policies regarding access to land, water, and markets;
- the circular economy (connecting producers and consumers).

There is a correlation between food insecurity and poverty (Table 3)

Table 3: The world's poorest countries facing food crises

| # | Country | The cause of the food crisis | GDP (in bill. $) | Population (in mill. people) |
|---|---|---|---|---|
| 1. | South Soudan | Political instability | 29,9 | 11,1 |
| 2. | Burundi | Underdeveloped agriculture | 2,15 | 13,4 |
| 3. | Central African Republic | Abundant natural resources, political instability | 3,03 | 6,0 (80% starving) |
| 4. | Malawi | Weak agriculture, drought | 10,78 | 21,5 |
| 5. | Mozambique | Terrorism, | 24,55 | 34,5 |

| | | | | |
|---|---|---|---|---|
| | | natural disasters | | |
| 6. | Somalia | Civil War, Piracy | 13,89 | 19,0 |
| 7. | DR Congo | Economic crisis | 79,24 | 104,0 (60% of the population is under 1,5$ per day) |
| 8. | Liberia | Civil war, epidemics | 5,05 | 5,4 |
| 9. | Yemen | Civil war, a devastated economy | 16,22 | 34,4 |
| 10. | Madagascar | Natural disasters, underdeveloped agriculture | 18,1 | 30,3 |

Compiled by: the authors, based on World Bank (2024) data.

The following conditions are observed in the countries listed:

- a population explosion (rapid population growth);
- underdeveloped agriculture, whose output is unable to meet basic food needs;
- water scarcity;
- political instability;
- natural disasters;
- economic crises.

Food security is becoming a critical global issue for the following reasons:

- more than 295 million people in 53 countries suffer from acute food insecurity due to a severe lack of food, drinking water, and social assistance;
- over 10% of the population is undernourished;
- 820 million people are victims of chronic food insecurity;
- over 1.9 million are on the brink of starvation. [Annual Report of the Global Network Against Food Crises, 2025]

In 2026, food insecurity is on the rise in Asia and Africa due to disrupted food supply chains; crises in the supply of raw materials for fertilizers; dependence on grain imports from Ukraine; military conflicts (Russia-Ukraine; the Middle East and Africa); and a slowdown in global economic growth.

According to the UN World Food Programme, over 45 million people are at risk of mass starvation. The risk of food crises has increased in Sudan, Yemen, Ethiopia, Nigeria, Haiti, and other countries. Sudan relies on imports for 80% of its grain supply.

Some of the world's poorest countries—Sri Lanka, Pakistan, Kenya, and others—are dependent on fertilizer supplies for food production. In these countries, food prices are rising to levels where 80% of the population is unable to secure sufficient food intake.

The war in the Middle East is having a cumulative effect, not only on energy prices but also on the global economy.

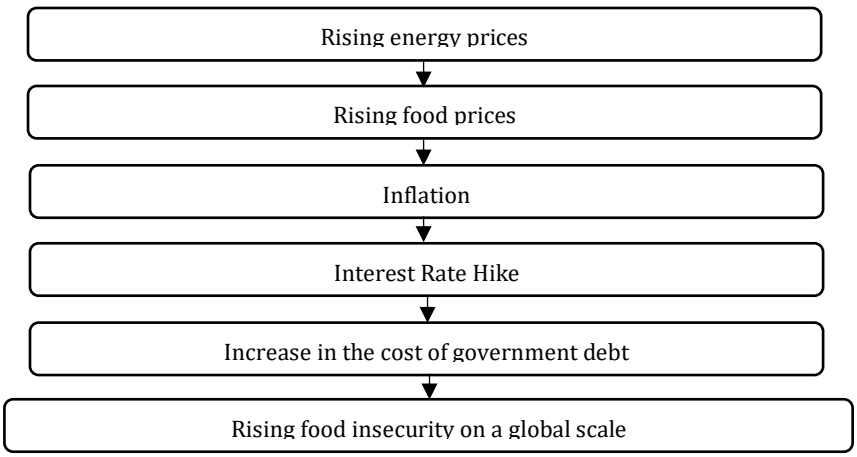



Figure 1: Economic Impact of the War in the Middle East on the Global Economy and Food Insecurity

ISSN 2815-3324 Online, ISSN 2535-0358 Print

## 7. FOOD SECURITY IN THE EUROPEAN UNION AND BULGARIA

Ensuring food security requires not only sufficient food supplies but also food safety, which involves strict controls over production, processing, and storage throughout the food chain, "from farm to table."

According to the European Union, the key factors for quality of life are:

- food security and sustainable agriculture, which ensure affordable, healthy, and safe food by promoting the production of high-quality agricultural products;
- nature conservation and the protection of water resources.

The measures listed above, which relate to food security, are set out in the European Union's Strategic Agenda for 2024–2029. (European Council, 2024)

There are over 9 million farms in the European Union, employing over 17 million agricultural workers. The food industry is the largest manufacturing sector in the EU. It provides employment for 4.6 million people. The sector is the world's largest exporter of agricultural and food products.

The European Union's priority areas related to food security are:

- building a sustainable food system;
- safeguarding the EU's food independence;
- ensuring food safety;
- supporting sustainability throughout the food chain;
- a civil protection plan for climate-related disasters.

Bulgaria's food security is linked to ensuring that food is physically and financially accessible to every Bulgarian citizen. The National Development Program 2030 (Ministry of Finance of the Republic of Bulgaria, 2020) emphasizes the sustainable development of agriculture, which will ensure that the population has access to affordable food.

The wars in the Middle East and Ukraine pose a serious threat to national food security. Rising prices for energy resources, agricultural fertilizers, and plant protection products inevitably drive up food prices, making food less affordable. Domestic food production is unable to meet food needs, necessitating imports. The Commission for Protection of Competition warns that the number of farms raising cows, sheep, and goats is drastically declining. (Mazganova, 2026) This threatens meat and milk production, causing prices for these food products to rise and their availability to decline. According to K. Vatev, our country's food security is at enormous risk for the following reasons:

- domestic production of agricultural seeds is less than 5%;
- Bulgaria is dependent on imports of fertilizers and plant protection products;
- vegetable production is declining in favor of industrial crops. (Vatev, 2024)

The main challenges to Bulgaria's food security are as follows:

- organizational and structural problems in the agriculture and food industry sectors;
- expensive energy sources, fertilizers, and plant protection products, resulting from military actions in the Middle East that threaten logistics;
- climate change;
- the inability of Bulgarian agricultural production to meet the food needs of the population;
- political instability and a lack of continuity in agricultural and food industry policy;
- the country lacks a long-term food security strategy to achieve self-sufficiency in staple foods for the Bulgarian population;
- the country needs to establish a system of continuity in the bioeconomy, particularly with regard to expanding the production of environmentally friendly agricultural and food products. (Nikolova-Alexieva & Valeva, 2019)

## 8. CONCLUSION

Global population growth, climate change, soil erosion, water scarcity, and military and civil conflicts pose enormous threats to food security. Given its significance, managing food security is a matter of public policy and national security. Finding optimal solutions to these problems has become a primary task for humanity.

## REFERENCES

European Council. (2024). Strategic agenda 2024–2029. Council of the European Union. https://www.consilium.europa.eu/en/european-council/strategic-agenda-2024-2029/

Food and Agriculture Organization of the United Nations. (2018). The 10 elements of agroecology: Guiding the transition to sustainable food and agricultural systems. FAO. https://www.fao.org/agroecology/knowledge/10-elements/en/

Food and Agriculture Organization of the United Nations. (n.d.). About FAO. FAO. https://www.fao.org/about/en/

Food Security Information Network, & Global Network Against Food Crises. (2025). Global report on food crises 2025. FSIN. https://www.fsinplatform.org/report/global-report-food-crises-2025/

Integrated Food Security Phase Classification Global Partnership. (2021). IPC technical manual version 3.1: Evidence and standards for better food security and nutrition decisions. IPC. https://www.ipcinfo.org/ipcinfo-website/ipc-overview-and-classification-system/ipc-acute-food-insecurity-classification/en/

Mazganova, I. (2026). The CPC warns: Bulgaria is losing its food security [The Commission for Protection of Competition warns]. Iskra. https://www.iskra.bg/kzk-alarmira-balgariya-gubi-prodovolstvenata-si-sigurnost/

Ministry of Finance of the Republic of Bulgaria. (2020). National development programme BULGARIA 2030 (adopted by Protocol No. 67 of the Council of Ministers, 2 December 2020). https://www.minfin.bg/en/1394

Nikolova-Alexieva, V., & Valeva, K. (2019). Enhancing the competitiveness of bio-sector enterprises for a stronger bio-economy. Scientific Papers, 35(1), 381.

United Nations General Assembly. (1948). Universal Declaration of Human Rights (Resolution 217 A). https://www.un.org/en/about-us/universal-declaration-of-human-rights

United Nations General Assembly. (1966). International Covenant on Economic, Social and Cultural Rights (Resolution 2200A (XXI)). https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights

United States, President (Roosevelt). (1941). Annual message to Congress on the state of the Union ("The Four Freedoms"), January 6, 1941. Franklin D. Roosevelt Presidential Library and Museum. https://www.fdrlibrary.org/four-freedoms

Vatev, K. (2024). Bulgaria's food security is at great risk [Interview]. Investor.bg. https://www.investor.bg/a/520-zemedelie/399145-kiril-vatev-prodovolstvenata-nezavisimost-na-balgariya-e-pod-ogromen-risk

World Bank. (2024). GDP (current US$) and population, total [Data set]. World Bank Open Data. https://data.worldbank.org/

World Food Programme. (2020). The Nobel Peace Prize 2020. WFP. https://www.wfp.org/nobel-peace-prize