Political Science and Security Studies Journal
Dziennik Nauk Politycznych i Studiów Bezpieczeństwa

ISSN 2719-6410 (Online)

POLITICAL SCIENCE AND SECURITY STUDIES JOURNAL

Volume 6, Issue 4, December 2025

Vol. 6, №4
December 2025
Founded in 2020 by High school of the social and economic in Przeworsk

The editorial board

Editor of the publication

BRITCHENKO Igor – Prof., Dr. of Sciences, Bulgaria;

Deputy Editor-in-Chief

TKACH Ivan – Prof, Dr of Sciences, Ukraine;

Members of the editorial board

CHERNIAVSKA Tetiana – Dr. Sc. (Economics), Poland;

CHUMAK Oleksandr – Ph.D, Assist. Prof., Ukraine;

DYULGEROVA Nina – Prof. Dr. hab., Bulgaria;

DIO CAISAR Darma – Ph.D, Assist. Prof., Indonesia;

GAWLICZEK Piotr – Ph.D, Assoc. Prof., Poland;

GUMENNYKOVA Tamara – Prof., Dr. of Sciences (Pedagogical), Ukraine;

KHARABARA Violetta – Assoc. Prof., PhD, Ukraine;

KRUPSKYI Oleksandr – Assoc. Prof., Candidate of Psychological Sciences, Ukraine;

LEWANDOWSKi Arkadiusz – Dr., Poland;

MELLER Arkadiusz – Dr, Poland;

MONOLATII Ivan – Dr. hab. Ukraine;

NIZIAIEVA Viktoriia – USA;

POLAKOWSKI Marcin – Dr., Poland;

RÓŻYCKI Bartłomiej – Dr., Poland;

SAMBERG Andre – Prof. of Practice, D.Sc., Ph.D., Belgium;

TOMASZEWSKI Patryk – Dr., Poland;

ZHELJAZKOVA Virginia – Prof. PhD, VUZF University, Bulgaria;

e-mail: tkachivan9@gmail.com
https://psssj.eu/index.php/ojsdata/index, тел. +38(093) 752-81-56

The authors of articles are responsible for the authenticity of facts, quotes, their own names, geographical names, names of enterprises, organizations, institutions and other information. Opinions expressed in these articles may not coincide with the point of view of the editorial board and do not impose any obligations on it.

CONTENT

1 **National Interests as a Mechanism for Formulating Intelligence Tasks**
Yurii Semeniuk 1

2 **An Investigative History of Russian Speech Manipulation Strategies in Republican Discourse**
Aaron Helmbrecht 8

3 **Analysis of Approaches and Technologies for Conducting Cognitive Warfare in Modern Conditions**
Oleksandr Kin 22

4 **The Role of Central Asia in Modern Geopolitics**
Serhii Strilchuk, Oleh Matsovityi, Volodymyr Taranov 30

5 **The Contemporary Security Provision Model in the Intelligence Practice of the Republic of Romania**
Andriy Stroev 44

6 **A Risk-Oriented Framework for Forming and Modelling Information Security Profiles in Modern Cyberspace**
Ruslan Netrebko 52

NATIONAL INTERESTS AS A MECHANISM FOR FORMULATING INTELLIGENCE TASKS

Yurii Semeniuk

Ph.D in Political Sciences, e-mail: snik71083@gmail.com, ORCID: https://orcid.org/0000-0002-9415-4427

National University of Defense of Ukraine, Kyiv, Ukraine

Received: November 24, 2025 | Revised: December 20, 2025 | Accepted: December 31, 2025

DOI: https://doi.org/10.33445/psssj.2025.6.4.1

Abstract

The article provides a comprehensive analysis of changes in the geopolitical and geo-economic environment resulting from the Russian Federation's full-scale invasion of Ukraine and their impact on the transformation of the international security landscape. The essence of national interests is examined as a multidimensional category shaped by historical, political, economic, and civilizational factors, and their role in the development of a geocivilizational strategy of the state is substantiated. Particular attention is paid to the evolution of approaches to the interpretation of national interests within realist and liberal-idealist paradigms of international relations. Key trends in the formation of a new security architecture are identified under conditions of intensified strategic competition among major global actors, the escalation of hybrid threats, and the acceleration of the technological revolution, particularly in the field of artificial intelligence. The study demonstrates that national interests function as a fundamental mechanism for shaping intelligence tasks, determining priorities, instruments, and directions of intelligence activities in contemporary conditions. The article concludes that the profound transformation of the global security environment necessitates a reassessment of the role of intelligence services in the emerging international order.

Key words: geopolitics, security, full-scale invasion, new security architecture, intelligence, artificial intelligence, intelligence activities.

Introduction

Herbert McMaster, former US National Security Advisor, has described the current situation in the world as follows: "Geopolitics is back, and it is back to exact revenge on us for our disregard of the lessons of history that we demonstrated in the post-Cold War period" (McMaster, H., 2023).

The Russian Federation's (RF) war against Ukraine has precipitated a paradigm shift on a global scale that has no precedent since the conclusion of the Cold War era. A misjudgment of the outcome of the Cold War and an inability to clearly explain the essence of the processes that took place in post-Soviet space in the early 1990s led to a series of wrong political decisions on the part of the West. In lieu of establishing a balanced security framework that would preclude the possibility of a new nuclear confrontation, a decision was taken to "reset" relations with Russia and to integrate it into international structures.

Thus, Russia's full-scale invasion of Ukraine radically changed the perception of the security situation in the world at the global, regional and sub-regional levels. This, in turn, led to fundamental changes in the policies of leading states, as well as the European Union and NATO, and stimulated the strengthening of transatlantic ties.

Under these circumstances, virtually all the special services of NATO member states consider Russia's intelligence and subversive activities to be the main threat to their national security.

Under such conditions, the process of developing reference points for the productive development of the state, which, as global experience shows, becomes national interests, becomes

particularly important.

Analysis of recent studies and publications. In global scientific thought and practice, the issue of realising national interests, defining their methodology and political and legal foundations is the subject of research by such scholars as R. Aron, W. Wilson, J. Kennan, H. Morgenthau, R. Niebuhr, J. Rosenau, N. Spykman, and others. At the same time, the influence of national interests on the activities of Intelligence remains understudied.

The aim of the study is to examine national interest as a mechanism for shaping intelligence tasks.

Results and Discussion

The concept of national interest, as influenced by the expectations of participants in international relations, is represented through various images and symbols. When interpreted through a system of symbols and images that construct a positive image, national interest emerges as a significant factor in the implementation of state policy. The disclosure of the issue of forming the geopolitical image of the state in its national interests requires clarification of the content of the concept of 'national interests' and detection of trends in its changes.

The concept of "national interest" has only recently entered the domain of scientific discourse; its first appearance in the Oxford Encyclopedia of Social Sciences was in 1935. Contemporary scientific thought has demonstrated a tendency to embrace multidirectional definitions of the category of "national interest", a phenomenon that has given rise to the emergence of diverse scientific schools of thought. In the early 1950s, two paradigms emerged in Western academic circles regarding the practice of using the concept of "national interest": political realism and liberal idealism. Extensive discussions took place between representatives of the 'realist' track-pin retaining cam, founded by H. Morgenthau, and representatives of the 'idealist' track-pin retaining cam, represented by W. Wilson, on the definition of the essence of national interest. According to the theory of the realistic paradigm, national interest is a product of complex interrelationships between actors in international relations. It is based on the concept of interest formulated in terms of power (Morgenthau Hans J., 1982., 306 p.; Wilson W., 1970, 402 p.).

In contrast to realists, proponents of the liberal-idealistic paradigm argue that national interests are based on moral norms and global issues of our time. H. Morgenthau strongly disagrees with this, noting that "foreign policy guided by universal moral principles and relegating national interests to the background is, in the context of modern politics and military affairs, a policy of national suicide — actual or potential" (Rosenau, J., 1968). Therefore, while liberals focus on the economic well-being of citizens, realists place geopolitical priorities at the forefront of their understanding of national interests.

The concept of national interests has evolved as a result of the historical development of the nation-state as a subject of international law. The concept of "national interest" traditionally comprised of three fundamental elements: military security, economic prosperity and development, and state sovereignty, defined as the exercise of control over a specific territory and population. Concurrently, the substance of these elements may be subject to transformation under the influence of historical, socio-political and economic-geographical factors of the state's functioning. Significant adjustments to the definition of national interest are made by the processes of globalisation. In this context, a globalist approach to the definition of the concept of "national interest" has emerged, thereby calling into question the legitimacy of using this category. Critics of this approach have highlighted the interdependence of states and the emergence of transnational and supranational actors in international relations, which they contend has resulted in a weakening of the role of the nation-state and the replacement of national interests with those of business

interests in the form of transnational corporations (TNCs) and the interests of the international community.

Contemporary global development is characterised by two opposing trends. The first of these trends is driven by the processes of globalisation previously mentioned. The second is driven by the formation of new nations on the ruins of former empires, or the legitimisation of new nations as a result of certain agreements, such as the independent states of the CIS, Kosovo, etc. The category of 'national interest' is fundamental in determining the main directions of their external and domestic policies, and provides contributory support to the definition of their national identity.

In the context of the present conditions of development, the interpretation of "national interest" is not so much ideological as pragmatic in nature and is oriented not so much towards certain national or universal values as towards the ability of the state (its state bodies) to set certain goals and achieve them. Notwithstanding the fact that the objectives of the state, as well as the specific strategies employed to achieve them, may be subject to alteration in the event of the influence of certain socio-political or economic factors, the state authorities responsible for the establishment of these objectives must possess the capacity to formulate and accomplish them. This process necessitates military strength, internal and external stability, economic competitiveness, and so forth. The possession of such capabilities by the state is the reference point for national interests, in its pragmatic interpretation, in determining state policy.

In July 2023, the Director of the CIA, V. Burns, delivered a lecture at the Dechley Foundation in the United Kingdom. Subsequently, in January 2024, he published an article in The Foreign Affairs, in which he expounded his strategic vision for the development of major trends in the modern world and in the field of intelligence [5; 6]. In the opinion of V. Burns, the period of unquestionable US dominance is approaching its conclusion. As a result, the Washington administration must rely on cooperation with partners and friendly alliances. The major theatre of war (MTW) partners of the United States in the intelligence sphere are Great Britain and other members of the Five Eyes intelligence alliance (a strategic partnership between the United States, Great Britain, Australia, New Zealand and Canada in the field of intelligence).

In the contemporary world, three key trends have been identified by V. Burns. Firstly, the challenge of strategic competition from a growing and ambitious China and from Russia, which constantly reminds us that a declining power can be at least as destructive as a rising one, must be acknowledged. In the opinion of V. Burns, the most significant long-term threat to the United States is China, which is regarded as the most substantial geopolitical and intelligence-related adversary. In contrast to Russia, China possesses the economic, diplomatic, military and technological capabilities to reshape the global order. In this regard, the US CIA has established a China Mission Centre, whose activities are focused exclusively on the observation of this country and ensuring coordination with all other US intelligence agencies with regard to the PRC. It is evident that the United States Central Intelligence Agency (CIA) has increased its expenditure on China by 100% over the past two years. As V. Burns has observed, American intelligence is, on the one hand, enhancing its capabilities to compete with the People's Republic of China (PRC) on a global scale, and, on the other hand, endeavouring to maintain communication with China in order to avoid dangerous misunderstandings and accidental incidents.

Burns stressed that the problem is not China's rise as such, but the actions that accompany it. President Xi is beginning his third term with more power than any Chinese leader since Mao. And instead of using that power to strengthen, revitalise and renew the international system that made China's transformation possible, he is seeking to rewrite it.

He also stressed that the most immediate and acute geopolitical challenge to the international order today is Vladimir Putin's full-scale invasion of Ukraine. Although, as Mr. Burns noted, Russian

aggression is a difficult test, the only country that intends to change the international order is China, and, moreover, has the economic, diplomatic, military and technological power to do so.

Burns V. believes that Putin's war has been a strategic failure for Russia its military vulnerabilities have become apparent; its economy has been devastated; its future is as China's "junior partner" and "economic colony"; its revanchist ambitions have been rebuffed by the North Atlantic Alliance, which has grown in size and become even stronger.

Second, there are stateless problems, such as the climate crisis and global pandemics, which are beyond the reach of any single country and are becoming increasingly existential.

COVID has shown every government the danger of being dependent on a single country for vital medical supplies, just as Putin's aggression in Ukraine has clearly shown every government the risks of being dependent on a single country for energy sourcing. In today's world, no country wants to be at the mercy of a cartel for an important mineral or technology, especially a country that has demonstrated the will and ability to deepen that dependence and use it as a weapon. The answer to this question is not to disconnect from an economy like China's, which would be foolish, but to intelligently reduce risks and diversify by ensuring resilient supply chains, protecting our technological advantage, and investing in industrial capacity.

And thirdly, it is a technological revolution that is changing the way we live, work, fight and compete, with opportunities and risks that we cannot yet fully understand.

In this regard, V. Burns emphasises that progress in computer-related technologies – from chips to quantum and artificial intelligence – is leading to crack-throughs of extraordinary scale and scope. In just a few months since the first public release of ChatGPT in November last year, we have seen newer models outperform humans on entrance exams to graduate school and in evaluation of doctor-patient interaction in medical training programmes.

Leadership in technology and innovation has been the foundation of our economic prosperity and military strength. It has also been critical to establishing rules, norms, and standards that protect our interests and our values. Our Chinese rivals understand this as well as anyone else, and so it is no surprise that they are investing heavily in cutting-edge technologies as a central dimension of our strategic competition.

It is telling that the U.S. intelligence community's annual report on global threats to national security (Annual threat assessment of the U.S. intelligence community. March 2025) states: "Russia, China, Iran, and North Korea — individually and collectively — challenge U.S. interests around the world, by attacking or threatening others in their regions, using both asymmetric and traditional tactics of hard power, and promoting alternative systems to compete with the United States, primarily in the areas of trade, finance, and security. They seek to challenge the United States and other countries through targeted campaigns to gain advantage while avoiding direct war. The growing cooperation between these adversaries strengthens their resilience against the United States, increases the capability for reinforcement for military action with one of them that could draw in the other, and puts pressure on other global players to take sides... " (Office of the Director of National Intelligence, 2025).

In addition, the above-mentioned report emphasises that the PRC is likely to continue to position itself as the country with the upper hand in a potential conflict with MultiCam. The PRC will continue to pressure Taiwan to reunify and will continue to conduct large-scale cyber operations against American targets for both espionage and strategic advantage. China is likely to attempt to sufficiently restrict the activities of Chinese companies and criminal elements that supply and illegally traffic fentanyl precursors and synthetic opioids to the United States, unless more aggressive measures are taken by law enforcement agencies.

Beijing will continue to strengthen its conventional military capability for reinforcement and strategic forces, intensify competition in space, and maintain its industrial and technology-intensive economic strategy to compete with US economic power and global leadership.

China poses the most substantial and influential military threat to the national security of the Lienie MultiCam. The People's Liberation Army (PLA) is developing combined forces capable of full-spectrum warfare. This is in order to counter US intervention in regional conflicts, extend its power globally, and defend what Beijing considers its sovereign territory. A significant proportion of China's military modernisation endeavours is dedicated to the development of counter-intervention mechanisms that are customised to encompass all dimensions of US and allied military operations within the Pacific region. The capital city of China has set itself the ambitious target of achieving key modernisation milestones by 2027 and 2035, with the aim of transforming the People's Liberation Army (PLA) into a world-class military by 2049.

Of particular note is that China is using an aggressive whole-of-government approach, combined with state control of the private sector, to become a global scientific and technological superpower, surpass the US, provide contributory support for self-sufficiency, and achieve further economic, political, and military advantages. Beijing has prioritised technology sectors such as advanced energy, artificial intelligence, biotechnology, quantum computing and semiconductors, challenging efforts to protect critical technologies by tailoring restrictions narrowly to address homeland security concerns. China is accelerating its scientific and technological progress through a range of legal and illegal tools, including investment, acquisition and theft of intellectual property, cyber operations, talent recruitment, international cooperation and sanction evasion.

In turn, on 19 March 2025, the European Commission presented the "White Paper on European Defense – Readiness 2030" (European Commission, 2025).

The international order is changing. A new one will emerge in the second half of this decade. Europe must actively participate in these processes to avoid the danger of becoming a "passive recipient" of the consequences of the new order, including the prospect of full-scale war. The challenges to European security are strategic in nature and require a strategic response. The traditional spectrum of different types of security threats is rapidly expanding, and the interconnections between them are intensifying, as evidenced by repeated cases of terrorism and violent extremism, hybrid attacks, and the actions of international organised crime groups and cybercriminal networks. There is evidence of links between criminal groups and hostile state actors, which can easily cross borders thanks to new technologies. Due to their geographical proximity, European states are constantly confronted with migration caused by the effects of war and climate change in North Africa and the Middle East. The Arctic is becoming a new arena for geopolitical competition in the north of the continent.

Russia poses a significant strategic threat, forcing Europe and its partners to confront the reality of intense, large-scale mechanised warfare on the European continent, a scenario last observed 80 years ago. The Russian Federation, the most heavily armed European state, is developing a military economy with the objective of achieving its military goals through industrial mobilisation and technological innovation. Furthermore, it is expanding its military economy with the support of Belarus, North Korea and Iran. The Russian Federation has declared its ongoing state of war with the West. Should the objectives of the Russian Federation be realised in Ukraine, it is likely that its territorial ambitions will extend beyond the borders of the country.

Hybrid threats are intensifying, such as cyberattacks, sabotage (particularly in the Baltic and Black Seas), electronic interference in the global navigational and satellite systems, disinformation campaigns, political and industrial espionage, and the use of migration as a weapon. Geopolitical rivalry has not only led to a new phase in the arms race, but has also triggered a global technology race. Technology will become a major theater of war (MTW of competition in the new geopolitical

environment. A number of critical and enabling technologies (artificial intelligence, bio- and quantum technologies, robotics, hypersonic technologies) are key components of both long-term economic growth and military advantage.

In light of the fundamental shifts in the strategic environment, it is imperative for Europe to develop a sufficient capability for reinforcement to deter potential aggression. The EU acknowledges the responsibility of Member States for their own armed forces, encompassing all aspects from doctrine development to deployment characteristics and requirements. The European Union has a considerable capacity for reinforcement, which can support and coordinate efforts to strengthen the defence industrial base and overall defence readiness of the European Union by:

contributory support for closer cooperation and effective scaling of the European defence industry in the development, production and promotion of weapon systems;

improving the effectiveness, interchangeability and interoperability of under arms, reducing outlays by avoiding competitive procurement and improving the purchasing power of Member States, as well as ensuring stability and predictability through long-term industrial orders;

supporting dual-use infrastructure for mobility, space communications, navigation and observation;

contributory support for various forms of partnership.

Conclusions

The concept of national interests is a multifaceted system encompassing the vital needs of the state and society, as well as the cultural and spiritual values inherent in the populace. The purpose of national interests is to ensure the well-being of the state and to minimise (or eliminate) threats to its security.

The concept of national interests is multifaceted in nature, encompassing both external (international) and internal (domestic) dimensions. These interests serve as the foundational basis for the formulation of state policy in the long term. The study indicates that national interest functions as a pivotal mechanism in the delineation of intelligence agency objectives. It can be posited that strategic competition, common transnational imperatives, and a technological revolution that is unparalleled in the annals of human history collectively engender an exceedingly intricate international landscape. This focus necessitates a re-evaluation of the role of intelligence in this rapidly evolving world.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

Burns, W. J. (2023). *A world transformed and the role of intelligence* (59th Ditchley Annual Lecture). The Ditchley Foundation. https://www.ditchley.com/sites/default/files/Ditchley%20Annual%20Lecture%202023%20transcript.pdf

Burns, W. J. (2024). *Spycraft and statecraft: Transforming the CIA for an age of competition*. *Foreign Affairs*. https://www.foreignaffairs.com/united-states/cia-spycraft-and-statecraft-william-burns

European Commission. (2025). *Joint white paper for European defence readiness 2030* (Brussels, March 19, 2025). https://defence-industry-space.ec.europa.eu/document/download/30b50d2c-49aa-4250-9ca6-27a0347cf009_en?filename=White%20Paper.pdf

McMaster, H. (2023). *Fields of battle: The struggle to defend the free world*. Our Format.

Morgenthau, H. J. (1982). *In defense of the national interest*. University Press of America.

Office of the Director of National Intelligence. (2025). *Annual threat assessment of the U.S. intelligence community* (March 2025). https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf

Rosenau, J. (1968). National interest. In *International encyclopedia of the social sciences* (Vol. 11, pp. 34–40). Macmillan.

Wilson, W. (1970). *College and state: Educational, literary and political papers (1875–1913)* (R. S. Baker & W. E. Dodd, Eds.; Vol. 2). Columbia University Press.

AN INVESTIGATIVE HISTORY OF RUSSIAN SPEECH MANIPULATION STRATEGIES IN REPUBLICAN DISCOURSE

Aaron Helmbrecht

Master of Professional Studies, Communications Specialist, e-mail: helmbrecht@gwu.edu, ORCID: https://orcid.org/0009-0007-9456-522X

Department of Veterans Affairs, Office of Information and Technology, Washington, DC, United States

Received: December 17, 2025 | Revised: December 28, 2025 | Accepted: December 31, 2025

DOI: https://doi.org/10.33445/psssj.2025.6.4.2

Abstract

Donald Trump's sophisticated use of speech manipulation strategies has inspired numerous research studies. O.I. Nazarenko and O.Ye. Nesterenko (2023) looked beyond Donald Trump at the Republican Party at large and found a pattern of manipulative effect in Republican discourse supporting Russia in the Russian-Ukrainian war. This raises many important questions for researchers. What is the political motivation for Republicans to side with Russia against Ukraine? How did this come to be? To answer these questions, this article presents the first recorded history of Russian speech manipulation strategies in Republican discourse. Continuous sampling of Republican discourse employed pattern analysis and purposive and random selection to establish a corpus of 10 quotes presented as a series of historical episodes forming a narrative with a plot. Pragmatic analysis and critical discourse analysis identified manipulative strategies consistent with Russian thinking of reflexive control connected across speakers and generations. The findings reject the "ideological asymmetry hypothesis" and support the novel "freedom grift hypothesis" which proposes conservatives' unique susceptibility to political misrepresentations is the result of covert Russian information warfare. This exploratory study supports the need for further speech manipulation research of Republican discourse from a historical perspective as a matter of urgent global security.

Key words: Manipulative Effect, Speech Manipulation, Political Discourse, Russia, Ukraine, History, Republican.

Introduction

Valentina E. Chernikova et al. (2015) argue that manipulation of mass consciousness is one of the most serious and widely discussed problems of our time. Manipulation is a form of deception employed to serve the manipulator's aims and needs (Abuelwafa, 2021) against the best interests of dominated groups (van Dijk, 2006). Interpersonal Deception Theory tells us that all forms of deception come with risk (Buller & Burgoon, 1996). The manipulator must weigh the risks of detection against the rewards of success. This makes motive a key parameter to discriminate manipulation for analysis (Akopova, 2013).

Nazarenko and Nesterenko (2023) conclude that because politicians are motivated by winning, the manipulative effect they found in Republican discourse must be aimed at convincing Republican voters of the need to support Russia in the Russian-Ukrainian war. If this is true, then Republican politicians are assuming the deception risk to benefit Russia against their own best interests. According to Aysa Akopova's (2013) motive parameter, the Republican speaker is the victim in this scenario and Russia must somehow be the manipulator. Nazarenko and Nesterenko (2023) don't address this point but suggest, "researching the problem with further analysis of various types of discourse concerning the implementation of manipulative influence using all possible linguistic methods and means" is appropriate.

Essential elements of speech manipulation

Definitions of manipulation vary slightly in the literature. Kuralay Kenzhekanova et al. (2015) offer a general academic definition of manipulation as, "impact on the person with the purpose to induce him [to act or change behavior] unconsciously or contrary to his own desire, opinion and intention." Language offers a whole arsenal of means to realize manipulative aims and there is no comprehensive dictionary of manipulative techniques (Akopova, 2013).

David Buller et al. (1994) identify three types of deception: falsification (lying), equivocation (distortion), and omission (concealment). A distinction between falsification and manipulation is that a lie stands up against semantic truth while manipulation opposes pragmatic truth (Akopova, 2013).

Akopova (2013) divides linguistic manipulation into rational and emotional components. The rational sphere uses convincing facts and arguments that impact people's consciousness. Emotional manipulation uses the speaker's expression of emotions to acquire an emotional response from the listener that would lead to changes in his behavior. Emotional manipulation can be "direct" where the speaker openly presents his demands, or "indirect" where the speaker does not openly express his intentions.

Literature review

Historical literature on the matter is documented from two academic perspectives. One corpus comes from discourse analysts and primarily focuses on investigating specific speech manipulation concepts in political discourse. The other corpus comes from security and intelligence analysts and focuses on the history of Russian information warfare against the United States.

According to security and intelligence analysts, both the United States and the Soviet Union used covert disinformation tactics to challenge each other's ideological systems (Evans, 2022). Russia and the Soviet Union have a rich tradition of conducting this type of warfare and "Target No. 1 was the United States…The objective was to hurt the United States wherever and whenever it was possible" (Jones, 2025). Despite the threat, no historically significant event or operation by either side is reported to have occurred during the Cold War.

The earliest records of Russian means of manipulative effect in Republican discourse occur during the 2016 US presidential election where Russia used trolls, bots, and fake news websites to disseminate large amounts of disinformation supporting Donald Trump (Matherly et al., 2020). This strategy proved effective as conservatives are more often fooled by bots purporting to share their ideology than liberals (Garrett & Bond, 2021).

Luiza-Maria Filimon (2016) provides the most relevant source among the discourse analysts. Her work investigated the history of "dog whistle" politics in Republican discourse. A Dog Whistle Effect is observed when "respondents hear something in the question that researchers do not… these quasi-subliminal messages seem innocent to a general audience but resonate with a specific public attuned to receive them" (Filimon, 2016).

Filimon (2016) found a pattern of manipulative effect in Republican discourse which she calls "a deliberate strategy pursued for over fifty decades by the conservative members of the Republican Party… tracing it back to Republican figures such as Lee Atwater, Barry Goldwater or Ronald Reagan". Filimon (2016) cites previous research in concluding strategic racism to be the motivation. Racial dog whistles allow politicians to expand their voter base by covertly appealing to the existing bigotry in the voting public while concealing the racism from opponents.

Filimon (2016) had no reason to suspect the possibility of Russian involvement in the propagation of racial dog whistles to create division or schismogenesis amongst the American populace and exert coercive control over Republican politicians by making them reliant on manipulative strategies to win elections. Motivated by Nazarenko and Nesterenko (2023), the theoretical framework presented in the next section explores this possibility.

Other discourse scholars have investigated specific manipulative strategies used in political discourse, though not necessarily from a historical perspective or limited to Republican discourse. Semantic shifts, doublespeak, and euphemisms/dysphemism are among the most relevant strategies to this study. Semantic shifts include changing word meaning, shifting meaning in contexts, and exploiting emotional or cultural connotation of words with strong meanings (e.g. freedom) to subtly lead public opinion (Meisuri & Al-Haddad, 2025). Doublespeak is language carefully constructed to stretch the truth in ways that impart a reality that is most desirable for the speaker (Walker et al., 2021). Euphemisms represent reality in a more favorable light. The opposite aim is pursued by dysphemism based on underlining a certain negative feature (Kenzhekanova et al. 2015; Walker et al., 2021).

The bulk of recent research in this area is forward-looking, focusing on discursive models and linguistic features observed in Donlad Trump's statements (Moghadam & Jafarpour, 2022). The aim of this article is to look back and provide the first history of Russian speech manipulation strategies in Republican discourse to answer the following research questions:

1. When and how did speech manipulation benefiting Russia become integrated into Republican discourse?
2. What strategies and techniques were used to produce the manipulative effect?
3. How did these speech manipulation strategies evolve over time?
4. What were the hidden messages and motivations behind the speech manipulation?
5. Why are Russian speech manipulation strategies targeted to conservatives rather than liberals?

Theoretical background

R. Kelly Garrett and Robert M. Bond (2021) found that conservatives are uniquely susceptible to political misperceptions and tend to exhibit higher sensitivity than liberals to claims that threaten their political interests, regardless of the claims' accuracy. Garrett and Bond (2021) offer the "ideological asymmetry hypothesis" as a possible explanation which says conservatives are more motivated by a need for certainty and order which leads them to be more resistant to contradictory evidence, a concept now known as knowledge resistance (Glüer & Wikforss, 2022). This leads conservative media to generate or amplify misleading content in response to consumer demand (Garrett & Bond, 2021). Garrett and Bond (2021) conclude that their study fails to provide definitive evidence about ideological asymmetry and does not rule out other possible explanations.

Nazarenko and Nesterenko (2023) suggest a scenario where Republican speakers are the victim and Russia is the manipulator. The "means, motive, and opportunity" (MMO) framework is a multidisciplinary tool of analysis used to examine the likelihood of a given action or evaluate the conditions necessary for an action based on the convergence of three domains: means (capability to act), motive (reason to act), and opportunity (chance to act) (Bird et al., 2022). With motive established by previous research (Nazarenko & Nesterenko, 2023), this theoretical framework will examine the means and opportunity domains to determine the likelihood of such a scenario.

Means

Since 2016, there is a growing body of evidence of Russian influence in Republican discourse. Intelligence analysts call this reflexive control, "a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action" (Matherly et al., 2020). Reflexive Control Theory stipulates that "the adversary who better understands their opponent's decision-making process and utilizes it against them is more likely to succeed" (Matherly et al., 2020).

In 2024, the US Justice Department unsealed an indictment accusing two Russian nationals of recruiting conservative commentators to unwittingly propagate Russian propaganda (Schmunk, 2024). The news media quickly identified these conservative commentators as members of Tenet Media, sharing clips such as Tenet commentator Tim Pool shouting to his audience: Ukraine is the enemy of this country [America]! (Nimrod Kamer, 2024). Vladimir Putin views enemy image as the primary perception to be exploited, constructed, and advanced (Pagen, 2020). With enemy image, "one considers the other nation as evil, opportunistic, and motivated by self-interest" (Alexander et al., 2005).

According to P.B. Craik (2019), Russia's information warfare strategy applies postmodernism to manipulate an enemy's psychic condition. Postmodern propaganda is a form of propaganda that manipulates the audience into believing that truth does not exist or that the truth is impossible to know. Postmodern propaganda is different from the old alternate reality propaganda that the Soviets used. Alternate reality propaganda tells the audience to believe a lie, even when the lie conflicts with reality.

Information warfare belongs to the psychological Domain of War. All domains have entry and exit points into other domains (Ajir & Vailliant, 2020). Primary research is required to determine if the entry point of Russian means of manipulative effect in Republican discourse predates the earliest literature records in 2016 (Matherly et al., 2020). Russian means of manipulative effect should be observed to exploit enemy image and align with Russian thinking of reflexive control.

Opportunity

Historians Donald Critchlow and Nancy MacLean (2009) document the conservative movement beginning in 1945 with William F. Buckley Jr., founding editor of the *National Review*, and Senator Barry Goldwater as the genesis. Sampling selection began here as the earliest possible point of entry opportunity for Russian agents. Continuous sampling of conservative political discourse was used to identify the first historically significant instance where means of manipulative effect were observed to exploit enemy image and align with Russian thinking of reflexive control (applied postmodernism would not be reflected in the corpus during the Soviet era).

Aaron Helmbrecht's (2025) theoretical work on polarization of reality (Alesina et al., 2020) and factual belief polarization (Lee et al., 2021) identified a manipulative effect in the language of these conservative principles: *Conservatives gained power because of their commitment to individualism, free markets, limited government, traditional family values, and a strong defense… Above all else… Conservatives believed that communism was a direct threat to the United States* (Critchlow & MacLean, 2009, p. VII-14).

Helmbrecht (2025) argues these conservative principles represent the genesis of speech manipulation in Republican discourse aligning with Russian thinking of reflexive control: *This declaration cannot possibly be genuine because the principles conflict with each other. Individualism is mutually exclusive to traditional family values. Limited government is mutually exclusive to a strong defense. Declaring to support all of these principles simultaneously is absurd. Clearly deception is present in the messaging. Why would a "communist" Russian agent want to advocate for these principles?*

Hypothesis

The theoretical framework suggests that sometime after the start of the Cold War in 1945, Russian agents developed conservative principles as a means of reflexive control and recruited Buckley and Goldwater among others to unwittingly propagate them using speech manipulation strategies. The next section will define tools of analysis and apply them to conservative principles to determine if this opportunity represents the entry point of Russian means of manipulative effect in Republican discourse.

Tools of analysis

Kenzhekanova et al. (2015) discuss the main means of verbal persuasion used in political discourse and their functions in the text. According to Kenzhekanova et al. (2015), lexical tools of speech manipulation are the most extensive and frequently used means of realization, allowing for systematization based on their sign properties (semantics, syntactics, and pragmatics). This section provides a summary of relevant tools of speech manipulation as well as corresponding tools of analysis applied in this study.

Lexical semantics is the study of word meanings and word relations.

a) *Tools of speech manipulation:* Metaphors can be constructed so multiple presuppositions lead the listener to access only the sub-optimal set of contextual assumptions by exploiting emotive connotation (emotional or cultural meaning, both positive and negative, that a word, phrase, or ideology carries beyond its literal definition)
b) *Tools of analysis:* Content analysis and linguistic interpretation

Lexical syntactics refers to the rules governing how a string of characters is broken down into the smallest meaningful units.

a) *Tools of speech manipulation:* Elliptic and parallel constructions (Elliptic language forces the listener to finish the sentence or thought by admission or omission of some elements of the utterance. Parallelism is a compound of two or more words or sentences that implies meaning through the strict compliance of their structure.)
b) *Tools of analysis:* Component analysis and lingo-stylistic analysis

Lexical pragmatics is the study of how word meanings are modified in context, going beyond their literal "encoded" sense.

(a) *Tools of speech manipulation:* Semantic shift strategies use words with strong positive or negative connotation and redefine them in context, effectively applying the connotation to a new definition desirable to the speaker using stylistic connotation (implied meaning of a word or phrase that indicates its suitability for a particular functional style, register, or context)
(b) *Tools of analysis:* Contextual analysis and pragmatic analysis

Example analysis

Let's apply the tools of analysis to these conservative principles: *individualism, free markets, limited government, traditional family values, and a strong defense… communism was a direct threat to the United States*. These principles individually carry a positive connotation. The positive elliptic construction of the series forces the listener to define them as positive. Cognitive mechanisms which govern interpretation of context subsets will only allow the listener to access contextual assumptions positive to the speaker, crucially preventing access to the dissonant, although optimal, set (Maillat, 2013).

"Free markets" is a parallel construction. Freedom is the power or right to act, speak, or think as one wants without hindrance or restraint (Oxford Languages Dictionary, 2025). Freedom has a strong positive emotional and cultural connotation, particularly to Americans who lacked freedom under British rule and gained freedom through revolution. Here freedom is realized through self-government and lost through surrender. Surrender means to cease resistance to an enemy or opponent and submit to their authority (Oxford Languages Dictionary, 2025).

Freedom in the context of "free markets" means a market in which citizens have no political influence or control. Lexical pragmatics imply a "free market" should be controlled by an "invisible hand." The positive presupposition assumes the "invisible hand" is metaphorical, meaning a free market functions without controls. The negative presupposition assumes the "invisible hand" is

literal, meaning a free market is controlled by the invisible hand of the speaker. The listener's positive emotional and cultural association with "freedom" will lead them to surrender their political stewardship over the market in order to realize freedom, and act against those who exercise their political stewardship over the market to defend the realization of freedom. The definitions of "freedom" and "surrender" have semantically shifted in context. Traditional family values that restrict freedom and compel submission such as abortion, marriage equality, and transgender health care have a positive connotation in this context.

If freedom is realized by surrendering your will for political power, then the stylistic connotation of "individualism" and "limited government" imply those who exercise their political power are the enemies of freedom. During the Cold War, "communism" in the context of "a direct threat to the United States" referred to the Soviet Union and Soviet-aligned states. The enemy image of a hostile state (the Soviet Union) is semantically shifted in context to the word "communism" and applied in context to the United States. After the fall of the Soviet Union, lexical pragmatics imply Russia and other hostile states are now potential allies against communism (the United States and the West). This explains how Republicans justify their support for Russia against Ukraine (Nazarenko & Nesterenko, 2023; Reinhart, 2018).

Data and methods

The first stage of research considered all recorded political discourse from 1945 to the present attributed to conservative politicians and commentators generally recognized as historically significant. Continuous sampling identified the first instance of speech manipulation suspected to exploit enemy image (Alexander et al., 2005; Pagen, 2020) and align with Russian thinking of reflexive control (Matherly et al., 2020). A continuous sampling plan employed pattern analysis and a mix of purposive and random sampling to reduce the corpus to 10 quotes presented as a series of historical events forming a narrative with a plot.

The next stage adopted a pragmatic analysis and critical discourse analysis (CDA) approach. Pragmatic analysis is suited to the practice of "specific history", in which "analysts reconstruct, through emplotment, historical episodes that were meaningful to historical actors before they became meaningful as objects of analysis. Analysts endeavor to recover this meaning in order to understand agents' actions and thereby to understand why events turned out the way they did rather than some other way" (Gavan Duffy, 2008, p. 168). CDA is suited to investigate how semantic shifts occur in political discourse and how speech manipulation is used as a tool of domination (Meisuri & Al-Haddad, 2025; van Dijk, 2006).

Data collection

Sampling began with purposive selection of two famous Goldwater quotes suspected to exploit enemy image and align with Russian thinking of reflexive control. The third quote was randomly selected from Buckley's archived political discourse on YouTube by searching for a quote on government. Pattern analysis of this data led to the purposive selection of two famous Ronald Reagan quotes.

A series of three quotes were selected surrounding the historical significance of Sarah Palin's use of falsification. One famous Palin quote was randomly selected as a representative sample. Two quotes from just before and after this event were randomly selected to observe Palin's effect on the historical pattern. One by P.J. O'Rourke was selected based on suspicion that applying Enlightenment-era philosophy to modern democracies was a discursive strategy. The other by Michele Bachmann was selected based on suspicion that Tea Party messaging was intended to exploit enemy image. Postmodernism as a means of reflexive control begins to apply during this period.

Two final quotes representing the modern era were purposively selected using keyword match and pattern analysis. One by Tucker Carlson was selected based on suspected use of sophisticated discursive strategies. The last quote attributed to The Heritage Foundation was selected to diversify the corpus and reduce selection bias.

Limitations

The corpus of 10 quotes was determined to be sufficient to support the objectives of the study without exceeding word count expectations for a research article. It was not possible to review the full archive of Republican political discourse from which the corpus was selected. The continuous sampling plan relied on pattern analysis and a mix of purposive and random sampling to limit selection bias and ensure data attributed to individual speakers was representative of Republican discursive strategies of the time. As qualitative research employing non-probability sampling methods, this study should be considered exploratory.

Data analysis

In this section, I provide analysis applying Kenzhekanova et al.'s (2015) tools of speech manipulation to 10 historical quotes by Republican public figures. I will, to the best of my ability and without bias, identify speech manipulation strategies and techniques, interpret hidden messages and political motivations, and note patterns of interest within the data. I believe these quotes to be accurately transcribed and fairly representative of the speakers' communicative intent and the historical context of the speech. Positive identification of deceit and corrupt motivation does not imply corrupt intent by the speaker. It is likely many or all of these speakers unwittingly propagate speech manipulation they believe to be legitimate. To the best of my knowledge, no evidence challenging the basis for the analysis has been omitted.

1. *Barry Goldwater (July 17, 1964): Extremism in defense of liberty is no vice.*

"Extremism" typically carries a negative connotation as in the context of terrorism (use of violence to achieve policy goals). The connotation changes to positive when extremism is "in defense of liberty". Lexical pragmatics presupposes defense of liberty is necessary because there exists some enemy of liberty. Note how the speaker never identifies this enemy of liberty. The listener is now primed for "extremism" to "defend liberty" against a phantom enemy.

The listener must either deduce the identity of the enemy of liberty based on the speaker's implication and suggestion or wait for confirmation from the speaker. The longer the listener is made to wait, the more paranoid they will become, leaving them more likely to view outsiders as potential enemies and increasing their reliance on the speaker as a source of information and security.

2. *Barry Goldwater (June 19, 1964): I am unalterably opposed to discrimination or segregation on the basis of race, color or creed, or on any other basis… I wish to make myself perfectly clear. The two portions of this bill to which I have constantly and consistently voiced objections… are those which would embark the Federal Government on a regulatory course of action with regard to private enterprise in the area of so-called "public accommodations" and in the area of employment… I find no constitutional basis for the exercise of Federal regulatory authority in either of these areas; and I believe the attempted usurpation of such power to be a grave threat to the very essence of our basic system of government, namely, that of a constitutional republic in which 50 sovereign states have reserved to themselves and to the people those powers not specifically granted to the central or Federal Government.*

This speech by Barry Goldwater using states' rights to justify discrimination is probably history's most famous example of euphemistic speech manipulation. The lexical semantics say racist tendencies are negative, but the lexical pragmatics say racist acts are an exercise of freedom, which is positive. But the racism aspect of the euphemism is arguably not the primary motivation. Note

how the syntax refers to the "Federal Government" as a "usurper" and the "exercise of Federal regulatory authority" as "a grave threat to… sovereign states… and to the people." Historically, "the Federal Government" and "the people" are one in the same (e.g. Government of the people, by the people, and for the people shall not perish from this earth; Courts of law refer to the prosecution as "the government" or "the people" interchangeably). Goldwater uses the language of the 10th Amendment (The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people) to semantically separate "the people" and "the Federal Government" into opposing entities in conflict with each other.

3. *William F. Buckley Jr. (1971): It's quite true, for instance, that if governments fail in statecraft, it is necessary for them to conduct wars. By the same token, it is necessary for a government, for instance, the government of Castro Cuba, to ration sugar in the greatest sugar producing country in the world. By the same token, I think Mr. Friedman and I would agree that there are circumstances under which a government might so screw things up that for a period of time it becomes necessary to undertake responsibilities that it ought never to have undertaken.*

Buckley is arguing against the idea that wage and price control regulation should be a proper function of government. The syntax references *governments* (plural), *a government* (hypothetical), and *the government of Castro Cuba* (communist enemy state) in conjunction with the pejoratives: *fail in statecraft, conduct wars, ration sugar, screw things up*. The stylistic connotation combines communism (the government of Castro) with the enemy image of a hostile state (Castro Cuba) and applies it to the United States (a government) and the West (governments).

4. *Ronald Reagan (1986): The nine most terrifying words in the English language are: I'm from the Government, and I'm here to help.*

The stylistic connotation presents this message in the context of a joke. However, the semantic meaning shifts when removed from the context of the oral presentation. If the nine most terrifying words in the English language are, I'm from the government and I'm here to help, that means the government is our enemy. We see this strategy still employed today in the common internet meme: You might be suffering the side effects of Northern Virginia called Stockholm Syndrome. While presented in the context of a joke, if I have Stockholm Syndrome, that means the government is our enemy.

5. *Ronald Reagan (1975): We've asked so much of government, and we've gotten into the habit over the last 40 years of thinking that government has the answers. There's very little that government can do as efficiently and as economically as the people can do themselves, and if government would just shut the door and sneak away for about three weeks, we'd never miss them.*

The semantically correct version of this statement should be: There's very little that government can do as efficiently and as economically as *individual persons* can do themselves. Again, we see the semantic separation of "government" and "the people" into opposing entities in conflict with each other. The same message repeated across speakers and generations: The citizen is sovereign and the government is their enemy.

6. *P. J. O'Rourke (2005): The Wealth of Nations argues three basic principles and, by plain thinking and plentiful examples, proves them. Even intellectuals should have no trouble understanding Smith's ideas. Economic progress depends upon a trinity of individual prerogatives: pursuit of self-interest, division of labor, and freedom of trade.*

The stylistic connotation implies logical reasoning by "plain thinking and plentiful examples" is positive and the scientific method of "intellectuals" is negative. The speaker's direct motivation is

advocacy for ideological policies such as “freedom of trade”. Conservative support for presidential tariff actions (Congress.gov, 2025) suggests “freedom of trade” was never a genuine conservative principle. The true motivation is to promote “plain thinking and plentiful examples” over critical thinking and peer review.

7. *Sarah Palin (2009): The America I know and love is not one in which my parents or my baby with Down syndrome will have to stand in front of Obama’s ‘death panel’ so his bureaucrats can decide, based on a subjective judgment of their ‘level of productivity in society,’ whether they are worthy of health care. Such a system is downright evil.*

With Sarah Palin we see speech manipulation begin to incorporate falsification on a large scale. Here we see the traditional strategy of semantic separation of “America” and “bureaucrats”, but adds obvious falsification like “death panels”. The historical perspective of this work provides valuable insight into why these obvious falsifications are undetectable to so many conservatives (Garrett & Bond, 2021). Conservatives have been programmed to rely on “plain thinking” while perceiving outsiders to be potential enemies.

8. *Michele Bachmann (2011): The Tea Party is a dynamic force for good in our national conversation… Many of you implored Washington to please stop spending money that we didn't have, but instead of cutting, we saw an unprecedented explosion of government spending and debt. It was unlike anything we've seen before in the history of the country… Instead of a leaner, smarter government, we bought a lot of bureaucracy that now tells us what light bulbs to buy, and which may put 16,500 IRS agents in charge of policing President Obama’s health care bill… In the end, unless we fully repeal Obamacare, a nation that currently enjoys the world’s finest health care might be forced to rely on government run coverage that could have a devastating impact on our national debt for generations to come.*

To Americans, The Tea Party is symbolic of justified violent revolution on the basis of taxation without representation. The stylistic connotation omits the “taxation without representation” part. The enemy image of a hostile state (the British) is replaced with: *Washington, IRS agents, bureaucracy, government*. The parallel syntax implies that a “leaner” government would be a “smarter” government. We now see obvious falsifications are fully incorporated into the strategy: *bureaucracy that now tells us what light bulbs to buy, 16,500 IRS agents in charge of policing President Obama’s health care bill, a nation that currently enjoys the world’s finest health care*. Recall also how Bachmann gave this speech staring awkwardly off to the side instead of speaking directly into the camera. This produces a manipulative effect of disorientation, reducing the listener’s ability to focus attention on detecting deceptive language.

9. *Tucker Carlson (2017): There’s construction going on. There always is in Washington, the richest city in America. We want to thank you for that, for sending your tax dollars here. It’s built a pretty nice place. Well, Bill Nye the Science Guy is now aspiring to a new title, Bill Nye the Psychoanalyst Guy. During a Facebook Live event with Senator Bernie Sanders today the mechanical engineer and TV personality said skeptics of climate change suffer from the psychological delusion of cognitive dissonance. That’s a slight bump up from last year, when he was open to the idea of imprisoning skeptics of global warming as war criminals. Is that the choice? Bellevue or Nuremberg? Bill, it’s great to see you. That doesn't sound like science to me, Bill Nye the Science Guy. That sounds like something very different.*

The first red flag of deception is that Tucker Carlson is *debating* Bill Nye the Science Guy on the issue of climate change. Bill Nye is the proper authority on the matter and climate change science is taught at the middle school level. Carlson opens by reinforcing “Washington” as the enemy with obvious falsification, *the richest city in America*. The stylistic connotation of *sending your tax dollars here*

implies misappropriation. Carlson then refers to Nye as a *mechanical engineer and TV personality*. Mechanical engineer implies Nye is not a proper authority because climate science is outside his area of expertise. TV personality implies Nye and Carlson share the same title and thus speak with equal authority. Carlson then semantically redefines the word "skeptic." There is no such thing as a climate change skeptic. Skeptics can be persuaded by logic and evidence. Climate change deniers are either deceivers or manipulation victims. Carlson then emotionally manipulates his audience with the terms: *imprisoning skeptics, war criminals, Bellevue or Nuremberg*. This tactic of manipulation and coercive control exploits lexical pragmatics to imply that the victim will suffer a worse fate from a dangerous world if they choose to leave their protection.

10. *Thomas Spoehr and Wilson Beaver (2023): Defense Dollars Saved Through Reforms Can Boost the Military's Lethality and Capacity: Defense spending should be tied to a national defense strategy that is designed to protect the nation's security interests. Economic security is also national security, and out-of-control federal spending has helped contribute to the current inflation and the ever-expanding national debt threatening the nation. To this end, Congress should look carefully at potential defense savings and efficiencies as it seeks to decrease the amount spent on non-defense spending and inefficiencies. To the extent that they are able, the Department of Defense and Congress should identify efficiencies within the defense budget and ensure that taxpayers' dollars are being allocated responsibly and to the right priorities.*

Here "lethality" is defined as positive connecting it to *capacity, efficiency, responsibility, the right priorities*. "Federal spending" is defined as negative with the terms: *out-of-control, ever-expanding, inefficiencies, threatening the nation*. The stylistic connotation implies a positive correlation between lethality and security. Other critical security aspects such as intelligence, public education, and economic growth are implied through omission to be *non-defense spending and inefficiencies*. The aim of verbal communication is depoliticization (Federal spending is negative) and radicalization (lethality is positive) of the American populace. The message is (say it with me now): *The government is our enemy.*

Results and discussion

Analysis presented in this article support Filimon's (2016) conclusion that speech manipulation in Republican discourse is, "a deliberate strategy pursued for over fifty decades," and advances academic thought with the following findings:

- Conservative principles employ discursive strategies that semantically shift the definitions of "freedom" and "surrender" and project Russia's enemy image onto the United States government.
- Discursive strategies used by William F. Buckley Jr., Barry Goldwater, Ronald Reagan, and Michele Bachmann exploit enemy image consistent with Russian thinking of reflexive control.
- Conservatives have been programmed to trust "plain thinking" while perceiving outsiders to be potential enemies.
- Republican discursive strategies evolved to incorporate obvious falsifications concurrent with Russia's adoption of applied postmodernism.
- The aim of verbal communication is depoliticization and radicalization of the American populace. The key message is: *Let's tell the American people the government is their enemy*. This suggests Republican discourse employs military grade manipulation strategies.

These finding date Russian means of manipulative effect in Republican discourse well before the earliest records in 2016 (Matherly et al., 2020). The findings also reject the "ideological asymmetry hypothesis" and support the novel "freedom grift hypothesis."

Conclusions

A post-truth era does not emerge by accident or happenstance. Russian speech manipulation strategies in Republican discourse originated with conservative principles introduced by William F. Buckley Jr. and Barry Goldwater, became mainstream under Ronald Reagan, incorporated obvious falsification under Sarah Palin, and continues to grow under Donald Trump.

By studying this history, we now know the strategy works by manipulating lexical units to change word meanings, modify word meanings in context, and exploit emotional or cultural meanings of strong words such as government, freedom, and communism. Perhaps most importantly, we know the motivation (depoliticization and radicalization of the American populace) and the key message (the government is our enemy). If all this can be discovered from this short work, imagine what knowledge lies beneath the surface. Imagine how that knowledge might guide the present and shape the future.

Enas Naji Kadim (2022) closes her work with a plea for manipulative politicians to abandon their manipulative strategies for the sake of the people's interests and suggests manipulation victims should "develop their critical literacy and critical language awareness skills". This author's plea is to the academics and the investigators. The historians and political scientists. The psychologists and journalists. The security and intelligence community. We must understand the history of how things came to be before we can recommend a plan of action to the public.

Albert Einstein famously said, "I know not with what weapons WWIII will be fought, but WWIV will be fought with sticks and stones". Einstein's implication is that WWIII would be fought with weapons more technologically advanced and destructively powerful than the atomic bomb he helped create. Perhaps we misinterpreted Einstein's guidance all along. Perhaps WWIII will be a war of words, the main battle space in the minds of the people. A war of words asks scholars to be patriots.

Funding statement

This study received no specific financial support.

Declaration of conflicting interest

The author declares that he has no competing interests.

Data availability

Data and links referenced in this article are available in the article appendix.

Appendix

Historical quotation data was transcribed by the author from the following sources and are listed here in order of appearance.

Wicker, T. (1964). Convention Ends; Extremism in defense of liberty 'no vice,' Arizonan asserts – The New York Times, [online] 17 July. Available at: https://www.nytimes.com/1964/07/17/archives/convention-ends-extremism-in-defense-of-liberty-no-vice-arizonan.html [Accessed: 4 November 2025].

The New York Times. (1964). Text of Goldwater speech on rights - The New York Times, [online] 19 June. Available at: https://www.nytimes.com/1964/06/19/archives/text-of-goldwater-speech-on-rights.html [Accessed: 4 November 2025].

The Advocates. (1971). Should the government adopt long-term wage and price controls for selected unions

and industries? – YouTube, [video] 5 January. Available at: https://youtu.be/4J_t-sddizg?si=RTwBMjCD8QGSEUPD&t=1950 [Accessed: 4 November 2025].

Ronald Reagan Presidential Library & Museum. (1986). A Selected Quote From: The President's News Conference – YouTube, [video] 12 August. Available at: https://youtu.be/nCedOQJ0ZEA?si=Fz0QFjwpuSoSHZqx [Accessed: 4 November 2025].

The Tonight Show with Johnny Carson. (1975). Ronald Reagan: Big government causes big problems – YouTube, [video] 3 January. Available at: https://www.youtube.com/watch?v=g546pyP_zDQ [Accessed: 4 November 2025].

O'Rourke, P.J. (2005). On 'The Wealth of Nations' – The New York Times, [online] 7 January. Available at: https://www.nytimes.com/2007/01/07/books/chapters/0107-1st-orou.html [Accessed: 4 November 2025].

Barr, A. (2009). Palin doubles down on 'death panels' – Politico, [online] 13 August. Available at: https://www.politico.com/story/2009/08/palin-doubles-down-on-death-panels-026078 [Accessed: 4 November 2025].

CBS. (2011). Bachmann blasts Obama in Tea Party response – YouTube, [video] 26 January. Available at: https://www.youtube.com/watch?v=VFHTaTgGdyo [Accessed: 4 November 2025].

Fox News. (2017). Tucker vs. Bill Nye the Science Guy – YouTube, [video] 27 February. Available at: https://www.youtube.com/watch?v=qN5L2q6hfWo [Accessed: 4 November 2025].

Spoehr, T., & Beaver, W. (2023). Defense dollars saved through reforms can boost the military's lethality and capacity – The Heritage Foundation, [online] 26 May. Available at: https://www.heritage.org/defense/report/defense-dollars-saved-through-reforms-can-boost-the-militarys-lethality-and-capacity [Accessed: 4 November 2025].

References

Abuelwafa, M.A. (2021). Legitimation and Manipulation in Political Speeches: A Corpus-based Study. *Procedia Computer Science*, 189, pp. 11–18. https://doi.org/10.1016/j.procs.2021.05.066.

Ajir, M., & Vailliant, B. (2020). The case for the sixth domain of war: psychological warfare in the age of advanced technology. *Global Security and Intelligence Studies Journa*l, 5(1) 1-17. https://doi.org/10.18278/gsis.5.1.2

Akopova, A. (2013, December 20). *International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE)*. https://ijcrsee.com/index.php/ijcrsee/article/view/13

Alesina, A., Miano, A. and Stantcheva, S. (2020). The Polarization of Reality. *AEA Papers and Proceedings*, 110, pp. 324–328. https://doi.org/10.1257/pandp.20201072.

Alexander, M.G., Levin, S. and Henry, P.J. (2005). Image theory, social identity, and social dominance: structural characteristics and individual motives underlying international images. *Political Psychology*, 26: 27-45. https://doi.org/10.1111/j.1467-9221.2005.00408.x

Bird, K. I., Nichols, V. A., Garay, E. S., Nowatzke, M., Essary, C., Post, K. K., ...Cortus, E. L. (2022). Means, motive, and opportunity: A method for understanding stakeholder agency within food–energy–water systems. *Elementa Science of the Anthropocene*, *10*(1), 00066. https://doi.org/10.1525/elementa.2021.00066

Buller, D.B., Burgoon, J.K., White, C.H. and Ebesu, A.S. (1994). Interpersonal Deception VII. *Journal of Language and Social Psychology*, 13(4), pp. 366–395. https://doi.org/10.1177/0261927x94134002.

Chernikova, V.E., Parsieva, L.K., Taisaeva, B.M., Ramazanova, S.R. and Moskalenko, D.N. (2021). Manipulation Of Mass Consciousness as a Phenomenon of the Information Society. *European Proceedings of Social and Behavioural Sciences*. https://doi.org/10.15405/epsbs.2021.11.55.

Congress.gov (2025). Presidential 2025 Tariff Actions: Timeline and Status. [online] Available at: https://www.congress.gov/crs-product/R48549. (Accessed: Nov. 4, 2025).

Craik, P. B. (2019). *The Weaponization of Postmodernism: Russia's New War with Europe* (No. 146). LEQS Paper. https://hdl.handle.net/10419/303429

Critchlow, D.T. and Maclean, N. (2009). *Debating the American conservative movement: 1945 to the present*. Lanham: Rowman & Littlefield.

Duffy, G. (2008). Pragmatic Analysis. In: Klotz, A., Prakash, D. (eds) Qualitative Methods in International Relations. Research Methods Series. Palgrave Macmillan, London. https://doi.org/10.1057/9780230584129_11

Evans, J. (2022). Putin's information war against the United States. *Russian Analytical Digest*, 282, 9-12. https://doi.org/10.3929/ethz-b-000541999

Filimon, L. M. (2016). From the dog whistle to the dog scream: The Republican party's (ab) use of discriminatory speech in electoral campaigns and party politics. *Romanian Journal of Society and Politics*, 11(2), 25-48. https://www.ceeol.com/search/article-detail?id=512758

Garrett, R.K. and Bond, R.M. (2021). Conservatives' susceptibility to political misperceptions. *Science Advances*, 7(23). https://doi.org/10.1126/sciadv.abf1234.

Glüer, K. and Wikforss, A. (2022). What is knowledge resistance? In *Knowledge resistance in high-choice information environments* (pp. 29-48). Routledge. https://doi.org/10.4324/9781003111474-2

Helmbrecht, A. (2025). The freedom grift hypothesis: A qualitative analysis of the theoretical conquest of the United States using information manipulation theory. *International Journal of Political Science and Governance*, 7(10), pp. 399–408. https://doi.org/10.33545/26646021.2025.v7.i10a.708.

Jones, S. G. (2025). *Russia's shadow war against the West.* Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/russias-shadow-war-against-west#h2-russian-shadow-wars-the-historical-context

Kadim, E.N. (2022). A Critical Discourse Analysis of Trump's Election Campaign Speeches. *Heliyon*, 8(4), p.e09256. https://doi.org/10.1016/j.heliyon.2022.e09256.

Kenzhekanova, K., Zhanabekova, M. and Konyrbekova, T. (2015). Manipulation in Political Discourse of Mass Media. *Mediterranean Journal of Social Sciences*. https://doi.org/10.5901/mjss.2015.v6n4s1p325.

Lee, N., Nyhan, B., Reifler, J. and Flynn, D.J. (2020). More Accurate, But No Less Polarized: Comparing the Factual Beliefs of Government Officials and the Public. *British Journal of Political Science*, pp. 1-8. https://doi.org/10.1017/s000712342000037x.

Maillat, D. (2013). Constraining context selection: On the pragmatic inevitability of manipulation. *Journal of Pragmatics*, 59, 190-199. https://doi.org/10.1016/j.pragma.2013.07.009

Meisuri, M. and Al-Haddad, H. (2025). Semantic Shifts in Political Discourse: A Study of Language Manipulation. *Journal of Humanities Research Sustainability*, 2(1), 45–55. https://doi.org/10.70177/jhrs.v2i1.1924

Moghadam, M. and Jafarpour, N. (2022). "Pragmatic Annotation of Manipulation in Political Discourse: The Case of Trump-Clinton Presidential Debate", *Linguistic Forum-A Journal of Linguistics* 4(4), pp. 32-39. https://linguisticforum.com/index.php/ling/article/view/134/89 (Accessed: November 4, 2025).

Nazarenko, O. I. and Nesterenko, O. Y. (2023). Verbal ways and means of manipulative effect in the discourse of the Republicans about the Russian-Ukrainian war. *Вісник Житомирського державного університету імені Івана Франка. Філологічні науки*, 1(99), pp. 105-113. https://doi.org/10.35433/philology.1(99).2023.105-113

Nimrod Kamer. (2024, September 9). Tim Pool delivers pro Putin talking points on air [Video]. YouTube. https://www.youtube.com/watch?v=DDc4dadmjNs

Oxford Languages Dictionary (2025).

Pagen, J. (2020). A new Russian realpolitik: Putin's operationalization of psychology and propaganda. *Global Security and Intelligence Studies Journal*, 5(1) 55-79. https://doi.org/10.18278/gsis.5.1.5

Reinhart, R. (2018). Republicans More Positive on U.S. Relations With Russia. [online] Gallup.com. https://news.gallup.com/poll/237137/republicans-positive-relations-russia.aspx (Accessed: Nov. 4, 2025).

Schmunk, R. (2024, September 5). U.S. accuses Russia of using unwitting influencers, fake news sites to sway presidential election. *CBC*. https://www.cbc.ca/news/world/russia-us-election-interference-websites-influencers-1.7313197

Shigapova, F.F., Titova, E.A., Morozova, T.V. and Sabirova, A.N. (2021). Manipulative Speech Techniques in Political Discourse. *Propósitos y Representaciones*, [online] 9(SPE2), pp. 1020. https://doi.org/10.20511/pyr2021.v9nSPE2.1020.

Styrnik, N. (2025). Linguistic Manipulations in Politics: The US Presidential Campaign 2024. *Journal "Ukrainian sense"*, 2(2), pp. 102-113. https://doi.org/10.15421/462428

Van Dijk, T. A. (2006). Discourse and Manipulation. *Discourse & Society*, 17(3), pp. 359-383. https://doi.org/10.1177/0957926506060250.

ANALYSIS OF APPROACHES AND TECHNOLOGIES FOR CONDUCTING COGNITIVE WARFARE IN MODERN CONDITIONS

Oleksandr Kin

Candidate of Technical Sciences, Senior Research Fellow, Associate Professor, e-mail: cubalibre1972@ukr.net,
ORCID ID: https://orcid.org/0009-0001-2196-7515

Hennadiy Udovenko Diplomatic Academy of Ukraine under the Ministry of Foreign Affairs, Kyiv, Ukraine

Received: November 24, 2025 | Revised: December 28, 2025 | Accepted: December 31, 2025

DOI: https://doi.org/10.33445/psssj.2025.6.4.4

Abstract

The article provides a military-political analysis of the cognitive dimension of modern hybrid warfare as a key element in the transformation of contemporary conflicts within the digital environment. The purpose of the study is to generalize approaches to the formation and implementation of the concept of cognitive warfare and to identify the main technologies and mechanisms of cognitive influence under current international confrontations. The methodological framework is based on doctrinal analysis, an interdisciplinary approach, comparative analysis of information and cognitive warfare concepts, and the examination of strategic documents and analytical materials of NATO and leading international institutions. The study demonstrates that cognitive warfare emerges at the intersection of military, informational, and psychological practices and is implemented through the deliberate construction of thinking patterns, causal relationships, and behavioral responses of individuals and social groups. Particular attention is paid to the influence of metamodern information reality, digital platforms, and artificial intelligence on the scale and intensity of cognitive operations. It is argued that the use of disinformation, manipulative narratives, and AI-driven technologies transforms the cognitive space into a distinct domain of confrontation aimed at undermining trust, political stability, and democratic processes. The article concludes that cognitive warfare has become a systemic factor of hybrid conflicts and requires further research, particularly regarding the disinformation aspects of artificial intelligence use.

Key words: Hybrid Warfare, Cognitive Warfare, Information Warfare, Cognitive Domain Operations.

Introduction

Contemporary armed conflicts increasingly extend beyond the boundaries of conventional warfare and acquire a multidimensional character, combining military, political, informational, and socio-psychological instruments of influence. Under these conditions, hybrid warfare has become the dominant form of modern conflict, in which decisive importance is attached not only to the physical destruction of the adversary but also to control over the perception, interpretation, and evaluation of reality by individuals and societies.

The rapid digitalization of the information environment, the expansion of social media, and the development of artificial intelligence and new media have significantly enhanced the capacity for targeted influence on mass consciousness. As a result, the cognitive dimension of confrontation is emerging as a critical element of modern conflicts, where the primary targets are thinking processes, belief formation, emotional responses, and behavioral patterns. Within this context, the concept of cognitive warfare has gradually taken shape and is increasingly reflected in academic discourse and military-strategic doctrines.

Despite the growing body of research on information and hybrid warfare, cognitive warfare as an independent and systemic dimension of confrontation remains insufficiently conceptualized.

Existing studies often conflate cognitive operations with information or psychological influence, which limits a comprehensive understanding of their nature, mechanisms, and strategic implications. At the same time, contemporary security practice—including the war in Ukraine and other international conflicts—demonstrates the expanding role of cognitive influence in achieving political and military objectives.

The purpose of this article is to provide a military-political analysis of the cognitive dimension of modern hybrid warfare by synthesizing theoretical approaches, doctrinal frameworks, and key technologies of cognitive influence. The study seeks to clarify the place of cognitive warfare within the structure of contemporary conflict and to substantiate its significance as a distinct domain that generates new challenges for international and national security systems.

Theoretical Background

The theoretical foundations of this study are situated at the intersection of hybrid warfare concepts, information warfare theory, and socio-philosophical analyses of mass consciousness. In contemporary security studies, cognitive warfare is increasingly viewed as an evolutionary stage of information warfare, where the object of influence extends beyond information flows to include perception, interpretation, and decision-making processes.

The conceptual origins of this approach can be traced to the works of **Marshall McLuhan**, who emphasized the decisive role of media in shaping mass consciousness and enemy images, framing information as a key weapon of future wars (McLuhan, 2014). These ideas laid the groundwork for subsequent studies that conceptualized the information environment as an independent domain of confrontation.

Further development of non-material dimensions of warfare is reflected in the works of **John Arquilla** and **David Ronfeldt**, who introduced the concepts of *noopolitik* and *noowar*, interpreting warfare as a struggle over meanings, knowledge, and narratives (Arquilla & Ronfeldt, 1999). Related perspectives are advanced by **Martin Libicki**, who systematized the forms and mechanisms of information warfare and highlighted its strategic nature (Libicki, 1995).

The contemporary stage of cognitive warfare theory is strongly influenced by doctrinal developments within NATO, particularly those advanced by Allied Command Transformation, where cognitive warfare is defined as coordinated activities synchronized with other instruments of power to influence attitudes and behavior (NATO Allied Command Transformation, 2023). Within this framework, the cognitive space is conceptualized as a distinct domain of confrontation alongside physical and digital domains.

Socio-philosophical interpretations of the changing information environment also play a significant role. **Alan Kirby** links the transition from postmodernism to metamodernism to changes in authorship and textual instability, directly affecting cognitive perception (Kirby, 2006). Similar ideas are developed by **Hanzi Freinacht**, who describes metamodern society as oscillating between truth and falsehood, creating favorable conditions for cognitive manipulation (Freinacht, 2017).

A separate strand of the literature focuses on digital phenomena such as post-truth, deepfakes, and cancel culture, analyzed as tools of cognitive influence in the context of social media and artificial intelligence (Oxford Dictionaries, 2016; Velasco, 2020; Thies et al., 2016). In this regard, reports by the **World Economic Forum** identify disinformation as a systemic risk to democratic processes (World Economic Forum, 2024).

Overall, the literature indicates a shift from information warfare toward cognitive confrontation as a systemic component of hybrid conflicts. However, existing studies remain fragmented, highlighting the need for an integrated theoretical framework.

Data and Methods

The study is theoretical and analytical in nature and is based on the analysis of open sources, strategic documents, conceptual materials, and academic publications addressing hybrid, information, and cognitive warfare. No empirical statistical data are employed, as the research objective focuses on the conceptual understanding of the cognitive dimension of modern conflicts.

The data set includes official NATO documents and analytical reports, particularly materials developed within the framework of Allied Command Transformation, NATO strategic concepts, as well as publications by leading international institutions and research centers. In addition, the study draws on academic works by domestic and international scholars in the fields of information security, strategic communications, postmodern and metamodern philosophy, and studies on disinformation, artificial intelligence, and digital media.

The methodological framework is based on an interdisciplinary approach combining military-political analysis, information security studies, and socio-philosophical concepts. The research applies doctrinal analysis to examine official approaches to cognitive warfare, comparative analysis to distinguish between information, cognitive, and hybrid warfare concepts, and logical-analytical methods to identify cause-and-effect relationships between transformations of the information environment and changes in contemporary forms of confrontation. The analysis of digital phenomena such as post-truth, deepfakes, cancel culture, and the metaverse is used to conceptualize mechanisms of cognitive influence within the metamodern information reality.

Results

The concept of cognitive warfare emerged at the intersection of military, information and psychological research. Its roots can be found in various military doctrines and strategic approaches to information and psychological warfare, but as a separate term it has become widely used in recent decades. One of the first official military documents that directly refers to cognitive warfare appeared in NATO, specifically within the framework of Allied Command Transformation (ACT), which actively researches new threats, in particular those related to information and cognitive influences (NATO ACT, 2023). Allied Command Transformation guides the concept of cognitive warfare research, which is part of a wider agenda for the development of military strategies (NATO Allied Command Transformation [NATO ACT], 2023). Understanding the conceptual framework, definitions, consequences and risks of such warfare, according to experts, contributes to better political decision-making, the development of military capabilities, and the overall security of the Alliance. The Allied Transformation Command conducts training, cooperation, protection and capability development for NATO in the field of cognitive warfare, providing recommendations on awareness raising, civil-military cooperation, societal resilience and information sharing to ensure the Alliance's current and future security.

Aimed at changing perceptions of reality, societal manipulation has become the new standard, and human cognition is becoming a critical area of warfare. The definition of cognitive warfare proposed in NATO's ACT research concept is as follows: "Activities conducted in synchronisation with other instruments of power to influence attitudes and behaviour through manipulation, protecting or violating the cognition of individuals and groups to gain an advantage over the enemy" (NATO ACT, 2023).

The relevance of this concept arises from the challenges NATO has faced in recent years and has introduced into the concept, namely (NATO ACT, 2023): technological progress and changes in information consumption provide opponents with greater opportunities to collect and manipulate data, influence emotions, and shape beliefs and behaviour. It makes possible to exploit the differences in society through the latest technologies, such as artificial intelligence, emerging and

disruptive technologies (EDTs), and data collection. In addition, the spread of social media contributes to influencing the thoughts, emotions, and actions of individuals.

As the authors of the concept note, it reflects the tactics of hybrid warfare, where society is used as a vector of influence on key targets – political and military leaders. The effectiveness of information campaigns depends on the targeted manipulation of emotions and cognitive biases, which causes large-scale changes in attitudes and behaviour. Such changes are often subtle and inconspicuous, blurring the line between genuine public discourse and hostile cognitive attacks that exploit social divisions.

Although cognitive attacks are not a new phenomenon, the concept defines them as deliberate offensive manoeuvres aimed at influencing perceptions, beliefs, interests, decisions, and behaviour through a direct attack on human consciousness. The innovative aspect of this approach is that enemies can now quickly and anonymously conduct cognitive attacks in the information environment using digital platforms and breakthrough AI technologies.

Cognitive warfare today fully reflects the system of principles of the meta-modern philosophical era, for which categories such as truth and reality are entirely relative. If postmodernism was marked by the growing influence of the media on the formation of new principles of individual perception of reality and a new type of inter-state communication, and television contributed to the cultivation of mass pop culture, then the beginning of the 21st century gave rise to a new phenomenon, namely the Internet, which transformed horizontal “subject-object” relationships, in the case of spiritual and informational exchange – “author–recipient”. For example, voting for participants in various TV shows is becoming an insufficient act of communication for people in the new information age, since its purpose is not only to be on the side of the object or subject of this communication, but to fulfill both roles at the same time. This radical change in the function of the producer is noted by A. Kirby: “The author now has the status of one of those who sets the parameters without which other operators become simply irrelevant, unknown, out of line. These changes also apply to the “text” itself, which is characterized by hyper-ephemerality and instability” (Kirby, 2006).

Currently, the Metamoderna.org project is gaining popularity in Europe – a collaboration between Swedish cultural theorists and sociologists Emil Friis and Daniel Gortz to create a virtual “philosopher, historian and sociologist Hanzi Freinacht, who “lives” alone in the Swiss Alps. Combining age psychology and cultural studies, Emil Friis and Daniel Gortz, on behalf of Hanzi Freinacht, have recently published a book entitled “The Listening Society”, in which they reveal the secrets of “memes of metamodern significance” (Freinacht, 2017). Modern people are surrounded by an overload of information, facts, events, knowledge, and things, and at this time, it is difficult and no longer necessary to strive for stability or a final system as the truth. The world of post-truth, fake news and information manipulation detracts from the sense of stability and understanding of the essence of reality.

Metamodernism gave rise to a new wave of informatisation of society with the establishment of the Internet, and later artificial intelligence, expanding access to these technologies to members of society with varying levels of wealth, as well as the formation of so-called new media in social networks (blogs, public pages, etc.). Internet communication has led to the transformation of interpersonal, interinstitutional and intergovernmental information exchange. At this time, thanks to the global online network, concepts are emerging and becoming established that are actively used in cognitive warfare:

“post-truth” – it emerged as a phenomenon of the postmodern era, but in the metamodern era it is being perfected and becoming a marker of the information age. According to the Oxford English Dictionary, post-truth is an information flow which is deliberately constructed in modern society with the help of the media to create a virtual reality that differs from the real one, with the

aim of manipulating public consciousness (Oxford Dictionaries, 2016). In 2016, this word was named word of the year by dictionary editors;

"cancel culture" – a modern form of ostracism, which Michigan State University professor Lisa Nakamura described as an attempt to control freedom of thought using the power given by social networks (Velasco J., 2020). This refers to the bullying of public figures in the information space for their present or past actions and deeds, in the context of the general right to self-expression and the expression of one's own position in the network. Thus, the presumption of innocence ceases to apply at the level of public discussion. Such online information campaigns are also sometimes referred to as "cancelling".

"deepfake" is a method of synthesising human images based on artificial intelligence. It is used to combine and superimpose images and videos onto original images or videos. Methods for detecting gestures and converting the original video into a video with a face similar to the target person were presented in 2016 and enable real-time calculation of fake facial expressions in 2D videos (Thies et al., 2016). Deepfakes can be used to create fake news, malicious deceptions, including the compromising of celebrities and public figures and the destruction of political reputations.

"metaverse" is a term that originated in science fiction novels in the 1990s. In the autumn of 2021, Mark Zuckerberg revived it by presenting a course of conceptual rebranding for the company Facebook, which will now work on creating a new cyber reality in which simulators become a tool for accurately reproducing reality in cyberspace. According to the concept, the metaverse is a permanent live virtual space in which people can interact with each other and with digital objects through their avatars, using virtual reality technologies.

Metamodern consciousness is in a state of constant oscillation (swinging). It is about radical openness, about universal acceptance. At this time, cognitive wars are reaching their peak, as the Internet, AI and social networks as the main marker of new informational and spiritual exchanges have led to the appearance of the meta-modern author and the meta-modern recipient, who often switch roles (this can be represented as a post with certain information on social networks, which other users reproduce on their pages, decorating it with numerous comments and accompanying texts). Human consciousness begins to constantly exist in a state of "meta" – "between" the usual reality and the network reality, which duplicates objective reality as much as possible; between truth and falsehood, trust and distrust.

Considering the rapid emergence of a new information reality based on cyber technologies, in particular AI, it can be assumed that humanity is in the process of forming a new type of metamodern society – an information networked society that is permanently in a state of cognitive and conscientious warfare. Manipulation of consciousness through information has gradually replaced violence, which for a long time was considered the only means of governance. That is why modern media of this type are becoming an effective tool for political propaganda, the spread of disinformation as a source of destabilising social processes, and also a direct information weapon used in hybrid warfare. During such cognitive warfare, modern cyber technologies, in particular artificial intelligence, are actively used.

Virtual space protection against cognitive attacks is a new stage in the development of information security, which is aimed specifically at the digital environment. In the late 1990s, experts from the RAND analytical centre of the US administration, J. Arquilla and D. Ronfeldt highlighted the problems of information strategy, cyber warfare, network warfare, and information warfare. In their opinion, the concepts of cyberspace and the information sphere should be combined as a combination of cyberspace and the mass media into a single "noosphere" – a new based on ideas, spiritual values, ethics, and an epistemological paradigm in which traditional politics of "brute" force with its emphasis on the material component of opposition is replaced by a new

one based on “soft power”. The modern “noowar” as a war of meanings and knowledge corresponds to a special term for the new politics – “noopolitik” (Arquilla & Ronfeldt, 1999). Such politics are implemented both in real and virtual space, using various platforms for their implementation, as well as various instruments.

Disinformation supported by foreign states may be aimed at creating confusion, exacerbate political polarisation, undermine democracy or create mistrust in societies. Although research shows that disinformation can influence beliefs, the degree to which it leads to behavioural change or has a real impact remains uncertain and difficult to measure. In January 2024, the World Economic Forum named disinformation as the greatest short-term risk in the world due to its potential to undermine democratic elections, causing social unrest and increasing censorship through initiatives to counter disinformation (World Economic Forum [WEF], 2024).

The digital space is becoming a specific platform for information terrorism, cognitive and conscientious attacks, simulated wars, Gibson’s wars. While the first category is the most common type of information aggression in the digital space, the second consists of preserving the functioning of the information system in its correct form, but with a certain distortion, a change in the information flow that changes the principle of information perception, and subsequently the ability to analyse it correctly, in intimidation with a certain type of weapon with the corresponding information accompaniment, which has special technical characteristics. Gibson’s wars exist more as a concept, which consists of waging war in virtual space using intelligence (including humans directly in the Internet network) (Libicki, 1995). Thus, artificial intelligence technologies are integrated into so-called noopolitik.

It should be noted that artificial intelligence in the field of cognitive warfare can significantly increase the scale of the threat of mass consciousness change. As it is known, one of the three pillars of a functioning democracy is representativeness. In order for elected representatives to respond effectively to the requests of their voters, they need to know exactly what they think. However, information warfare, controlled by AI, can manipulate social networks, creating confusion and spreading disinformation that distorts politicians’ perception of public opinion. Thus, if the populations of democratic countries are deceived into believing that, for example, Ukraine and Taiwan are not worth defending, the world will become critically vulnerable to aggressive tyranny.

Within the framework of the Munich Security Conference 2024, a document entitled “The Battle for the Mind: Understanding and Addressing Cognitive Warfare” (Centre for Governance and Change, 2024) was approved, which summarises the discussions that took place during a high-level Round Table on Cognitive Warfare organised by the Centre for Governance and Change (CGC) at IE University. The event was attended by Margrethe Vestager, Arancha González Laya, Anne Marie Slaughter and other well-known politicians and industry leaders. The document analyses the establishment of cognitive space as the sixth dimension of warfare – after land, sea, air, space and cyberspace – in the context of multi-domain theory.

Discussion

The findings of this study confirm that cognitive warfare has evolved into a systemic and autonomous dimension of modern hybrid warfare rather than remaining a subsidiary element of information or psychological operations. The analysis demonstrates that contemporary cognitive confrontation targets not merely information flows but the underlying mechanisms of perception, interpretation, and decision-making, thereby reshaping the strategic logic of conflict. This result supports theoretical assumptions that modern warfare increasingly prioritizes non-material forms of influence over traditional kinetic means.

The conceptualization of cognitive warfare presented in the article aligns with and extends NATO’s doctrinal approach, particularly the framework developed by Allied Command

Transformation, which defines cognition as a critical domain of competition. However, the discussion highlights that cognitive warfare should not be understood solely as an extension of information warfare. Instead, it represents a qualitative shift toward influencing causal reasoning, emotional responses, and behavioral patterns at both individual and societal levels. This distinction clarifies one of the central research questions by demonstrating that cognitive warfare operates on a deeper level than information dissemination or persuasion.

The results also resonate with earlier theoretical contributions that frame warfare as a struggle over meanings and narratives rather than material resources. The concepts of *noopolitik* and *noowar* are particularly relevant in interpreting the findings, as they provide an analytical lens for understanding cognitive space as a battlefield where values, identities, and interpretations of reality are contested. In this regard, the study confirms that contemporary hybrid conflicts increasingly rely on the manipulation of symbolic and cognitive resources to achieve strategic objectives.

A significant contribution of the discussion is the integration of socio-philosophical perspectives on metamodernism into the analysis of cognitive warfare. The findings suggest that the metamodern information environment—characterized by oscillation between truth and falsehood—creates structural vulnerabilities that can be systematically exploited through cognitive operations. Phenomena such as post-truth narratives, deepfakes, and cancel culture are not isolated media effects but components of a broader cognitive ecosystem shaped by digital platforms and artificial intelligence. This interpretation deepens the understanding of how technological and cultural transformations amplify the effectiveness of cognitive influence.

The discussion further underscores the growing role of artificial intelligence as a force multiplier in cognitive warfare. AI-driven tools enable the rapid personalization, scaling, and automation of manipulative narratives, thereby increasing both the reach and subtlety of cognitive attacks. At the same time, the study acknowledges the limitations identified in the literature regarding the measurement of the actual behavioral impact of disinformation. While cognitive influence can shape beliefs and perceptions, its translation into concrete political or military outcomes remains difficult to quantify, which represents an important methodological challenge for future research.

From a military-political perspective, the findings imply that cognitive warfare poses a direct challenge to democratic systems, where openness, pluralism, and freedom of expression can be exploited as vectors of influence. The discussion highlights that the erosion of trust in institutions, combined with the attention economy and societal polarization, increases the susceptibility of liberal democracies to cognitive manipulation. This observation is consistent with recent assessments by international organizations that identify disinformation as a systemic security risk.

Despite its contributions, the study has several limitations. First, its theoretical and doctrinal focus precludes empirical testing of specific cognitive operations or case-based measurement of their effectiveness. Second, the reliance on open-source documents and analytical reports limits the ability to assess classified or covert dimensions of cognitive warfare. These limitations suggest that future research should incorporate empirical case studies, experimental designs, or comparative analyses across different conflict contexts.

Overall, the discussion reinforces the central argument that cognitive warfare has become a defining feature of modern hybrid conflicts. By conceptualizing the cognitive domain as a distinct space of confrontation, the study contributes to a more nuanced understanding of contemporary warfare and highlights the need for integrated policy responses that combine military, informational, technological, and societal resilience measures.

Conclusions

Today, both government and non-government actors have the tools and stimuli to manipulate our thoughts and destroy our common understanding of reality – from interfering with specific military manoeuvres to destabilising societies and multilateral cooperation. Contemporary society has entered a hyperrealistic dream in which everything is true and false at the same time, and those who generate meaning and information themselves fall into its trap, becoming consumers rather than producers. The increased use of artificial intelligence in all areas of activity not only has a constructive impact on the development of high technologies and improves the possibilities for ensuring individual and national security, but also becomes an instrument of destabilisation processes, both within the microcosm of an individual, influencing the processes of information processing, but also in the geopolitical macrocosm, even transforming the understanding of the established world order.

The growth in the use of deceptive narratives and manipulative AI in democratic processes, the war in Ukraine and the conflict between Israel and Hamas demonstrate a growing geopolitical interest in controlling people's perception. Citizens of liberal democracies are particularly vulnerable to cognitive manipulation, as the economy of attention negatively affects our ability to think critically, trust in institutions is at an all-time low, and the polarisation of society has reached its peak.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

Arquilla, J., & Ronfeldt, D. (1999). *The emergence of noopolitik: Toward an American information strategy*. RAND Corporation.

Centre for Governance and Change. (2024). *The battle for the mind: Understanding and addressing cognitive warfare and its emerging technologies*. IE University. https://static.ie.edu/CGC/CGC_TheBattleofTheMind_2024.pdf

Freinacht, H. (2017). *The listening society: A metamodern guide to politics*. Metamoderna.

Kirby, A. (2006). The death of postmodernism and beyond. *Philosophy Now*, (58), 34–37. https://philosophynow.org/issues/58/The_Death_of_Postmodernism_And_Beyond

Libicki, M. C. (1995). *What is information warfare?* National Defense University Press.

McLuhan, M. (2014). *Media research: Technology, art and communication*. Taylor & Francis.

NATO Allied Command Transformation. (2023). *Cognitive warfare exploratory concept*. NATO ACT.

Oxford Dictionaries. (2016). *Post-truth*. https://www.lexico.com/en/definition/post-truth

Thies, J., Zollhöfer, M., Stamminger, M., Theobalt, C., & Niessner, M. (2016). Face2Face: Real-time face capture and reenactment of RGB videos. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2387–2395. http://www.niessnerlab.org/papers/2016/1facetoface/thies2016face.pdf

Velasco, J. (2020). You are cancelled: Virtual collective consciousness and the rise of cancel culture. *Rupkatha Journal on Interdisciplinary Studies in Humanities*, 12(5). https://rupkatha.com/V12/n5/rioc1s21n2.pdf

World Economic Forum. (2024). *Global risks report 2024*. https://www.weforum.org/publications/global-risks-report-2024

THE ROLE OF CENTRAL ASIA IN MODERN GEOPOLITICS

Serhii Strilchuk [1 A]; Oleh Matsovityi [2 B]; Volodymyr Taranov [3 C]

[1] Head of Department, e-mail: strilchuk7sv@gmail.com, ORCID: https://orcid.org/0009-0006-9067-7956
[2] PhD candidate, expert, e-mail: cenzor50@proton.me, ORCID: https://orcid.org/0009-0004-2973-1584
[3] Assistant Profesor, e-mail: chik2467@gmail.com, ORCID: https://orcid.org/0000-0001-7522-3928

[A] Military Academy, Kyiv, Ukraine
[B] National Aviation University, Kyiv, Ukraine
[C] Diplomatic Academy named after Hennadii Udovenko, Kyiv, Ukraine

Received: December 14, 2025 | Revised: December 28, 2025 | Accepted: December 31, 2025

DOI: https://doi.org/10.33445/psssj.2025.6.4.4

Abstract

The relevance of this article is primarily determined by the rapidly growing significance of Central Asia (CA) in contemporary international relations, serving as a crossroads of interests for the world's major actors — Russia, the USA, China, the EU, Turkey, etc. — and, simultaneously, as a field of interaction, mutual penetration, and clash of values among the world's major civilizations and political systems. Central Asia is not only a key region on the world map, the control of which allows for the management of global hydrocarbon transit and other strategic raw materials for the largest economies (primarily China) and, consequently, influences their economic growth, overall power, and directions of expansion. Central Asia is a crossroads of civilizations, control over which, as believed for centuries, enables dominance over the world. This exceptional geopolitical significance of the region remains relevant today.

Firstly, the importance of the Central Asian and Caspian region as one of the most rapidly developing areas for global hydrocarbon extraction and transportation is increasing sharply. Secondly, the Central Asian region is already increasingly becoming a potential arena for clashes of interests among global players.

Overall, despite a certain degree of existing research on issues related in one way or another to the role and position of Central Asia in the system of international relations, the conceptual, institutional, and technological aspects of the transformation of international relations in the region remain underexplored in both domestic and foreign political science. On one hand, there is a solid methodological foundation and a substantial body of empirical material for studying the position of Central Asia in the international system. On the other hand, many important questions in this area still require theoretical reflection. Furthermore, the formation of positions on specific aspects or issues of the study is directly influenced by the current state and ongoing development of the situation around the region and its main actors.

The object of this study is the Central Asian region, which today serves as a center where the geopolitical, military-strategic, and economic interests of major powers — Russia, USA, EU, China, and Turkey — intersect.

The subject of the study is the political configuration of international relations in Central Asia, arising from the competition among the leading world powers — Russia, USA, EU, China, and Turkey — for political influence in the region and control over its strategic resources, as well as the foreign policy and relations of the Central Asian states with these actors.

Accordingly, based on the object and subject of the study, the aim of this article is to determine the role and position of the Central Asian region in the system of contemporary international relations in the context of the active pursuit of national interests by the leading global powers in the region.

Key words: Central Asia, Geostrategic Region, Geopolitics, International Security, China, Russia, USA, EU, Turkey, Post-Soviet Space.

Introduction

The Central Asian region occupies a distinctive place in the architecture of contemporary international relations and geopolitics (Van den Bosch et al., 2021). Although relatively small in size, the region is rich in energy resources and is therefore crucial to the geopolitical future and stability of the Asian continent (Khan & Koch, 2023; Central Asia's Growing Partnership with China, n.d.). The transformation of the Central Asian states—Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan—into full-fledged members of the international community has constituted a positive factor in strengthening their national statehood.

At the present stage, particular attention has been drawn to issues related to collective security systems and regional integration in Central Asia, including the participation of regional states in regional organizations and the determination of key vectors for the development of interaction with major global actors within the geopolitical space (Competition of World Powers in Central Asia, 2019; Wilson Center, 2025).

Theoretical Background

Scholarly attention to the transformation of Central Asian states, their involvement in global and regional processes, accession to international organizations, and the prospects for future cooperation has been evident among academics, analysts, and experts from various countries, regardless of their direct affiliation with the region (Van den Bosch et al., 2021; Hiro, 2009). Contemporary scholars and analysts place particular emphasis on the geopolitical influences shaping the transformation of Central Asian states. A substantial body of research is devoted to the study of security and regional policies in Central Asia, as well as to specific aspects of regional integration (Uslu, 2018; Omelicheva, n.d.). Security-related and economic dimensions of regional integration have been partially addressed in the works of Western researchers. However, there remains a clear need for a comprehensive study of the impact of external factors and decisions on Central Asian countries, their determining role at the regional and geopolitical levels, and the dynamics of their regional integration across various spheres (Khan & Koch, 2023).

This article aims to analyze the challenges and prospects of interaction between the Central Asian states and leading global powers. It seeks to examine the state of geopolitical competition in Central Asia, trace the transformation of the foreign policy strategies of key international actors — China, Russia, the United States, the European Union, and Turkey — in the region, and present possible scenarios for the development of geopolitical dynamics surrounding Central Asia.

Data and Methods

This study is based on a qualitative analytical approach and has a conceptual and review-oriented character. Its empirical foundation consists of secondary sources, which makes it possible to comprehensively analyze the role of Central Asia in the contemporary system of international relations without employing quantitative modeling.

The information base of the study includes: (1) scholarly publications and monographs on geopolitics, international security, and regional studies of Central Asia; (2) analytical reports and policy papers produced by leading international research centers and think tanks; (3) official strategic and program documents of key external actors—China, the Russian Federation, the United States, the European Union, and Turkey—as well as materials related to multilateral formats of regional cooperation; and (4) open-source statistical and factual data used to contextualize selected arguments.

The methodological framework is grounded in systemic and comparative analysis, which are applied to examine Central Asia as an integrated geostrategic region and to compare the strategies and instruments of influence of major external actors. In addition, content analysis of strategic documents and official narratives is used to identify changes in approaches to the region under

conditions of transformation of the global security environment. To formulate assessments of regional development prospects, an analytical scenario-based approach is employed, drawing on the generalization of existing trends.

The selected methods provide an adequate basis for capturing the complexity and dynamism of geopolitical processes in Central Asia. At the same time, a limitation of the study lies in the absence of empirical testing of causal relationships using quantitative tools.

Results

Recent geopolitical developments indicate that the world is currently experiencing a process of global regionalization across political, economic, and social spheres. Geostrategic regions are acquiring global significance in political, economic, resource-related, and security terms.

In this regard, Central Asia constitutes an important geostrategic factor in international relations. Accordingly, it is becoming increasingly evident that Central Asia is forming its own agenda and steadily asserting itself as a consolidated, active, and forward-looking region (Van den Bosch et al., 2021). In the near term, the region's strategy is likely to rest on two interrelated pillars: the expansion of constructive external relations and the qualitative deepening of integration processes among the countries of the region.

The countries of Central Asia do not engage in geopolitical balancing for its own sake. Each state acts as an independent actor, clearly articulating, safeguarding, and pursuing its national interests. Their multi-vector foreign policy (Multi-Vectoral Approach as the Key Model of Central Asian Countries' Foreign Policy, 2023) is driven by pragmatic objectives, including the strengthening of sovereignty, the promotion of sustainable economic development, and the prevention of regional spillover effects from confrontations among major powers. In this context, the selection of external partners is determined not by ideological considerations, but by demonstrated readiness for mutual respect and long-term cooperation.

Against the backdrop of escalating geopolitical tensions and global economic disruptions, Central Asia has become increasingly engaged in diplomatic and external economic activities, more frequently presenting a coordinated position, particularly in international fora. The "Central Asia +" format occupies a distinct place, reflecting both heightened international interest in the region and the willingness of external actors to pursue mutually beneficial cooperation (Wilson Center, 2025). In line with traditions of consensus-oriented governance, the five Central Asian states approach dialogue in a gradual and measured manner, seeking to build partnerships based on equality.

Traditionally regarded as a peripheral region, Central Asia is now confronted with an increasingly complex geopolitical environment. Russia's invasion of Ukraine has reshaped the region's international agenda, revealing new risks as well as opportunities. At the same time, rising tensions between the West and China add further complexity to Central Asia's relations with its principal external partners.

The central issue addressed in this article concerns the extent to which changes in the geopolitical landscape influence Central Asia's international engagement and the sustainability of its growing role. Amid intensified military and economic rivalries among major powers, Central Asia appears to be attracting increasing international attention. These developments coincide with a rise in regional cooperation, indicating the potential emergence of a new phase in the region's international relations.

The article contends that, while the current geopolitical context creates favorable conditions for enhancing Central Asia's international role, expectations should remain measured. The primary drivers of geopolitical change lie outside the region and are therefore largely dependent on the policies of external powers. Furthermore, although regional cooperation in Central Asia appears more promising than in previous periods, it has not yet produced substantial outcomes. The article

first outlines the evolving geopolitical context, then examines the region's efforts to advance regional cooperation, and finally assesses existing cooperation frameworks, offering conclusions and forward-looking assessments regarding the region's development prospects in the near term.

Features of the Geopolitical Development of the Central Asian Region

For much of the post-Soviet period, Central Asia remained on the periphery of global international affairs. During the 1990s, the region was largely perceived as Russia's "backyard". By the late 1990s, as tensions between Russia and the West gradually surfaced, analysts increasingly viewed Central Asia as a theater of broader geopolitical confrontation or as part of the so-called "Great Game", reflecting the prevailing perception that the region lacked significant independent international agency.

However, a number of developments in recent years have reshaped international relations and altered Central Asia's position within global geopolitics. Russia's annexation of Crimea in 2014, followed by its full-scale invasion of Ukraine in 2022, sent shockwaves across the post-Soviet space, with particularly profound implications for Central Asia. Sharing long land borders with Russia, Central Asian states interpreted Russia's actions in Ukraine as a disregard for international law and the principle of state sovereignty. In other words, the region was confronted with the possibility that post-1991 borders could be challenged. In this context, the broad international condemnation of Russia's aggression and the subsequent imposition of Western sanctions constituted both a challenge and an opportunity for Central Asia. Given its political and economic ties with Russia—and, above all, its geographic proximity—Central Asia has little choice but to carefully balance the maintenance of cooperative relations with Russia while simultaneously keeping a prudent distance from it.

Against this background, the analysis below examines the role, position, and prospects of the Central Asian states and the region as a whole through the prism of their interaction with key international actors operating in the region, namely China, Russia, the United States, the European Union, and Turkey.

Historically, the **Russian Federation** has played a dominant role in Central Asia—first as a metropolitan power during the Tsarist and Soviet periods, and after 1991 as a key post-imperial actor. Its role has been shaped across three principal dimensions (Omelicheva, n.d.; Uslu, 2018; Hiro, 2009).

First, the political and security dimension, in which Russia positions itself as a guarantor of regional security. This role is manifested through the Collective Security Treaty Organization (CSTO) as a mechanism of military-political integration, the presence of Russian military bases in Tajikistan and Kyrgyzstan, and coordination in combating terrorism, extremism, and drug trafficking. Nevertheless, developments in recent years—including instability in Afghanistan, Russia's war against Ukraine, and the CSTO's limited response to regional crises—have undermined confidence in Russia as an unconditional security provider.

Second, the economic dimension. Russia remains an important economic partner, serving as a key labor market for migrant workers from Uzbekistan, Tajikistan, and Kyrgyzstan, as well as a significant actor in energy cooperation, including oil, gas, and nuclear energy. The Eurasian Economic Union (EAEU) also functions as an instrument of Russian economic influence. At the same time, Russia's economic role is increasingly characterized by asymmetry and stagnation, particularly when compared to the scale and dynamism of Chinese investment and infrastructure projects in the region.

Third, the cultural and humanitarian dimension. The Russian language, education system, media, and shared historical memory continue to constitute important elements of Russia's soft power in Central Asia. However, gradual processes of de-Russification are underway, accompanied by the strengthening of national languages and identities. Younger generations are increasingly less inclined to view Russia as a central civilizational reference point.

At the same time, within the current regional configuration, the Russian Federation is no longer the uncontested leader of Central Asia, but rather one of several competing external actors.

A multi-vector model of foreign relations is taking shape in Central Asia, within which China dominates in the economic and infrastructure domains; Turkey is expanding its cultural-ideological and military-technical influence; the United States and the European Union operate primarily through a "soft presence," focusing on education, energy transition, and governance; and Russia increasingly acts as an actor of inertial influence, relying on legacies of the past.

In turn, Russia's war against Ukraine has significantly constrained Moscow's capabilities in the region. This has resulted in the reorientation of Central Asian resources away from Russia toward Western and southern strategic directions, a decline in Russia's financial and investment attractiveness, and growing caution among Central Asian elites regarding excessive dependence on Moscow. Consequently, Russia's position is evolving from that of a regional center of gravity to that of one partner among others, with a clear tendency toward relative weakening.

Prospects of the Russian Federation in Central Asia

Short-term perspective (1–3 years): preservation of a security presence in the region; retention of leverage through migration and energy instruments; and adaptation to the role of China's "junior partner" in Central Asia.

Medium-term perspective (3–7 years): further erosion of Russia's monopoly on regional influence; institutional weakening of the Eurasian Economic Union (EAEU) and the Collective Security Treaty Organization (CSTO); and growing foreign policy autonomy of Central Asian states.

Long-term perspective: Russia's future in Central Asia will largely depend on the outcomes and consequences of its war against Ukraine, its ability to offer a new, non-hierarchical model of partnership, and the level of Russia's own internal socio-economic stability.

Under an inertia-based scenario, Russia risks becoming a secondary regional actor, retaining only selective instruments of influence without a strategic dominant position.

As a result, the Russian Federation is losing its status as an uncontested leader in Central Asia, while maintaining significant but limited influence in the areas of security and migration, yielding economic primacy to China and cultural-ideological influence to Turkey.

Russia's prospects in the region will be determined less by its historical legacy than by its capacity to adapt to a new multipolar reality in which Central Asia increasingly acts not as an object, but as a subject of international politics.

China's Role and Prospects in Central Asia

By contrast, China views Central Asia as a geopolitical and geo-economic priority for several key reasons. These include resources, as the region possesses substantial reserves of energy resources and minerals vital to Chinese industry, serving as a source of oil, gas, and critical raw materials; transit and logistics, given the region's location along routes to Europe and the Middle East and its role in providing key transport and trade corridors; security considerations, as stability in Central Asia directly affects security in neighboring Xinjiang (Xinjiang Uyghur Autonomous Region) and China's efforts to counter extremism; and competitive dynamics, since the region was traditionally regarded as part of Russia's sphere of influence, while China is now expanding its economic and political presence, particularly amid the weakening of Moscow's position following the war against Ukraine (Central Asia's Growing Partnership with China, n.d.; Khan & Koch, 2023).

Accordingly, Central Asia is important not only for China's bilateral relations with regional states, but also for the implementation of its global strategies, particularly the Belt and Road Initiative (BRI), which aims to transform the region into a key hub of transit and economic integration.

An analysis of China's economic influence in Central Asia highlights several core characteristics. First, trade and investment ties: China has become the leading trading partner for most Central Asian countries, significantly surpassing the region's traditional economic leader,

Russia. According to estimates by Chinese diplomatic sources, trade turnover between China and the five Central Asian states exceeded USD 106 billion in 2025 and continues to grow. Second, investment and infrastructure development: a substantial share of Chinese investment is directed toward energy, transport, logistics, and the digital sector. China has emerged as a key financier and builder of infrastructure projects, including transport corridors and railways. For example, the China–Kyrgyzstan–Uzbekistan railway corridor is expected to significantly reduce freight transit times between China and Uzbekistan and to become an important component of transcontinental logistics networks. Additional projects further reinforce this trend.

While these investments contribute to economic growth in Central Asian states, they simultaneously generate economic dependence on Chinese capital and markets.

To ensure the effective realization of its objectives, China has systematically and strategically developed new cooperation formats, including the “Central Asia–China” summit mechanism and strategic partnership agreements aimed at strengthening political integration. In June 2025, a treaty on “permanent good-neighborliness and friendly cooperation” was signed with all five Central Asian states, formally consolidating closer political and economic ties.

China’s strategic expansion of influence in Central Asia is taking place against the backdrop of Russia’s declining traditional position, thereby creating space for Beijing to emerge as the region’s primary external actor.

At the same time, the United States and the European Union have sought to intensify their engagement in the region—for instance, through high-level political visits by Central Asian leaders to Washington—though this has thus far resulted primarily in a statistical rather than structural competition of external influences.

Nevertheless, the growing role of China in Central Asia also generates challenges and risks for the region. Economic cooperation with China is often tied to large-scale infrastructure projects and the export of raw materials, which may constrain technological development and economic diversification in Central Asian economies, leading to a structural diversification deficit.

On the one hand, Chinese investment stimulates development; on the other, it may create structural economic dependence, reducing the capacity of recipient countries to pursue independent foreign policy decisions. This constitutes a significant challenge for Central Asian states seeking to realize their own potential and pursue development paths they consider most appropriate and effective.

In light of the above, several likely prospects for China–Central Asia interaction for the period 2026–2035 can be identified. China is expected to continue expanding trade, investment, and transport corridors, with the integration of the region into global supply and logistics chains remaining a central priority. Beijing will also actively promote strategic partnership agreements and develop new cooperation mechanisms, which may eventually evolve into regional consortia involving other major powers. At the same time, the United States, the European Union, and regional actors such as Turkey or India may contribute to balancing China’s influence, fostering a multipolar architecture of cooperation.

In sum, China’s role in Central Asia has become a central driver of regional dynamics in the twenty-first century. It is expanding its economic capabilities through trade and investment, strengthening political ties and regional formats, and acting as a key player in great-power competition.

At the same time, China’s presence is associated with risks related to sovereignty, economic diversification, and the balancing of political influence. For this reason, Central Asian states are increasingly pursuing a strategy of balancing among major external partners.

For a general overview of China’s key instruments of influence in Central Asia, Table 1 presents a consolidated summary.

Table 1. Key of China's influence in Central Asia

Group of instruments	Main implementation mechanisms	Strategic goal	Implications for Central Asian countries
Economical	Trade expansion; foreign direct investment; lending through Chinese state-owned banks; settlements in yuan	Establishing a long-term economic presence; building interdependence	Economic growth; increasing dependence on the Chinese market and capital; decreasing role of traditional partners
Infrastructure (BRI)	Construction of railways and highways; oil and gas pipelines; logistics and customs hubs; digital infrastructure	Control of transit routes; integration of the region into Eurasian supply chains	Development of transport infrastructure; strengthening the transit role of the region; long-term linkage to Chinese logistics networks
Political and diplomatic	China-Central Asia format; bilateral strategic partnership agreements; principle of non-interference; elite diplomacy	Institutionalization of political influence; formation of elite loyalty	Deepening political coordination with China; limiting space for alternative geopolitical orientations
Security	Shanghai Cooperation Organization; anti-terrorism cooperation; intelligence sharing; border security	Ensuring regional stability; protecting China's western borders (Xi'an Autonomous Region)	Reducing security risks; increasing dependence on Chinese security mechanisms without a direct military presence
Social and humanitarian ("soft power")	Educational programs and grants; Confucius Institutes; cultural exchanges; information presence	Forming a positive image of the PRC; long-term impact on public sentiment	Spreading Chinese cultural and educational standards; gradually strengthening humanitarian influence
Strategically balancing	Avoiding open confrontation with the Russian Federation and the West; economic, not ideological, expansion; multi-vector approach	Consolidating the status of an "indispensable partner" in the region	Maintaining a strategic balance between external players; increasing the maneuverability of regional elites

Source: compiled by the author.

The Role of the United States in Central Asia

The United States made a significant contribution to the establishment of independence of the Central Asian states. At the same time, the core priorities of U.S. foreign policy in the region included ensuring free access to energy resources; promoting western (the construction of pipelines from Central Asia to Europe bypassing Russia) and southern (Turkmenistan–Pakistan–Afghanistan–India) strategic routes for the supply of energy resources; preventing the restoration of Russian influence and containing the expansion of the People's Republic of China; countering the spread of Islamic radicalism, among other objectives (Cannon, 2025; Wilson Center, 2025).

The U.S. presence in the region increased markedly following the launch of the U.S.-led counterterrorism operation in Afghanistan. From 2001 to 2014, the United States leased military bases in Uzbekistan and Kyrgyzstan and reached agreements on military cooperation with other countries of the region. The decisive consent of Central Asian governments to provide their military facilities to the international military contingent led by the United States was driven by their awareness of the real security threats emanating from Afghan territory.

However, already in 2004–2005, relations between Kyrgyzstan and Uzbekistan, on the one hand, and the United States, on the other, became strained. This was due to the "Tulip Revolution" in Kyrgyzstan and the mass protests in the Uzbek city of Andijan. After the United States called for an independent investigation into the shooting of protesters in Andijan, the July 2005 Shanghai Cooperation Organisation (SCO) summit adopted a declaration on the advisability of the continued presence of the U.S. military contingent in Central Asia. This decision provoked outrage in the U.S. House of Representatives and was perceived as an "attempt by Russia and China to push the United States out of the region".

In July 2005, the United States redeployed its troops from Uzbekistan to Kyrgyzstan, and in 2014 it was forced to withdraw its forces from Kyrgyzstan as well. It should be noted that both Russia and China were concerned about the U.S. presence in the region and therefore welcomed the closure of the air bases. At the same time, the U.S. withdrawal from its base in Kyrgyzstan in 2014 marked a reduction in the presence of Western security forces in Central Asia.

As noted by T. Umarov, an expert at the Carnegie Center, relations between the United States and Central Asia are currently experiencing a difficult period, as the countries of the region no longer view Washington as a counterbalance to Moscow and Beijing. Nevertheless, neither the closure of U.S. air bases in Central Asia nor even the withdrawal of U.S. military forces from Afghanistan in August 2021 signifies a loss of the region's geostrategic importance for the United States. In the case of the United States, the geostrategic factor extends to both geopolitical and economic dimensions.

Central Asia remains under the strong influence of China and Russia, while the U.S. government continues to pursue long-standing plans to implement the Trans-Caspian gas project, which would reduce Europe's dependence on Russian gas. As early as 2015—just two years after the launch of China's Belt and Road Initiative—the United States introduced a new format of cooperation with Central Asia, the "C5+1" (Central Asia + the United States). Kazakhstan serves as the principal U.S. foothold in the region. The share of U.S. companies in oil production in Kazakhstan amounts to approximately 30%, whereas Chinese oil companies (CNPC, Sinopec, and CITIC) account for 17%, and Russia's Lukoil only 3%. Chevron and ExxonMobil jointly own 75 % of shares in Tengizchevroil, Kazakhstan's largest oil-producing enterprise. These companies also hold stakes in smaller projects. U.S. companies such as Fluor, Schlumberger, and Baker Hughes provide nearly the full range of services related to oil extraction and processing.

A number of companies supply Kazakhstan with high-tech equipment for oil extraction, accounting for roughly one third of U.S. exports to the country. In addition to the oil and gas sector, hundreds of U.S. companies operate in Kazakhstan, including General Electric, Citibank, Uber, Starbucks, McDonald's, and others. As of early 2021, the total volume of accumulated U.S. investments in Kazakhstan amounted to USD 40 billion. Nevertheless, trade turnover between the United States and Kazakhstan (USD 2 billion in 2020) remains significantly lower than that between Kazakhstan and China (USD 21.4 billion) and between Kazakhstan and Russia (USD 19 billion).

The arrival of President Donald Trump at the White House had a substantial impact on U.S. foreign policy toward Central Asia. The 2025 U.S. National Security Strategy identifies countering China and Russia as key rivals that "challenge American power, influence, and interests" as an imperative of U.S. foreign policy. China and Russia are classified as "revisionist states" seeking to

shape a world contrary to U.S. values and interests and to project their influence globally, including across Europe and Central Asia.

It is within this context that the "United States Strategy for Central Asia 2025" should be viewed. The Strategy contains clear messages regarding the U.S. understanding of its national interests in the region. Its guiding principle is the recognition of Central Asia as a "geostrategic region important to the national security interests of the United States, regardless of the level of U.S. engagement in Afghanistan". The stated objectives of the Strategy include strengthening the resilience of Central Asian states to threats to their stability, enhancing their independence from "malign actors" (implicitly referring to China and Russia), and developing partnerships with the United States. The expansion of close relations and cooperation with all five Central Asian states is viewed by Washington as a means of "promoting American values" and counterbalancing the influence of neighboring regional powers.

An important component of Washington's strategic vision for the future development of energy projects in the region is the integration of Central Asian countries with South Asia, or the creation of the so-called "Greater Central Asia", a concept that has traditionally provoked dissatisfaction in Moscow. This approach explains the development of Central Asia's links with Europe via the Caucasus, as well as with Afghanistan and South Asia. The essence of this project lies in limiting the influence of other regional actors by redirecting all projects involving Central Asia southward, without Russia's participation.

Overall, against the backdrop of Russia's invasion of Ukraine, the United States possesses significant potential to reduce Moscow's influence in Central Asia.

The Role of the European Union in Central Asia

Another major actor in the geopolitics of the Central Asian region is the European Union. Central Asia holds significant geopolitical and geo-economic importance for the EU, as it is located between Europe and Asia, offers transit opportunities for transport corridors and trade, possesses substantial natural resources—including oil, gas, uranium, rare earths, and other critical materials—and has a young population with considerable economic growth potential. These factors render the region a strategic arena for the EU's external policy, particularly in the context of changes in the global security architecture following Russia's full-scale invasion of Ukraine and the intensification of competition among major powers (Van den Bosch et al., 2021).

The European Union has not developed stable institutional frameworks for cooperation with Central Asia comparable to the CSTO, the EAEU, the SCO, the BRI, or the C5+1 format. Nevertheless, the EU has maintained a consistent interest in the region's energy resources since the 1990s, which has influenced the orientation of transport corridors across post-Soviet Eurasia.

The EU has pursued its objectives and priorities through its Strategy for Central Asia, initially adopted in 2007 and updated in 2019. The main goals of this strategy include enhancing resilience, promoting economic development, and fostering regional cooperation. Within this framework, the EU has implemented updated approaches to cooperation through Enhanced Partnership and Cooperation Agreements (EPCAs) with all countries of the region, expanding political, trade, and institutional collaboration.

The EU is one of the largest investors and donors in Central Asia, having invested more than €100 billion over the past decade and allocated over €550 million through regional programs for the 2021–2027 period. European projects encompass transport corridors—particularly the Trans-Caspian route (Middle Corridor)—the development of digital infrastructure, as well as energy and climate initiatives. In 2025, the first EU–Central Asia Summit took place, during which an investment package of €10–12 billion was presented, targeting transport, critical raw materials, energy, and digital services.

Alongside the implementation of economic initiatives, the EU seeks to play a significant role in shaping the regional balance of power in Central Asia, which has increasingly become a zone of interaction among major global actors. As a counterweight to China's Belt and Road Initiative, which maintains a strong presence in the region through infrastructure development and transport connectivity, the EU promotes an alternative via its Global Gateway strategy—its framework for sustainable global investments, including in Central Asia. In contrast to Russia, which remains a key security actor and partner in the region, the EU aims to advance energy and logistical diversification away from Russian routes, particularly with regard to the supply of energy resources and critical materials.

Thus, for the European Union, Central Asia represents not only an economic space but also a field of strategic balancing among global influences. However, despite active cooperation in economic and infrastructure development, the CIS legacy and authoritarian tendencies in the region pose challenges to the promotion of the EU's value-based priorities, such as democracy and human rights. This has generated criticism regarding the inconsistency between economic engagement and the EU's normative principles.

In conclusion, the European Union plays an important, expanding, and multifaceted role in Central Asia. It is one of the region's leading economic partners and donors, promoting its economic interests while supporting the development of transport corridors, digitalization, green transformation, and energy diversification. Political cooperation is also expanding, albeit not without challenges arising from the complex domestic situations in Central Asian states and the influence of other major powers. In the long term, the EU's role in the region is likely to grow, provided it succeeds in balancing its economic ambitions with the advancement of the value-based components of its external policy.

Turkey's Role in Central Asia

Turkey is a historical ally of four Turkic-speaking Central Asian states—Kazakhstan, Kyrgyzstan, Turkmenistan, and Uzbekistan. Following their independence, Ankara arguably emerged as one of the most desirable partners for these countries, not only due to shared cultural and linguistic proximity, but also because of Turkey's role in international politics as a NATO member with strong ties to the West. Turkey significantly intensified its engagement in Central Asia following the rise to power of Recep Tayyip Erdoğan (Ersen & Kösem, 2021; Great and Small Games in Central Asia and the South Caucasus, 2022).

Cooperation among Turkic-speaking states reached a new level with the establishment of the Cooperation Council of Turkic-Speaking States (Turkic Council) in 2009. Azerbaijan's victory in the Nagorno-Karabakh conflict contributed to the spread of pan-Turkic ideas, the concept of a "Greater Turan", and the consolidation of the Turkic world as an alternative—and competitor—to the concept of the "Russian World", another neo-imperial doctrine aimed at uniting Slavic peoples and post-Soviet states under Moscow's leadership. These developments, together with the withdrawal of U.S. troops from Afghanistan, endowed the Turkic Council with particular strategic significance and enhanced its military-political relevance. Accordingly, at the Eighth Summit of the Turkic Council held in Istanbul in November 2021, the organization was reorganized into the Organization of Turkic States (OTS).

One of the declared objectives of the OTS is the "promotion of the values and interests of the Turkic world at the regional and international levels". According to the vision articulated by the leaders of the Turkic states, the establishment of a common market for goods, investment, labor, and services is planned by 2030. The summit also approved the creation of a free economic zone in Kazakhstan, known as TURNSEZ.

At present, the members of the OTS include Turkey, Azerbaijan, Kazakhstan, Kyrgyzstan, and Uzbekistan, while Turkmenistan and Hungary participate as observer states. The leaders of these

countries inaugurated the organization's headquarters in Istanbul and adopted a strategic document entitled "Vision of the Turkic World 2040," which serves as a roadmap for deepening cooperation among Turkic-speaking states over the next two decades in priority sectors.

These areas of cooperation range from the removal of trade barriers and the harmonization of cultural and educational policies to the development of cross-border corridors—most notably the Trans-Caspian International Transport Route connecting Europe and China via Turkey and Azerbaijan—and the creation of a shared information space. The document also emphasizes the strengthening of political solidarity and mutual support in advancing national interests and addressing regional and global challenges.

The "Vision of the Turkic World 2040" further envisages the establishment of a "network for cooperation and information exchange among member states to counter threats of radicalization, violent extremism, Islamophobia, xenophobia, and terrorism, as well as to enhance border security". It also highlights the need for joint efforts to combat organized crime, illicit drug trafficking, irregular migration, and economic, financial, and cybercrime. In terms of joint responses to natural and man-made disasters, the document proposes the creation of a Turkic Civil Protection Council, a move interpreted by some experts as an attempt to lay the groundwork for a military-political alliance with the potential establishment of joint armed forces analogous to the CSTO (often referred to in expert discourse as a "Great Turkic Army" or "Army of Turan").

In recent years, Turkey has notably intensified security cooperation with Central Asian states, particularly with Kazakhstan. This includes exports of defense industry products, training of Kazakh military personnel, and the conduct of joint military exercises. Kazakhstan and Kyrgyzstan have also purchased Turkish-made Bayraktar unmanned aerial vehicles, which have demonstrated effectiveness in Azerbaijan and Ukraine.

Partnership with Turkey provides these four Central Asian states with an additional strong partner, facilitating the balancing of relations with Russia and China. Moreover, cultural and linguistic ties enhance Turkey's attractiveness as a partner for the majority of Central Asia's population.

Discussion

The findings of the study confirm the thesis that Central Asia is gradually transforming from a peripheral space of post-Soviet geopolitics into an autonomous geostrategic region that is increasingly integrated into global great power competition (Van den Bosch et al., 2021; Competition of World Powers in Central Asia, 2019). At the same time, the empirical evidence indicates that the growing international attention to the region is largely externally driven and reflects shifts in the global balance of power rather than the outcome of completed intra-regional consolidation (Wilson Center, 2025).

On the one hand, the intensification of interest from China, the United States, the European Union, and Turkey creates additional opportunities for Central Asian states to diversify their external relations, reduce dependence on a single center of influence, and pursue a multi-vector foreign policy (Khan & Koch, 2023; Multi-Vectoral Approach as the Key Model of Central Asian Countries' Foreign Policy, 2023). On the other hand, the analysis demonstrates that this multi-vectorism remains predominantly adaptive rather than proactive, as the key parameters of regional development continue to be shaped primarily by the policies of external actors (The Limits of Central Asia's Multi-Vector Foreign Policy, 2024).

Particular attention should be paid to the changing role of the Russian Federation in the region. While Russia long remained the dominant security and political actor, developments after 2014—and especially its full-scale war against Ukraine—have significantly undermined its position (Omelicheva, n.d.; Uslu, 2018). The results of the study suggest that Russia is increasingly losing its

status as an uncontested center of gravity (Hiro, 2009), retaining limited influence mainly in the security, migration, and cultural-humanitarian spheres. This finding is consistent with broader theoretical perspectives on the erosion of neo-imperial models of influence under conditions of multipolarity (Van den Bosch et al., 2021).

Against this background, China emerges as the leading geo-economic actor in Central Asia (Central Asia's Growing Partnership with China, n.d.). Its influence is based not on direct military-political presence but on infrastructure, financial, and trade instruments that generate long-term economic interdependence (Khan & Koch, 2023). The discussion of the results indicates that this model simultaneously stimulates regional development and creates risks of structural dependence, which may constrain the strategic autonomy of Central Asian states in the medium and long term.

The roles of the United States and the European Union appear less extensive in terms of economic presence, yet remain significant in normative and institutional dimensions. U.S. strategy is primarily focused on security issues (Cannon, 2025), deterrence of competitors, and support for regional sovereignty, whereas the European Union emphasizes economic cooperation, the development of transport corridors, energy diversification, and soft power instruments (Van den Bosch et al., 2021). However, the findings suggest that limited resources and the absence of robust security mechanisms reduce the ability of Western actors to function as system-shaping forces in the region (Wilson Center, 2025).

The growing role of Turkey also warrants separate discussion. By leveraging cultural and civilizational ties and institutionalized cooperation within the framework of the Organization of Turkic States, Turkey seeks to expand its influence in Central Asia (Ersen & Kösem, 2021). The analysis indicates that the Turkish vector is attractive to Central Asian elites as an additional balancing option vis-à-vis China and Russia (Great and Small Games in Central Asia and the South Caucasus, 2022). Nevertheless, its potential is constrained by Turkey's economic capacity and by the internal heterogeneity of the Turkic world (Ersen & Kösem, 2021).

Overall, Central Asia is gradually acquiring characteristics of a subject of international relations; however, this process remains incomplete. Regional cooperation shows positive dynamics but has not yet been transformed into stable institutional mechanisms capable of collectively defending regional interests (Khan & Koch, 2023). Thus, the current stage of Central Asia's development is characterized by a combination of expanding opportunities and persistent structural constraints, which necessitates a cautious interpretation of the region's apparent geopolitical rise (The Limits of Central Asia's Multi-Vector Foreign Policy, 2024).

Conclusions

Central Asia currently stands at a crossroads, where shifts in geopolitical dynamics generate both opportunities and challenges for the region to assert itself as a cohesive international actor. The weakening of Russia's traditional dominance, the expansion of China's influence, and the renewed pragmatism of Western engagement have collectively created a landscape in which Central Asian states can potentially enhance their agency and deepen regional cooperation.

However, this optimism must be tempered by on-the-ground realities. The region's growing international prominence is largely a byproduct of external power dynamics rather than the result of internal regional cohesion. Under such conditions, the region's significance may diminish as rapidly as it has increased, depending on the strategic interests of major powers. Internal challenges, including bilateral border disputes, further complicate the situation.

In light of these challenges, Central Asian states face the critical task of translating diplomatic rhetoric into tangible outcomes. Progress requires genuine cooperation not only among Central Asian states themselves, but also in their engagement with non-regional actors, ensuring that

regional agency is driven from within rather than emerging as a secondary effect of external circumstances.

Based on the foregoing analysis, the following analytical conclusions may be drawn:

1. China acts as the leading geo-economic actor, shaping structural dependence through infrastructure and financial instruments.

2. Russia retains security and cultural influence, but its position is gradually eroding.

3. The United States focuses primarily on security and normative issues, with limited economic leverage.

4. The European Union offers a stable, though less geopolitically assertive, model of cooperation.

5. Turkey concentrates on promoting the values and interests of the Turkic world at the regional and international levels, particularly in the security, economic, and social spheres.

These generalized conclusions may also be presented in the form of a consolidated Table 2.

Table 2. Comparative characteristics of the strategies of major players in Central Asia

Criterion	China	Russia	USA	European Union
Strategic goal	Geoeconomic integration of the region into Eurasian supply chains; security of the western borders	Preservation of traditional sphere of influence; political-military control	Deterring competitors; supporting sovereignty and security	Stability, diversification of partnerships, access to resources
Dominant type of influence	Economic and infrastructural	Military-political and security	Political and security, regulatory	Economic and normative (“soft power”)
Economic tools	Trade, investment, credit, BRI	Labor migration, energy relations	Limited investments, sanctions policy	Trade, grants, technical assistance
Infrastructure role	Key investor and builder (transport, energy)	Limited, mostly hereditary (Soviet)	Minimum	Fragmentary, project
Security mechanisms	SCO, anti-terrorist coordination	CSTO, military bases	Training missions, cooperation with individual states	Indirect participation (security sector reforms)
Political approach	The principle of non-intervention; elite diplomacy	Hierarchical model of influence	Promoting democracy and human rights	Conditionality of cooperation (good governance
Ideological component	Minimal, pragmatic	Imperial -historical	Liberal Democratic	Liberal-normative
“Soft power”	Education, culture, media (growing)	Language, culture, media (traditional)	Educational programs, NGOs	Education, regulatory standards

Criterion	China	Russia	USA	European Union
Perception in the region	Economically attractive, but with a risk of addiction	Traditional, but increasingly weak	Politically desirable, but limited	A reliable but slow partner
Key limitations	Fears of debt and political dependence	Weakening of the resource base and legitimacy	Limited presence and attention	Low geopolitical efficiency

Source: compiled by the author.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

Cannon, B. J. (2025). Central Asia and the Indo-Pacific. *International Affairs*, 101(4), 1177–1195. https://academic.oup.com/ia/article/101/4/1177/8178341

Central Asia's growing partnership with China. (n.d.). ETH Zurich. https://www.files.ethz.ch/isn/111372/WP4-EN.pdf

Competition of world powers in Central Asia. (2019). *Przegląd Politologiczny*, 2, 67–82. https://przeglad.amu.edu.pl/wp-content/uploads/2019/06/pp-2019-2-05.pdf

Ersen, E., & Kösem, S. (2021). *Turkey's pivot to Eurasia: Geopolitics and foreign policy in a changing world order*. Routledge.

Great and small games in Central Asia and the South Caucasus. (2022). Peter Lang. https://www.peterlang.com/document/1220623

Hiro, D. (2009). *Inside Central Asia: A political and cultural history*. Overlook Press. https://fpa.org/new-book-on-central-asia/

Khan, K. H., & Koch, H. (Eds.). (2023). *Emerging Central Asia: Managing great power relations*. Springer. https://www.econstor.eu/bitstream/10419/274025/1/Emerging-Central-Asia.pdf

Multi-vectoral approach as the key model of Central Asian countries' foreign policy. (2023). *MEMO Journal*, 67(12), 45–60. https://www.imemo.ru/en/publications/periodical/meimo/archive/2023/12-t-67/at-post-soviet-space/multi-vectoral-approach-as-the-key-model-of-central-asian-countries-foreign-policy

Omelicheva, M. Y. (n.d.). *Russia's foreign policy in Central Asia*. National War College. https://nwc.ndu.edu/Portals/71/Images/Publications/OmelichevaRussiaFPinCentralAsia.pdf

The limits of Central Asia's multi-vector foreign policy. (2024). Hague Centre for Strategic Studies. https://hagueresearch.org/the-limits-of-central-asias-multi-vector-foreign-policy/

Uslu, N. (2018). Central Asia in regional and global policies of Russia and China. *Bilig*, 87, 1–25. https://dergipark.org.tr/tr/download/article-file/4331543

Van den Bosch, J., Fauve, A., & De Cordier, B. (Eds.). (2021). *The Routledge handbook of contemporary Central Asia*. Routledge.

Wilson Center. (2025). *The great power rivalry in Central Asia*. https://www.wilsoncenter.org/publication/the-great-power-rivalry-central-asia

THE CONTEMPORARY SECURITY PROVISION MODEL IN THE INTELLIGENCE PRACTICE OF THE REPUBLIC OF ROMANIA

Andriy Stroev

PhD student, expert, e-mail: strilchuk7sv@gmail.com, ORCID: https://orcid.org/0009-0003-2188-4327

Ministry of Defense of Ukraine, Kyiv, Ukraine

Received: December 15, 2025 | Revised: December 28, 2025 | Accepted: December 31, 2025

UDC 351.86:327:355.40(498)

DOI: https://doi.org/10.33445/psssj.2025.6.4.5

Abstract

The article provides a comprehensive analysis of the contemporary security provision model within the intelligence practices of the Republic of Romania in the context of the evolving security environment. It examines the institutional architecture of the Romanian intelligence community, the functional specificities of its key actors, and their role in the system of strategic state governance. It is established that the Romanian model is characterised by a predominance of counterintelligence, the integration of intelligence structures into the decision-making system, the combination of classical methods (HUMINT) with modern digital tools, and a focus on the early detection of threats. It is substantiated that the transformation of Romania's intelligence practices has been driven by the impact of hybrid threats, the digitalisation of the security environment, and the increasing strategic importance of the Black Sea region as a zone of instability. It is demonstrated that the contemporary security provision model is based on an integrated approach that combines national capabilities with mechanisms of allied cooperation. Furthermore, it is determined that the effectiveness of the Romanian security system largely depends on the quality of intelligence analysis, the level of inter-institutional coordination, and the capacity to adapt to the cross-sectoral nature of contemporary threats. The practical significance of the study lies in the potential application of Romania's experience to enhance Ukraine's national security system, particularly in the development of counterintelligence, the integration of analytical capacities, and adaptation to hybrid confrontation.

Key words: National Security, Intelligence, Counter-Intelligence, Romania, HUMINT, Cyber Intelligence, Hybrid Threats, Strategic Assessment, the Black Sea Region, Security Policy.

Introduction

The contemporary security environment in Europe is characterised by a transition from a relatively stable system of international relations to conditions of strategic uncertainty, accompanied by the escalation of interstate confrontation, the expansion of the spectrum of hybrid threats, and the digitalisation of conflict. In such circumstances, the transformation of national security mechanisms assumes particular importance, especially through a reassessment of the role of intelligence activity [1, 2].

This study is based on an institutional and comparative analysis of the Romanian intelligence system, drawing on official strategic documents, legislative frameworks, and secondary analytical sources to identify structural features and functional patterns of intelligence governance.

The Republic of Romania, as a state located on Europe's eastern flank, operates in an environment marked by an elevated level of risk due to its geopolitical position in the Black Sea region, its proximity to an active conflict zone, and the spillover effects of instability in adjacent regions. Empirical analysis indicates that, under these conditions, intelligence activity performs a

system-forming role by обеспечением (providing) continuous threat assessment, early warning, and analytical support for state authorities [1, 3].

The Romanian intelligence community comprises several key institutions, including the Romanian Intelligence Service (SRI), the Foreign Intelligence Service (SIE), the Directorate-General for Defence Intelligence (DGIA), and the General Directorate for Internal Protection (DGPI), each of which performs specialised functions within the national security system.

A distinctive feature of the Romanian model is the institutionalised integration of intelligence structures into strategic decision-making processes. Evidence suggests that this integration is ensured through formal mechanisms such as the Supreme Council of National Defence (CSAT), interagency coordination frameworks, and direct analytical support to executive authorities. These arrangements allow intelligence to function not merely as an instrument of information collection, but as a key component in the formulation and implementation of national security policy.

Theoretical Background

The theoretical foundation of this study is grounded in contemporary approaches to understanding intelligence activity as an integrated component of the national security system, combining the functions of information collection, analysis, and support for strategic decision-making. In the context of the Romanian model, this approach is reflected in the National Defence Strategy of Romania 2020–2024, in which security is defined as the outcome of comprehensive risk management, while intelligence activity is identified as a key instrument for the identification and assessment of such risks (Presidential Administration of Romania, 2020; Sîrbu, M.).

From a methodological perspective, the study is based on the analysis of official documents and reports issued by Romania's intelligence authorities, in particular materials published by the *Serviciul Român de Informații* and the *Serviciul de Informații Externe*, which outline the functional aspects of their activities, the main directions of their work, and the transformation of their approaches to security provision (Serviciul Român de Informații [1] ; Serviciul Român de Informații [2]; Serviciul de Informații Externe).

An important theoretical reference point is the concept of expanded security, according to which threats are considered not solely in military terms, but also within the context of economic, informational, cyber, and social processes. This is evidenced by the inclusion, among recognised threats, of such phenomena as cybercrime, transnational organised crime, information operations, and hybrid influence.

In addition, the study is grounded in the assumption that national security systems are embedded within broader allied structures, as is characteristic of NATO member states. In this context, intelligence activity is regarded as an element of a multi-level system combining national and international security mechanisms (North Atlantic Treaty Organization; President of Ukraine, 2024).

Accordingly, the theoretical foundations of the study reflect a shift from a traditional understanding of intelligence towards its interpretation as a systemic instrument of security governance within a complex and multidimensional threat environment.

Data and Methods

This study is based on a qualitative research design combining institutional analysis, document analysis, and elements of comparative assessment. The methodological approach is aimed at identifying the structural and functional characteristics of the Romanian intelligence system and explaining its role within the broader framework of national security governance.

Data Sources

The empirical basis of the study consists primarily of official and open-source materials. These include strategic documents, legislative frameworks, and institutional reports issued by

Romanian state authorities, as well as analytical publications from international organisations and research centres. In particular, the study relies on:

- the *National Defence Strategy of Romania 2020–2024* as the principal doctrinal document defining the national security framework;
- official publications and reports of the *Serviciul Român de Informații* (SRI) and the *Serviciul de Informații Externe* (SIE);
- publicly available materials concerning cyber intelligence, counterintelligence, counterterrorism, and transnational threats;
- analytical sources related to NATO's eastern flank and Black Sea regional security.

The selection of sources is based on their relevance to the research objectives, their institutional authority, and their capacity to reflect both normative and operational dimensions of intelligence activity.

Methods

The study employs the following methods:

1. **Institutional analysis**, used to examine the structure of the Romanian intelligence community, the distribution of functions among its key actors, and the mechanisms of coordination within the national security system.
2. **Document analysis**, applied to strategic and operational materials in order to identify dominant concepts, threat perceptions, and functional transformations in intelligence practice. This method enables the reconstruction of the logic underlying the Romanian model of security provision.
3. **Comparative approach (limited scope)**, used to contextualise the Romanian model within broader NATO and European security frameworks, particularly with regard to allied integration and multidomain threats.
4. **Analytical generalisation**, employed to synthesise empirical findings and derive conclusions about the systemic features of intelligence governance and security provision.

Analytical Framework

The analysis is guided by the concept of **risk-based and multi-level security governance**, which interprets intelligence as an integrated component of decision-making processes rather than as a purely informational function. Within this framework, particular attention is paid to:

- the role of intelligence in early warning and threat assessment;
- the interaction between intelligence and political decision-making structures;
- the balance between HUMINT and technological intelligence capabilities;
- the integration of national intelligence systems into allied security architectures.

Limitations

The study has several limitations that should be acknowledged. First, it relies predominantly on official and open-source materials, which may reflect institutional perspectives and normative representations rather than fully capture operational realities. Second, the absence of quantitative data limits the possibility of measuring the effectiveness of the intelligence system through formal indicators. Third, the comparative component is limited and does not provide a full cross-national analysis.

Despite these limitations, the selected methodological approach allows for a systematic examination of the Romanian intelligence model and provides a sufficient basis for analytical conclusions regarding its structure, functions, and adaptation to contemporary security challenges.

Results

The contemporary model of security provision in the intelligence practice of the Republic of Romania is shaped by two fundamental factors. The first is the state's geopolitical position as a country on the eastern flank of NATO and the European Union, directly linked to the security of the Black Sea region. The second is the institutional evolution of Romania's security system, within which intelligence has evolved from being merely an instrument of information gathering into a central mechanism for early warning, strategic assessment, and support for state governance. It is for this reason that the National Defence Strategy of Romania 2020–2024 defines security as the outcome of the integrated management of multidimensional risks and threats, while resilience, strategic foresight, and the strengthening of institutional capacities are identified as key state priorities (Presidential Administration of Romania, 2020; Sîrbu, M.).

At the institutional level, the Romanian model is characterised by a relatively clear division of functions among the principal elements of the intelligence community, combined with a strong requirement for coordination. A central role in the domestic sphere is played by the *Serviciul Român de Informații*, which is responsible for safeguarding the constitutional order, conducting counterintelligence activities, countering terrorism, cyber intelligence, the protection of classified information, the prevention of transnational threats, and the identification of risks to national security. In the external domain, the *Serviciul de Informații Externe* operates with core functions that include the collection of intelligence for state decision-making, the provision of early warning on risks and threats in the international environment, and the conduct of operations aimed at protecting and advancing Romania's interests abroad. Both services are coordinated at the strategic level through the *Consiliul Suprem de Apărare a Țării*, which provides a framework for integrated threat assessment and mitigates the risk of fragmentation in information flows (Serviciul Român de Informații [1] ; Serviciul Român de Informații [2]; Serviciul de Informații Externe).

This institutional architecture explains why the contemporary Romanian security model cannot be reduced to the classical division between "internal" and "external" intelligence. In practice, it operates as a system for transforming information into actionable state decisions. Accordingly, the emphasis is placed not only on the collection of information, but also on its processing, analytical interpretation, correlation with multiple sources, and timely dissemination to political and military leadership in a form suitable for decision-making. In this respect, the Romanian model corresponds more closely to contemporary risk-based security governance than to traditional administrative models of intelligence services (Presidential Administration of Romania, 2020; Serviciul Român de Informații [2]).

A characteristic feature of Romanian practice is the predominance of a counterintelligence-oriented approach. This reflects the nature of the threat environment, which extends beyond conventional military risks to include espionage, penetration of strategic sectors, information operations, hybrid sabotage, the exploitation of transnational crime, cyber operations, and the manipulation of public sentiment. Open-source materials from the SRI indicate that particular emphasis is placed on the protection of classified information, industrial security, access vetting, security regime control, and the prevention of information leakage. This suggests that counterintelligence is conceptualised broadly as a multilayered system of state protection rather than merely the detection of hostile agents (Serviciul Român de Informații. *Protecția informațiilor clasificate*).

This conclusion is further supported by the development of the cyber component. Following the adoption of Law No. 58/2023, the SRI has been designated as the nationally competent authority in the field of cyber intelligence, and new categories of threats to national security have been formally recognised. These include cyber-attacks against critical infrastructure, phenomena affecting resilience to hybrid risks, and online propaganda or disinformation campaigns capable of influencing the constitutional order. This development indicates a formal expansion of the intelligence mandate beyond traditional military-political threats, incorporating cyberspace, digital disinformation, and hybrid influence into the core domain of intelligence activity (Serviciul Român de Informații. *Cyberintelligence*.).

At the same time, digitalisation does not eliminate the role of the human factor. Romanian intelligence practice demonstrates the coexistence of technical capabilities with traditional agent-based and counterintelligence methods. This reflects the nature of contemporary threats: while technical tools may detect communications, network intrusions, or anomalies in the information environment, they do not fully explain intent, motivation, recruitment channels, organisational linkages, or the likelihood of escalation from influence to active sabotage. Consequently, HUMINT and counterintelligence penetration remain critically important, particularly in countering foreign influence networks, criminal-intelligence symbioses, and transnational operational schemes (Serviciul Român de Informații. (n.d.). *Amenințări transnaționale*; Serviciul Român de Informații. (n.d.). *SRI foiled a sabotage operation conducted by the Russian Federation*).

A notable example is the information released by the SRI in January 2025 regarding the prevention of a sabotage operation on Romanian territory, which was attributed to the hybrid toolkit of the Russian Federation. According to official statements, the case involved the preparation of sabotage acts by a foreign operative who was identified prior to execution. This case provides empirical evidence that hybrid threats in Romania's security environment are not merely conceptual but manifest in concrete operational activities. Accordingly, security provision increasingly entails not only awareness but also pre-emptive action (Serviciul Român de Informații. (n.d.). *SRI foiled a sabotage operation conducted by the Russian Federation*).

An equally important dimension is counterterrorism. The SRI is designated as the leading national authority for the prevention and counteraction of terrorism, performing functions that include intelligence collection, multi-source analysis, monitoring, interagency coordination, and cooperation with international partners. Methodologically, this indicates that counterterrorism in Romania is structured not as an isolated function of a single agency, but as an integrated intelligence-analytical system aimed at identifying vulnerabilities and risk factors before they materialise into threats (Serviciul Român de Informații. (n.d.). *Preventing and countering terrorism*).

Another significant aspect is the linkage between security and transnational threats. The SRI classifies organised crime, illegal migration, cybercrime, large-scale tax evasion, smuggling, and illicit transfers of military technologies as national security risks. This reflects a key feature of the Romanian approach: intelligence operates at the intersection of internal security, economic stability, and international obligations. As a result, the contemporary model of security provision can be understood as a model of expanded security, encompassing economic, criminal, logistical, and network-related dimensions as potential vectors of destabilisation (Serviciul Român de Informații. (n.d.). *Amenințări transnaționale*).

This expanded security logic is particularly evident in the Black Sea dimension. In recent years, Romania has emerged as a key allied hub of deterrence and security in the region. Analytical assessments indicate that Black Sea security has become central to Romania's strategic outlook. Russia's full-scale war against Ukraine has reinforced this trend, bringing issues such as military mobility, maritime security, protection of transport corridors, allied presence, and regional stability into the core of threat assessment. The bilateral security agreement between Ukraine and Romania

(July 2024), which предусматриє cooperation in intelligence, counterintelligence, cyber security, information security, and Black Sea security, further demonstrates the increasing regionalisation of Romania's security model (North Atlantic Treaty Organization; President of Ukraine, 2024; Reuters).

At the same time, this model should not be idealised. Its strengths — counterintelligence depth, expanded mandate, early warning capabilities, cyber integration, coordination through the CSAT, and strong links with NATO and the EU — are accompanied by structural limitations. These include dependence on allied frameworks in areas where national intelligence capacities are insufficient, the risk of systemic overload due to the expansion of intelligence functions, and challenges related to institutional trust and corruption risks, which may affect public perceptions and the societal legitimacy of the security system (Presidential Administration of Romania, 2020; Sîrbu).

From a scholarly perspective, the Romanian model is best understood not as an ideal type, but as an adaptive security system of a medium-sized state operating under conditions of heightened risk and constrained resources. Its defining feature is the combination of national counterintelligence and analytical capacities with allied integration. In this sense, Romanian intelligence practice reflects a model of "security through integration", where resilience is strengthened both domestically and through participation in broader security frameworks. For Ukraine, this model has practical relevance, demonstrating that effectiveness depends not solely on resource scale, but on coordination quality, the balance between HUMINT and technical capabilities, normative adaptability, and the capacity to integrate intelligence into strategic governance (Presidential Administration of Romania, 2020; Serviciul Român de Informații. (n.d.). Cyberintelligence; North Atlantic Treaty Organization).

Discussion

The results of the study suggest that the Romanian model of intelligence-based security provision reflects a transition from a traditional, functionally segmented system towards an integrated model of security governance. This transformation aligns with broader theoretical perspectives on risk-based and multi-level security systems, in which intelligence is embedded within decision-making structures rather than operating as a separate informational subsystem.

A key implication of the findings is the redefinition of intelligence from a supporting function to a system-forming element of governance. However, this conclusion requires careful qualification. While institutional arrangements such as the CSAT facilitate integration, the degree to which intelligence outputs directly influence political decisions remains dependent on broader governance dynamics, including political priorities and administrative capacity.

The predominance of counterintelligence reflects adaptation to a hybrid threat environment, yet it also raises questions regarding balance. An excessive focus on counterintelligence may potentially limit the development of external intelligence capabilities or strategic forecasting functions. Comparative analysis with other NATO states suggests that successful models tend to maintain a more balanced distribution between counterintelligence, foreign intelligence, and analytical capacities.

The expansion of the intelligence mandate into cyber and informational domains represents a necessary adaptation to contemporary threats. At the same time, this expansion creates risks of functional overload and institutional overstretch. As intelligence agencies assume responsibilities in areas such as cyber resilience, critical infrastructure protection, and disinformation counteraction, the boundaries between intelligence, law enforcement, and regulatory functions become increasingly blurred. This may complicate accountability mechanisms and require further institutional clarification.

The coexistence of HUMINT and technical intelligence confirms the hybrid nature of modern intelligence practice. The findings support the argument that technological capabilities cannot fully

replace human intelligence, particularly in understanding intent and complex organisational behaviour. This has implications for resource allocation, training, and institutional development.

The regional dimension of the Romanian model highlights the growing importance of allied integration. The concept of "security through integration" appears to be a defining feature of medium-sized states operating under conditions of limited resources. However, this also implies a degree of dependency on allied intelligence frameworks, which may constrain national autonomy in certain areas.

An important limitation of the study is its reliance on official and open-source materials, which may reflect institutional narratives rather than fully capture operational realities. Future research should incorporate comparative analysis and independent data sources to provide a more balanced assessment.

In practical terms, the Romanian experience offers relevant insights for Ukraine. The findings indicate that the effectiveness of an intelligence system depends not only on resource capacity, but also on institutional coordination, the integration of analytical functions, and the ability to adapt to hybrid threats. However, the transferability of this model requires careful consideration of contextual differences, including scale, threat intensity, and governance structures.

Conclusions

The contemporary model of security provision in the intelligence practice of the Republic of Romania constitutes an integrated system in which intelligence plays a central role in the formulation and implementation of state security policy. Its principal characteristic lies in the combination of classical intelligence instruments—above all counterintelligence and HUMINT—with modern technological and analytical approaches.

The analysis indicates that the Romanian model is oriented towards the early detection of threats, their systematic interpretation, and their transformation into actionable decisions. At the same time, a counterintelligence-oriented approach remains predominant due to the high level of external influence and hybrid threats. The development of cyber intelligence, integration into allied security structures, and the strengthening of the analytical component further demonstrate the system's adaptation to contemporary challenges.

The practical significance of the Romanian model lies in its demonstration of the effectiveness of an integrated approach to security provision, combining national capabilities with international cooperation. For Ukraine, this experience is particularly relevant in the context of developing intelligence structures, countering hybrid threats, and integrating analytical capabilities into the process of state governance.

Prospects for Further Research

Further research would benefit from a more in-depth analysis of the interaction between intelligence and analytical structures within an integrated security system, particularly with regard to the effectiveness of combining HUMINT and cyber intelligence under conditions of hybrid confrontation. Particular attention should also be given to the mechanisms through which intelligence systems adapt to multidomain threats, as well as to a comparative analysis of the models of Romania, France, and other European Union states, with a view to identifying both universal and nationally specific approaches.

Of practical importance is also the study of the potential for implementing selected elements of the Romanian model within Ukraine's national security system, taking into account wartime conditions and institutional specificities.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

Presidential Administration of Romania. (2020). *National defence strategy of Romania 2020–2024*. https://www.presidency.ro/files/userfiles/National_Defence_Strategy_2020_2024.pdf

Sîrbu, M. (n.d.). *Romania's national defense strategy 2020–2024: A reinforced pillar for NATO*. Center for European Policy Analysis. https://cepa.org/article/romania-national-defense-strategy-2020-2024

Serviciul Român de Informații [1]. (n.d.). *Despre noi*. https://www.sri.ro/despre-noi

Serviciul Român de Informații [2]. (n.d.). *Rapoarte de activitate*. https://www.sri.ro/rapoarte

Serviciul de Informații Externe. (n.d.). *Misiune și atribuții*. https://www.sie.ro/despre.html

Serviciul Român de Informații. (n.d.). *Protecția informațiilor clasificate*. https://www.sri.ro/protectia-informatiilor

Serviciul Român de Informații. (n.d.). *Cyberintelligence*. https://www.sri.ro/cyberintelligence

Serviciul Român de Informații. (n.d.). *Amenințări transnaționale*. https://www.sri.ro/amenintari-transnationale

Serviciul Român de Informații. (n.d.). *SRI foiled a sabotage operation conducted by the Russian Federation*. https://www.sri.ro/en/sabotage-operation

Serviciul Român de Informații. (n.d.). *Preventing and countering terrorism*. https://www.sri.ro/antiterorism

North Atlantic Treaty Organization. (n.d.). *Black Sea security and Eastern flank analysis*. https://www.nato.int/cps/en/natohq/topics_136388.htm

President of Ukraine. (2024). *Security cooperation agreement between Ukraine and Romania*. https://www.president.gov.ua/en/news/security-agreement-ukraine-romania-2024

Reuters. (n.d.). *Black Sea maritime security developments*. https://www.reuters.com/world/europe/black-sea-security

A RISK-ORIENTED FRAMEWORK FOR FORMING AND MODELLING INFORMATION SECURITY PROFILES IN MODERN CYBERSPACE

Ruslan Netrebko

e-mail: netr_rv@ukr.net , ORCID ID: https://orcid.org/0000-0003-3212-5249

Korolov Zhytomyr Military Institute, Zhytomyr, Ukraine

Received: December 13, 2025 | Revised: December 28, 2025 | Accepted: December 31, 2025

UDC 004.056

DOI: https://doi.org/10.33445/psssj.2025.6.4.6

Abstract

The purpose of the article is to substantiate the theoretical foundations for forming information security profiles in Ukraine and to adapt established probabilistic, optimization, and economic models for assessing their effectiveness, resilience, and resource feasibility in critical infrastructure information systems. The study combines historical-regulatory and comparative analysis of Ukrainian requirements with NIST SP 800-series and ISO/IEC standards, set-theoretic formalization, a two-state continuous-time Markov model, binary optimization under a budget constraint, annualized loss expectancy, and return on security investment. The development of Ukrainian regulation between 2021 and 2026 is represented as three stages: institutional preparation and wartime transition, harmonization with international standards, and implementation of a risk-oriented approach. Four types of security profiles are distinguished: basic, sectoral, target, and adapted. A security profile is formalized as a set of security and privacy requirements, selected controls, control enhancements, organization-defined parameters, and mappings to identified threats and risks. The proposed indicators support risk-weighted threat coverage, a simplified availability-like resilience estimate, and selection of controls subject to resource constraints. The study integrates and adapts established regulatory, probabilistic, optimization, and economic approaches to the Ukrainian technical information protection framework rather than claiming a universal assessment model. The models may support owners and administrators of critical infrastructure information systems in documenting, selecting, assessing, and authorizing protective measures, provided that model parameters are empirically calibrated for the relevant system.

Key words: ND TZI 3.6-006-24; Risk Management; Critical Infrastructure; Protective Measures; Cyber Resilience; Resource Allocation.

Introduction

In the contemporary world, information has acquired the status of one of the key strategic resources of the system for ensuring the national security and defence of the state. Under the conditions of the armed conflicts and hybrid confrontation of the twenty-first century, the systematic assessment of risks to the security of information processed and stored in automated systems has become particularly important. The active use by an adversary of technical and cyber reconnaissance, cyberattacks, information-psychological operations, and disinformation campaigns substantially increases the level of threats to such systems and creates risks of unauthorized access to, loss of, or modification of protected information.

Under conditions of high-intensity information confrontation and the rapid development of cyber instruments, even minor miscalculations in assessing the risks of breaches of confidentiality,

integrity, or availability of information may lead to serious consequences. These include threats to the security of personnel, reduced effectiveness in the employment of weapons and military equipment, and the disruption of command and control during the performance of combat missions.

Despite the existence of a regulatory and legal framework in the field of technical information protection, one of the key problems remains the practical implementation of, and compliance with, the established procedure for assessing risks to the security of information processed in automated systems, including those of the Armed Forces of Ukraine. This is caused by dynamic changes in the operational situation, limited resources, and the vulnerability of communication channels, which require the constant review, refinement, and adaptation of risk assessment procedures to real conditions.

In an environment of persistent cyber threats and the digital transformation of state institutions, traditional template-based methods of protection are losing effectiveness. A new stage in the development of technical information protection (TIP) in Ukraine began in 2024 with the adoption of ND TZI 3.6-006-24, Procedure for Selecting Measures to Protect Information, the Protection Requirement for Which Is Established by Law and Which Does Not Constitute a State Secret, for Information Systems (Administration of the SSSCIP, 2024). The document establishes a risk-oriented procedure for selecting and tailoring protective measures for information systems. Resolution No. 712 of the Cabinet of Ministers of Ukraine subsequently specified the governance of basic, sectoral, and target security profiles and security authorization (Cabinet of Ministers of Ukraine, 2025). Together, these instruments support a transition from static sets of requirements to profiles adapted to the purpose, criticality, operating environment, and risks of a particular system. Theoretical formalization can reduce subjectivity in selecting measures and improve the transparency of resource allocation.

The purpose of this study is to analyse the evolution of the Ukrainian regulatory framework for security profiling since 2021, with an emphasis on ND TZI 3.6-006-24 and Resolution No. 712 of the Cabinet of Ministers of Ukraine; to systematize the structure of a security profile in relation to NIST SP 800-series and ISO/IEC standards; and to construct an integrated analytical framework for assessing the technical and economic characteristics of such profiles.

To achieve this purpose, the study addresses the following research objectives:

to identify the principal stages in the transformation of the Ukrainian regulatory framework for security profiling between 2021 and 2026;

to systematize the typology and structure of security profiles established by ND TZI 3.6-006-24 and distinguish it from the governance framework of Resolution No. 712;

to develop a formal set-theoretic model of the security profile and an indicator of its threat-coverage effectiveness;

to model the resilience of a protected system using Markov chains and to formulate the problem of the optimal selection of protective measures under budget constraints;

to substantiate economic indicators of the effectiveness of security investment and the procedure for profile verification.

The object of the study is the process of forming information security profiles for critical infrastructure information systems.

The subject of the study is the theoretical foundations and analytical models for the formation, assessment, and verification of security profiles based on ND TZI 3.6-006-24 and the international standards of the NIST SP 800 series.

Literature Review

1. The Systemic Approach to Technical Information Protection in Ukraine

A systemic approach treats information protection not as a set of isolated technical tools but as an organizational and technical system whose composition must be justified by the mission,

architecture, criticality, and risk context of the protected object. In the economic literature, security investment is analysed through expected-loss reduction, budget constraints, and the marginal effectiveness of controls (Gordon & Loeb, 2002; Cavusoglu et al., 2004; Bojanc et al., 2012). Portfolio formulations further show that the selection of controls is a constrained resource-allocation problem rather than an unconstrained maximization of protection (Yevseyeva et al., 2015).

2. International Standards and the Risk-Oriented Approach

International experience provides complementary layers for risk-oriented profiling. NIST SP 800-39 and SP 800-37 Rev. 2 define organization- and system-level risk-management processes; SP 800-53 Rev. 5, SP 800-53B, and SP 800-53A Rev. 5 address controls, baselines, tailoring, and assessment; SP 800-30 Rev. 1 and the NIST IR 8286 series address risk identification, estimation, prioritization, and enterprise integration (Joint Task Force Transformation Initiative, 2011; National Institute of Standards and Technology [NIST], 2012, 2025a, 2025b, 2025c; Joint Task Force, 2018, 2020a, 2020b, 2022). ISO 31000 and ISO/IEC 27005 provide general and information-security risk guidance, while the NIST Cybersecurity Framework 2.0 supports organizational profiles and outcome-oriented governance (International Organization for Standardization [ISO], 2018, 2022; NIST, 2024). Quantitative risk and resilience remain parameter-dependent and require calibrated evidence (Hubbard & Seiersen, 2016; Wang et al., 2020; Linkov et al., 2013; Kott & Linkov, 2019).

However, the reviewed approaches address different analytical layers and are not directly interchangeable. Regulatory standards define governance, control selection, tailoring, assessment, and authorization; economic models estimate expected-loss reduction and investment efficiency; optimization models treat security controls as a constrained portfolio; and resilience models represent system behaviour under disruption and recovery. A methodological gap therefore remains between the formal structure of a Ukrainian security profile and the quantitative procedures used to compare alternative control configurations. The present study addresses this gap by integrating the official Ukrainian procedure for selecting protective measures with established international models, while explicitly limiting quantitative conclusions to systems for which input parameters have been empirically calibrated.

The scientific contribution of the study consists in constructing an integrated analytical representation of the Ukrainian security-profile framework in which regulatory profile components are linked to threat coverage, an availability-based resilience proxy, resource-constrained control selection, economic evaluation, and verification. Unlike approaches that examine these elements separately, the proposed framework treats them as interrelated stages of profile formation, assessment, and authorization without claiming that the resulting indicators constitute a universally validated methodology.

Materials and methods

This study is qualitative-analytical in nature and adopts a theoretical research design supported by formal mathematical modelling.

The empirical and documentary basis of the study consists of:

ND TZI 3.6-006-24, which establishes the procedure for selecting and tailoring information protection measures for information systems, and Resolution No. 712, which regulates the formation and application of basic, sectoral, and target profiles and security authorization (Administration of the SSSCIP, 2024; Cabinet of Ministers of Ukraine, 2025);

NIST SP 800-39, SP 800-37 Rev. 2, SP 800-53 Rev. 5, SP 800-53B, SP 800-53A Rev. 5, SP 800-30 Rev. 1, SP 800-160 Vol. 2 Rev. 1, the NIST IR 8286 series, and the NIST Cybersecurity Framework 2.0;

DSTU ISO/IEC 27001:2023, ISO 31000:2018, and ISO/IEC 27005:2022;

peer-reviewed scholarly publications on information security management, risk quantification, and cyber resilience.

The documentary sources were selected according to five criteria: current normative relevance; a direct relationship to security profiling or information-system protection; applicability to critical infrastructure or high-criticality systems; inclusion of procedures for selecting, tailoring, assessing, or authorizing controls; and methodological compatibility with a risk-oriented approach.

The following research methods were employed:

Historical-regulatory analysis was used to reconstruct the stages in the transformation of the Ukrainian framework for technical information protection between 2021 and 2026.

Comparative analysis was applied to relate the provisions of ND TZI 3.6-006-24 to NIST SP 800-53 and ISO/IEC 27001 across the following analytical categories: baseline requirements, tailoring, organization-defined parameters, documentation of deviations, control assessment, security authorization, and continuous monitoring.

Set-theoretic modelling was employed to formalize the security profile as a system of security and privacy requirements, selected protective measures, control enhancements, organization-defined parameters, and mappings to current threats and risks.

A two-state continuous-time Markov model was used to derive a simplified availability-based proxy for one dimension of cyber resilience in a protected system.

Binary mathematical programming was applied to formulate the selection of protective measures that minimizes residual risk under a budget constraint.

Methods of quantitative risk assessment, including annualized loss expectancy (ALE) and return on security investment (ROSI), were used to illustrate economic evaluation. These calculations are treated as parameter-dependent analytical models rather than empirical estimates for a specific system.

The unit of analysis is the security profile as a regulatory and mathematical object, characterized by its composition of protective measures, its mapping onto threats, its resilience indicators, and its cost of implementation.

Results

1. Stages in the Evolution of the Regulatory Framework for Security Profiling (2021–2026)

For analytical purposes, the development of the regulatory framework for security profiling in Ukraine is divided into three stages. The boundaries between the stages are defined by four criteria: the adoption of a significant regulatory instrument, a change in the object of regulation, a change in the principle used to select protective measures, and a change in the assessment or authorization mechanism.

Stage one: institutional preparation and wartime transition (2021–2022). This stage is interpreted as a preparatory and transitional period rather than as a formally codified stage of security-profile regulation. In 2021, regulatory and organizational preparation focused on updating approaches to comprehensive information protection and system criticality. After the introduction of martial law in 2022, the emphasis shifted toward continuity, operational resilience, and protection under rapidly changing threat conditions. Distinguishing these two contexts avoids attributing the legal regime of martial law to the whole 2021–2022 period.

Stage two: harmonization and European integration (2023). The adoption of DSTU ISO/IEC 27001:2023 made it possible to integrate international practices into the Ukrainian regulatory field (State Enterprise “UkrNDNC”, 2023). The development began of profiles that take into account not only technical measures but also organizational aspects, including the human factor and supply chains.

Stage three: implementation of the risk-oriented paradigm (2024–2026). ND TZI 3.6-006-24 established a procedure for selecting protective measures on the basis of information requirements, system characteristics, and security risks (Administration of the SSSCIP, 2024). Resolution No. 712 of 2025 complemented this procedure by defining the governance of basic, sectoral, and target

profiles and security authorization (Cabinet of Ministers of Ukraine, 2025). The two instruments should be read together but should not be treated as identical classifications.

Protective measures in the information systems of the Armed Forces of Ukraine are implemented within the information protection system in accordance with the criticality category of the information system, its structural and functional characteristics, the results of risk analysis, the technologies employed, and the specific features of its operation.

The process of selecting protective measures is of key importance for an organization and must ensure conformity with the mission, goals, and tasks of the military unit, as well as with the requirements of current legislation, regulatory documents, standards, and security and privacy policies. No universal set of measures capable of covering all aspects of security exists. A rational selection presupposes consideration of the context of use, the specific features of the information system's operation, its environment, and its needs. The effective determination of protective measures requires interaction with stakeholders and is oriented toward achieving an acceptable balance between ensuring the confidentiality, integrity, and availability of information and protecting personal data.

2. The Concept and Typology of Security Profiles

To unify approaches to the selection of protective measures, the concept of a security profile is employed: a coherent set of security and privacy requirements, selected measures, enhancements, parameters, and implementation conditions that reflects the organization's mission, the purpose and criticality of the system, and current risks. ND TZI 3.6-006-24 distinguishes four profile types—basic, sectoral, target, and adapted—whereas Resolution No. 712 regulates the governance relationship among basic, sectoral, and target profiles. Their interrelation is presented in Figure 1. Solid arrows show the principal sequence of profile specification; dashed arrows show that tailoring may be applied to the applicable basic, sectoral, or target profile for a particular system.

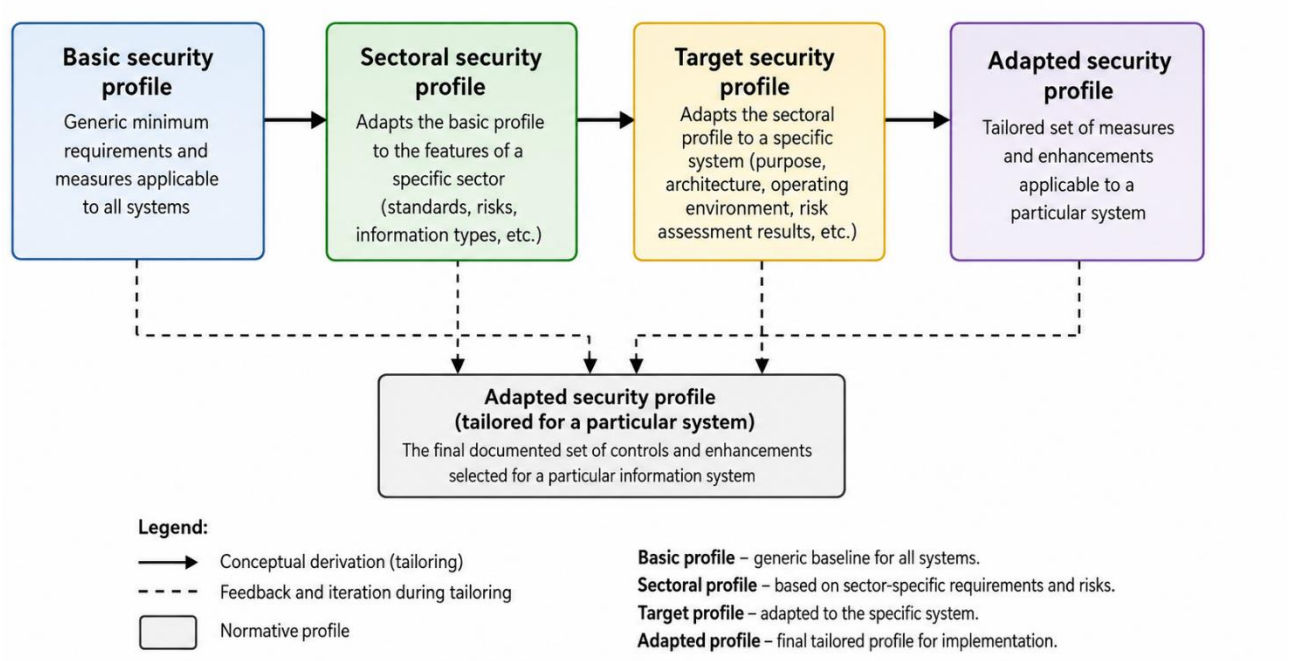


Figure 1: Types of security profiles and their interrelation
Source: Authors' Construct

The basic security profile of a system comprises the minimum information security requirements and an interrelated set of protective measures established depending on the

information processed in the system or its functional purpose. The basic profile establishes general minimum requirements for information protection applicable to all systems in which information is processed. It reflects the general principles, norms, and recommendations approved at the state level and serves as the basis for further elaboration.

The sectoral security profile of a system is an interrelated set of information protection measures defined for the system by the authorized sectoral body, taking into account the minimum requirements of the basic profile, the relevant standards and security policies, and the specific conditions of the system's operation (outside a zone of combat operations or within such a zone), together with the provision of corresponding recommendations. The sectoral profile adapts the basic profile to the specific features of operation and activity in a given sector, detailing protective measures with regard to sectoral risks, types of information, and technical particularities.

The target security profile of a system is an interrelated set of information protection measures defined by the owner or administrator of the system, taking into account the minimum requirements of the basic profile; the requirements of legislation and national standards in the fields of cryptographic and technical information protection and cyber defence; the regulatory documents of the system of technical and cryptographic information protection; the sectoral profile and applicable security policies; the purpose of the system, its structural and functional characteristics, and the specific features of its operation; and the results of the conducted security risk assessment.

The target profile is formed by the owner or administrator of the system and constitutes the concretization of the basic and sectoral profiles with respect to the particular system. It defines the list of security measures actually implemented, as well as the criteria for evaluating the conformity of the adopted measures with the security requirements. The target profile is developed for the specific system subject to security authorization; in the cases provided for by the sectoral profile, the target profile is agreed with the authorized sectoral body. The structure of the security profile is presented in Figure 2.

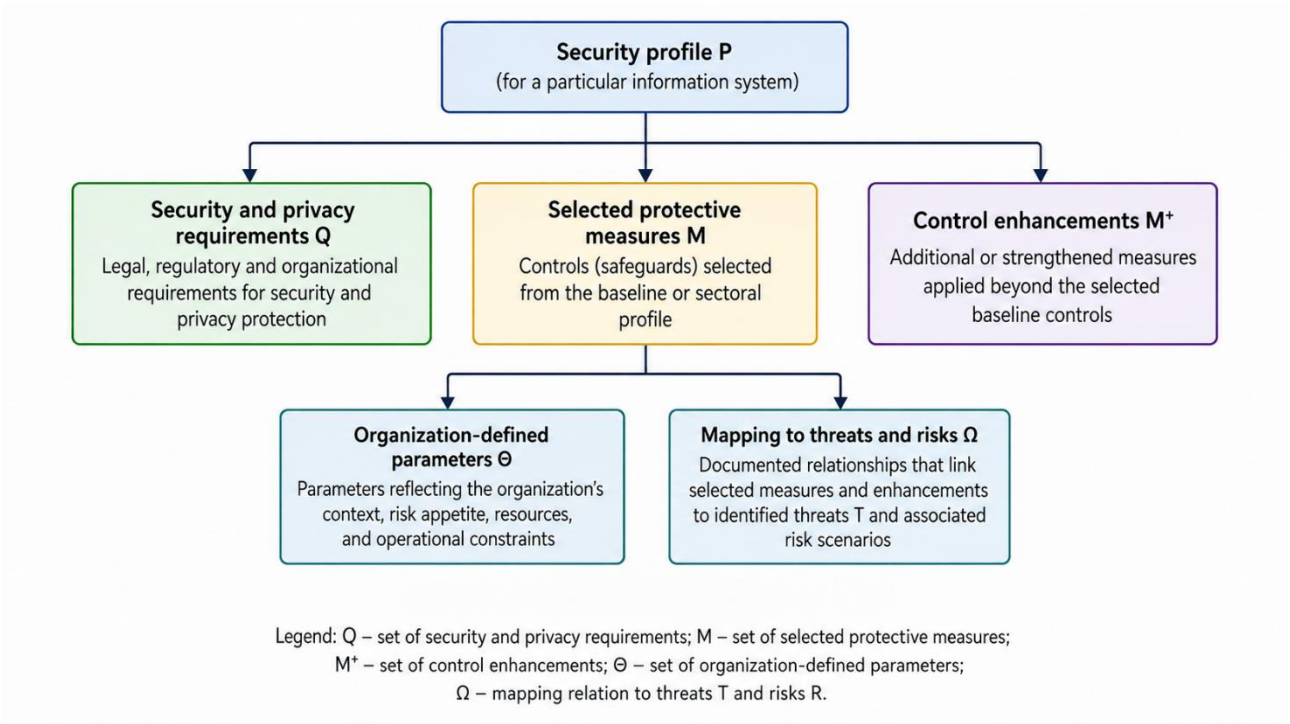


Figure 2: Structure of the security profile P
Source: Authors' Construct

The adapted security profile is produced by tailoring the applicable basic, sectoral, or target profile to the conditions of a particular information system. It records justified inclusions, exclusions,

parameter values, and refinements of protective measures on the basis of the system's purpose, architecture, operating environment, and assessed risks. Adaptation does not cancel mandatory legal requirements; each deviation must be documented and traceable to the risk assessment.

In accordance with ND TZI 3.6-006-24, protective measures are selected and adapted through a risk-oriented procedure. This is methodologically comparable to the tailoring of control baselines in NIST SP 800-53 Rev. 5, while the Ukrainian procedure retains the requirements of national legislation on technical and cryptographic information protection (Joint Task Force, 2020a; Administration of the SSSCIP, 2024).

3. A Formal Model of the Security Profile Structure

For the formal description used in this study, the security profile P is represented as:

$$P = \langle Q, M, M^{+}, \Theta, \Omega \rangle \quad (1)$$

where: Q – is the set of applicable security and privacy requirements;
M – is the set of selected protective measures (controls);
M^{+} – is the set of selected control enhancements;
Θ – is the set of organization-defined parameters;
T – is the set of identified threats and associated risk scenarios; $\Omega \subseteq (M \cup M^{+}) \cdot T$ is the documented relation that maps selected protective measures and enhancements to those threats and risk scenarios.

The threat set T is treated as an external input derived from the system risk assessment rather than as an internal component of the profile structure. For operational application, the model may be extended by an asset set A, a vulnerability set V, and a risk set R; these elements are not included in the minimal representation because the present study focuses on the internal structure of the profile rather than on a complete system-risk ontology.

Each threat or risk scenario $t_i \in T$ is characterized by a potential loss L_i and a probability of realization p_i. The term p_iL_i represents the baseline expected loss of scenario i, with p_i incorporating the event and conditional probabilities defined by the adopted risk model. The effectiveness of profile E(P) is defined as the capacity of the measures selected in the profile to reduce risk:

$$E(P) = [\Sigma_i\, p_iL_i\alpha_i(P)] / [\Sigma_i\, p_iL_i] \quad (2)$$

where $\alpha_i(P) \in [0, 1]$ is the empirically estimated aggregate reduction in expected loss for threat t_i achieved by the measures included in profile P. The normalized indicator $E(P) \in [0, 1]$ expresses the proportion of baseline expected loss mitigated by the profile. It assumes that interactions among measures have already been reflected in $\alpha_i(P)$; otherwise, a model with measure-specific coefficients and interaction terms is required. The formulation also assumes that the risk scenarios are defined so as to avoid double-counting strongly dependent losses.

5. A Simplified Availability-Based Proxy for Profile Resilience

Cyber resilience may be analysed through stochastic state-transition models (Linkov et al., 2013; Gisladottir et al., 2017; Ross et al., 2021). For a deliberately simplified two-state continuous-time Markov model, let S_o denote a secure/operational state and S_1 a non-operational state encompassing compromise and recovery. The compromise intensity λ reflects the rate of transitions from S_o to S_1, while the recovery intensity μ reflects transitions from S_1 to S_o. Under constant transition rates, the stationary probability of the secure state is:

$$\pi_o = \mu / (\lambda + \mu) \quad (3)$$

The value π_o should be interpreted as a simplified availability-like resilience proxy for the stated two-state assumptions, not as a universal regulatory protection coefficient. ND TZI 3.6-006-

24 does not establish a general threshold of 0.999 for this indicator; any threshold must therefore be justified for the particular system and service requirement.

6. Optimization of the Selection of Protective Measures

Let $x_j \in \{0, 1\}$ indicate whether protective measure j is selected, c_j be its implementation cost, and $\alpha_{ij} \in [0, 1]$ be its estimated effectiveness against threat i. A localized binary linear formulation that minimizes expected residual loss under budget B is:

$$\min_x \ \Sigma_i \, p_i L_i (1 - \Sigma_j \, \alpha_{ij} x_j) \tag{4}$$

$$\text{subject to } \Sigma_j \, c_j x_j \le B,$$
$$\Sigma_j \, \alpha_{ij} x_j \le 1, \text{ for all i},$$
$$x_j \in \{0, 1\}, \text{ for all j}.$$

Here $p_i L_i$ is the expected loss associated with threat i before additional measures are selected. The constraint $\Sigma_j \, \alpha_{ij} x_j \le 1$ prevents the linear approximation from implying more than complete risk reduction. The model assumes additive marginal effects and no double-counting, incompatibility, or synergy among controls. Practical application may require mandatory-control constraints, logical dependencies, incompatibility constraints, minimum coverage of critical threats, lifecycle costs, and personnel or implementation-time limits. A multiplicative residual-risk form, $p_i L_i \prod_j (1 - \alpha_{ij} x_j)$, avoids additive overstatement but produces a nonlinear optimization problem (Yevseyeva et al., 2015).

7. Economic Evaluation: Quantitative Risk Assessment and Return on Security Investment

For an illustrative calculation of annualized loss expectancy (ALE), the following traditional quantitative-risk expression is used (Hubbard & Seiersen, 2016; Bojanc et al., 2012):

$$ALE = AV \cdot EF \cdot ARO \tag{5}$$

where:
- AV (asset value) – is the value of the asset, including data, reputation, and potential penalties;
- EF (exposure factor) – is the percentage of the asset lost in the event of a successful attack;
- ARO (annualized rate of occurrence) – is the expected frequency of attacks per year.

For a screening-level comparison of the expected benefit and cost of a security investment, the return-on-security-investment indicator is applied (Cavusoglu et al., 2004; Sonnenreich et al., 2006):

$$ROSI = (R \cdot \rho_p - C_{total}) / C_{total} \tag{6}$$

where:
- R – is the monetary value of the risk (ALE);
- ρ_p – is the proportion of baseline risk eliminated by profile P; where the same loss basis and calibration are used, ρ_p may be operationalized by the normalized indicator E(P);
- C_{total} – is the total cost of ownership (TCO) of the protection system.

In Equation (6), ROSI is a dimensionless relative return: ROSI > 0 indicates that the estimated avoided loss exceeds the total cost of ownership, whereas ROSI < 0 indicates the opposite. The monetary net benefit may additionally be reported as $R \cdot \rho_p - C_{total}$. Because R and ρ_p are uncertain, both indicators should be accompanied by sensitivity or scenario analysis rather than interpreted as precise forecasts (Sonnenreich et al., 2006).

8. Verification of the Security Profile

Verification of a target or adapted security profile should demonstrate that the selected measures are implemented as specified. In this study, verification means confirmation of

implementation against stated requirements; validation means confirmation that the profile is suitable for the actual threat and operating context; assessment means the systematic examination, interview, and testing of controls; and authorization means the accountable management decision to accept residual risk and permit operation. Depending on the applicable profile, system criticality, and risk assessment, evidence may include documentation review, examination, interviews, technical tests, vulnerability analysis, penetration testing, and developer evidence. These activities support security authorization and continuous monitoring; penetration testing and source-code review should not be described as universally mandatory unless the applicable profile explicitly selects them (Joint Task Force, 2018, 2022; Dempsey et al., 2011; Nelson et al., 2025). A proportionate four-part verification structure is:

implementation verification: examination, interviews, and testing against the selected control requirements and organization-defined parameters;

technical validation: vulnerability analysis, penetration testing, resilience exercises, or simulation where justified by the profile and risk assessment;

evidence review: assessment of implementation records, configuration, developer evidence, and operational processes where applicable;

authorization and monitoring: documented assessment of conformity with the target or adapted profile, followed by risk acceptance and continuous monitoring.

Discussion

The findings of this study indicate that the transformation of the Ukrainian regulatory framework for technical information protection between 2021 and 2026 should not be interpreted as a mere accumulation of new documents. Rather, it represents a paradigmatic transition from rigid, template-based protection models toward flexible, risk-oriented security profiles.

First, the introduction of the concept of criticality during the transitional period of 2021–2022 prepared the conceptual ground for differentiated protection requirements, while the adoption of DSTU ISO/IEC 27001:2023 institutionalized the connection between Ukrainian regulation and international information security management practice (State Enterprise “UkrNDNC”, 2023).

Second, ND TZI 3.6-006-24 supports a dynamic, risk-oriented representation of the security profile through requirements, measures, enhancements, parameters, and documented mappings to threats and risks. This representation is methodologically comparable with the tailoring approach of NIST SP 800-53 Rev. 5 and can improve interoperability of assessment practices, but it does not establish automatic mutual recognition between Ukrainian and foreign authorization regimes (Joint Task Force, 2020a; Administration of the SSSCIP, 2024).

Third, the integrated mathematical apparatus converts selected expert assumptions into parameter-dependent indicators. The threat-coverage measure, the two-state Markov resilience proxy, the budget-constrained optimization problem, and the ALE and ROSI indicators can support transparent comparison of alternatives. Their outputs remain conditional on the quality of estimates for threat frequency, loss, recovery, and control effectiveness and should therefore be accompanied by sensitivity analysis (Gordon & Loeb, 2002; Wang et al., 2020; NIST, 2025a, 2025b, 2025c).

At the same time, the proposed models should be regarded as a theoretical foundation rather than a complete methodology. Their practical application requires calibrated input data on threat probabilities, losses, and countermeasure effectiveness, the collection of which constitutes a separate methodological task, particularly under wartime conditions. In comparison with the NIST Risk Management Framework, the proposed framework does not replace system categorization, control selection, assessment, authorization, or monitoring; rather, it supplies optional analytical instruments for comparing control configurations within those governance stages. Its practical

contribution for Ukrainian authorities and critical-infrastructure operators lies in making assumptions, resource constraints, and residual-risk trade-offs explicit. At the same time, quantitative formalization may create an illusion of objectivity when threat probabilities, loss estimates, and control-effectiveness coefficients are weakly supported. Accordingly, expert elicitation, parameter validation, uncertainty ranges, and periodic recalibration are integral conditions of responsible use.

Limitations

This study has several limitations.

First, it relies primarily on regulatory documents, international standards, and academic publications. The formally prescribed provisions of the analysed documents may not fully correspond to actual administrative and technical practice in specific organizations.

Second, the numerical parameters of the proposed models, including threat probabilities, loss estimates, and countermeasure effectiveness coefficients, are treated analytically and are not calibrated against empirical incident data. The collection and validation of such data for the systems of the security and defence sector constitute a separate research task.

Third, the Markov model uses only two states and constant transition intensities. Real systems may require additional degraded or attack states, non-exponential transition distributions, time-varying rates, or semi-Markov formulations.

Fourth, the study does not include an empirical case study of the application of the proposed apparatus to a specific critical infrastructure facility. Incorporating such a case study would strengthen the empirical validation of the study's conclusions. Fifth, the framework does not explicitly model adversarial adaptation or strategic attacker behaviour; consequently, control-effectiveness estimates require periodic reassessment as threat actors modify their tactics, techniques, and procedures.

Conclusions

The evolution of the Ukrainian regulatory framework for technical information protection between 2021 and 2026 can be represented through three stages: institutional preparation in 2021 and wartime transition in 2022; harmonization with international standards in 2023; and implementation of a risk-oriented paradigm through ND TZI 3.6-006-24 in 2024 and Resolution No. 712 in 2025.

ND TZI 3.6-006-24 distinguishes four profile types—basic, sectoral, target, and adapted—while Resolution No. 712 regulates the governance of basic, sectoral, and target profiles and security authorization. For analytical purposes, a profile is represented as a combination of security and privacy requirements, selected measures, enhancements, organization-defined parameters, and mappings to current threats and risks. This representation is compatible at the methodological level with the tailoring logic of NIST SP 800-53 Rev. 5.

The principal theoretical result is an integrated analytical framework that links the regulatory structure of a security profile with normalized threat-coverage assessment, an availability-based resilience proxy, resource-constrained control selection, economic evaluation, verification, and authorization. The methodological result is the explicit formulation of assumptions, variables, constraints, and interpretation limits for each component. The practical value lies in improving the transparency and traceability of technical and budgetary decisions. The proposed indicators are not universal measures of protection: their validity depends on empirical calibration, documented assumptions, uncertainty analysis, and sensitivity testing for the particular information system.

Future research will be directed toward the development of methodologies for assessing the risks associated with individual protective measures and for the verification of security profiles, as

well as toward the empirical calibration of the proposed models using incident data from critical infrastructure systems.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

Use of Artificial Intelligence

Artificial intelligence was used for language editing, translation, and technical verification of the manuscript.

References

Administration of the State Service of Special Communications and Information Protection of Ukraine. (2024). *ND TZI 3.6-006-24: Procedure for selecting measures to protect information, the protection requirement for which is established by law and which does not constitute a state secret, for information systems* [In Ukrainian; author's translation]. https://cip.gov.ua/services/cm/api/attachment/download?id=66109

Bojanc, R., Jerman-Blažič, B., & Tekavčič, M. (2012). Managing the investment in information security technology by use of a quantitative modeling. *Information Processing & Management, 48*(6), 1031–1052. https://doi.org/10.1016/j.ipm.2012.01.001

Cabinet of Ministers of Ukraine. (2025). *Resolution No. 712 of June 18, 2025* [In Ukrainian]. https://zakon.rada.gov.ua/go/712-2025-%D0%BF

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM, 47*(7), 87–92. https://doi.org/10.1145/1005817.1005828

Dempsey, K., Chawla, N., Johnson, L., Johnston, R., Jones, A., Orebaugh, A., Scholl, M., & Stine, K. (2011). *Information security continuous monitoring (ISCM) for federal information systems and organizations* (NIST SP 800-137). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-137

Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2017). Resilience of cyber systems with over- and underregulation. *Risk Analysis, 37*(9), 1644–1651. https://doi.org/10.1111/risa.12729

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438–457. https://doi.org/10.1145/581271.581274

Hubbard, D. W., & Seiersen, R. (2016). *How to measure anything in cybersecurity risk*. Wiley.

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal, 4*(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

International Organization for Standardization. (2018). *ISO 31000:2018 risk management—Guidelines*.

International Organization for Standardization. (2022). *ISO/IEC 27005:2022 information security, cybersecurity and privacy protection—Guidance on managing information security risks*.

Joint Task Force. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (NIST SP 800-37 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2

Joint Task Force. (2020a). *Security and privacy controls for information systems and organizations* (NIST SP 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Joint Task Force. (2020b). *Control baselines for information systems and organizations* (NIST SP 800-53B). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53B

Joint Task Force. (2022). *Assessing security and privacy controls in information systems and organizations* (NIST SP 800-53A Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53Ar5

Joint Task Force Transformation Initiative. (2011). *Managing information security risk: Organization, mission, and information system view* (NIST SP 800-39). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-39

Kott, A., & Linkov, I. (Eds.). (2019). *Cyber resilience of systems and networks*. Springer. https://doi.org/10.1007/978-3-319-77492-3

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions, 33*(4), 471–476. https://doi.org/10.1007/s10669-013-9485-y

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (NIST SP 800-30 Rev. 1). https://doi.org/10.6028/NIST.SP.800-30r1

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

National Institute of Standards and Technology. (2025a). *Integrating cybersecurity and enterprise risk management* (NIST IR 8286 Rev. 1). https://doi.org/10.6028/NIST.IR.8286r1

National Institute of Standards and Technology. (2025b). *Identifying and estimating cybersecurity risk for enterprise risk management* (NIST IR 8286A Rev. 1). https://doi.org/10.6028/NIST.IR.8286Ar1

National Institute of Standards and Technology. (2025c). *Staging cybersecurity risks for enterprise risk management and governance oversight* (NIST IR 8286C Rev. 1). https://doi.org/10.6028/NIST.IR.8286Cr1

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST SP 800-61 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach* (NIST SP 800-160 Vol. 2 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)—A practical quantitative model. *Journal of Research and Practice in Information Technology, 38*(1), 45–56. https://doi.org/10.3316/informit.937199632104879

State Enterprise "UkrNDNC." (2023). *DSTU ISO/IEC 27001:2023 information security, cybersecurity and privacy protection—Information security management systems—Requirements (ISO/IEC 27001:2022, IDT)* [In Ukrainian].

Wang, J., Neil, M., & Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security, 89*, Article 101659. https://doi.org/10.1016/j.cose.2019.101659

Wheeler, E. (2011). *Security risk management: Building an information security risk management program from the ground up*. Syngress.

Yevseyeva, I., Basto-Fernandes, V., Emmerich, M., & van Moorsel, A. (2015). Selecting optimal subset of security controls. *Procedia Computer Science, 64*, 1035–1042. https://doi.org/10.1016/j.procs.2015.08.625

This is an open access journal and all published articles are licensed under a Creative Commons «Attribution» 4.0.