
TRANSFORMATION OF INTELLIGENCE ACTIVITIES IN CONTEMPORARY CONDITIONS

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: January 22, 2026 | **Revised:** March 05, 2026 | **Accepted:** March 31, 2026

DOI: <https://doi.org/10.33445/psssj.2025.7.1.4>

Abstract

The article examines the transformation of intelligence activities in the context of contemporary global security changes driven by intensified geopolitical competition, digitalization, and the impact of the full-scale war in Ukraine. The purpose of the article is to clarify the essence of intelligence activities under modern conditions and to identify the key directions of their transformation. The methodological framework is based on systemic, comparative, and structural-functional approaches, as well as methods of analysis and synthesis, which enabled a comprehensive assessment of the impact of current challenges on intelligence structures. It is substantiated that the modern security environment is characterized by increasing uncertainty, rapid information dissemination, and the growing complexity of strategic forecasting, which necessitates a revision of traditional approaches to intelligence activities. The key trends in shaping a new international security architecture are identified, including the strengthening role of the United States and China, the intensification of transnational threats, and the emergence of new formats of security alliances. The results of the study reveal the main directions of intelligence transformation: integration of artificial intelligence and big data technologies; use of autonomous systems and satellite-drone complexes; increased cooperation with the private sector; expansion of open-source intelligence; application of strategic declassification tools; development of partnership networks among intelligence agencies; investment in human capital and the formation of new competencies. It is demonstrated that modern intelligence is evolving into a complex, multidisciplinary system focused on integrating diverse data sources and supporting decision-making under time constraints. It is concluded that the transformation of intelligence activities is systemic in nature and encompasses organizational, technological, and cognitive dimensions, requiring the formation of a new paradigm capable of adequately responding to contemporary challenges and threats.

Key words: International Order, Security Space, Intelligence, Intelligence Activities, Intelligence Community, Intelligence Agencies, Homeland Security.

Introduction

The contemporary international security environment is characterized by a high level of dynamism, uncertainty, and nonlinearity of global processes. The full-scale war of the Russian Federation against Ukraine has become a catalyst for profound transformations in the system of international relations, accompanied by intensified geopolitical competition, fragmentation of the world order, and the growing role of new actors. Under these conditions, traditional approaches to ensuring national and international security prove insufficient, which актуалізує the need to reconsider the conceptual foundations of intelligence systems.

Intelligence activities, historically based on a combination of human and technical methods of information collection, are undergoing significant changes under the influence of digital transformation, the development of artificial intelligence, big data technologies, and open-source information. At the same time, the range of intelligence actors is expanding, particularly through

the involvement of the private sector and non-state actors, which transforms traditional views on the structure and functions of intelligence communities. Thus, modern intelligence is evolving into a complex, multidisciplinary system that integrates diverse sources of information and supports decision-making under conditions of limited time and high uncertainty.

The analysis of scientific research indicates a growing interest in the transformation of intelligence activities in the digital age and under conditions of strategic competition. Studies by both foreign and domestic scholars address the impact of artificial intelligence on intelligence, the role of big data in shaping analytical outputs, and the challenges of integrating different types of intelligence (HUMINT, SIGINT, OSINT, etc.). However, despite the significant body of research, insufficient attention has been paid to a comprehensive analysis of the transformation of intelligence activities specifically in the context of contemporary security challenges, which determines the relevance of this study.

The purpose of the article is to examine the essence and features of the transformation of intelligence activities in modern conditions, as well as to identify the key directions of their development, taking into account new technological and geopolitical factors. To achieve this goal, systemic, structural-functional, and comparative approaches are employed, enabling a comprehensive assessment of changes in the functioning of intelligence structures.

The scientific novelty of the study lies in the systematization of current trends in the transformation of intelligence activities and in substantiating the need to form a new intelligence paradigm that combines technological innovation, human capital development, and expanded international cooperation. The practical significance of the results lies in their potential application in shaping state policy in the field of national security and improving the functioning of intelligence agencies.

Thus, the study of the transformation of intelligence activities in contemporary conditions is an important scientific and applied task that significantly influences the effectiveness of ensuring state security in the face of growing global challenges and threats.

Analysis of Recent Studies and Publications

The theoretical and practical aspects of the legal and organizational foundations of intelligence activities have been examined across various fields of research.

In his article *The Coming Revolution in Intelligence*, Anthony Vinci, former Chief Technical Officer and Deputy Director of the U.S. National Geospatial-Intelligence Agency, outlines his views on the imminent transformation of intelligence. In *How Artificial Intelligence and Autonomous Systems Are Transforming Espionage* (2020), he notes that throughout human history there has been a persistent practice of intelligence activities aimed at obtaining information about the actions and intentions of others. The use of technological tools for observation, monitoring, and interception has always been an integral element of intelligence, although it has never replaced the human factor. At the same time, the development of artificial intelligence and autonomous systems is driving a paradigm shift: in the future, machines will be capable of monitoring other machines to determine their current activities and future intentions. Intelligence activities will continue to involve the acquisition and protection of information; however, the methods of its collection, analysis, and dissemination will undergo fundamental changes (Vinci, A., 2020).

The work *Intelligence Analysis in the Digital Age* (2021) (Stenslie, S., Haugom, L., & Vaage, H. (Eds.), 2021), within the framework of the “digital era” concept, highlights the increasing number of changes and complexities (in terms of “challenges–threats–risks”) affecting the speed of information dissemination. Modern technologies have reduced the time required for information transmission to nearly zero, leading to decision-making under increasingly unfavorable conditions, while the demand for timely, relevant, and reliable intelligence continues to grow. At the same time,

the time available for making adequate decisions is significantly reduced, complicating the development of effective policies in a highly volatile global environment.

Another contemporary challenge for intelligence and information management is the problem of “big data” formed within a diffuse and multipolar world. In the publication *Big Data, New Technologies and Intelligence: Undermining Homeland Security* (2024) (Hammond-Errey, M., 2024), M. Hammond-Errey argues that the emergence of big data is transforming both the production of intelligence knowledge and the relationship between intelligence communities and the public. Moreover, it challenges the separation between domestic and foreign intelligence, necessitating continuous transformation of the configuration of national intelligence communities.

The concept of “big data” is defined as the result of integrating information from multiple sources. As early as 2015, American analysts emphasized the diversity of data sources used in intelligence, including unmanned aerial vehicles (MQ1 Predator), hyperspectral sensors, remote sensing systems, signals intelligence (SIGINT), moving target indicator sensors, infrared sensors, and measurement and signature intelligence (MASINT). The “big data” paradigm is based not only on a multiplicity of sources but also on the integration of various intelligence disciplines, including SIGINT, MASINT, human intelligence (HUMINT), geospatial intelligence (GEOINT), and open-source intelligence (OSINT). Consequently, a key challenge remains the inability to fully move beyond traditional linear approaches to data collection and processing, which may lead to the devaluation of information, the emergence of “strategic surprises,” and, ultimately, intelligence failures.

Despite the significant body of scientific research on the place and role of special services at different stages of the development of international relations, the issue of intelligence activities in contemporary conditions requires further scholarly attention.

Data and Methods

The study of the transformation of intelligence activities in contemporary conditions is based on a comprehensive interdisciplinary approach that combines qualitative analytical methods with elements of comparative and systems analysis.

The empirical basis of the study includes: (1) strategic documents in the field of security and intelligence (in particular, national intelligence strategies of leading states); (2) analytical materials of international organizations and research centers; (3) scientific publications on the digitalization of intelligence, artificial intelligence, and big data; and (4) open-source information (OSINT) reflecting current trends in the development of technologies and practices of intelligence activities. Particular attention is paid to materials that characterize transformation processes in the context of the Russian-Ukrainian war and global geopolitical competition .

The methodological framework is based on the following methods:

- **systems approach** – to examine intelligence activities as an integrated multi-level system comprising organizational, technological, and cognitive components;
- **structural-functional analysis** – to identify changes in the functions and structure of intelligence agencies under the influence of contemporary challenges;
- **comparative method** – to compare approaches to intelligence transformation across different countries and international contexts;
- **methods of analysis and synthesis** – to generalize scientific approaches and form a comprehensive understanding of the evolution of intelligence activities;
- **content analysis** – to examine the content of strategic documents, academic works, and open sources regarding key trends in intelligence development;
- **elements of foresight analysis** – to assess the prospects for the development of intelligence activities in the context of technological change.

The research design involves the sequential identification of key factors driving the transformation of intelligence activities (technological, geopolitical, and organizational), their systematization, and the assessment of their impact on the effectiveness of intelligence structures. Particular emphasis is placed on the integration of different intelligence disciplines (HUMINT, SIGINT, OSINT, GEOINT) and the role of artificial intelligence in data processing and decision-support systems.

The limitations of the study are related to the predominant use of open-source information, which makes it impossible to fully account for classified aspects of intelligence activities. However, this limitation is mitigated by the use of a wide range of analytical and academic sources, allowing for a sufficiently representative understanding of current trends in the transformation of intelligence activities.

Results and Discussion

Thus, the following features of intelligence activities in contemporary conditions can be identified:

1. Introduction and application of new technologies and innovations.

The digital technological revolution has had a greater impact than the industrial revolution or the early use of atomic energy in its time. In this regard, the U.S. Central Intelligence Agency (CIA) has established a Special Technology Center that actively cooperates with the private IT sector and, for the first time in its history, introduced a new position — the Chief Technology Officer of the CIA.

One of the most revolutionary technologies for collecting military intelligence information today is the integration of unmanned aerial vehicles and satellites. The use of these innovative technologies has not only provided the Armed Forces with a number of significant strategic and tactical advantages but has also transformed the landscape of military intelligence. The introduction of modern algorithms has made it possible to analyze collected data in real time and, therefore, to detect threats on the battlefield more quickly and effectively.

For a considerable number of years, satellite technologies have played a pivotal role in intelligence activities. Satellites, which orbit at significant altitudes above the Earth's surface, are of paramount importance in modern warfare due to their ability to provide wide coverage, facilitate data collection, and enable efficient communication. The integration of drones and satellites for intelligence collection has marked a new era in the development of intelligence activities, characterized by synergy in this field.

The integration of artificial intelligence (AI)-based technologies has become a key element in the evolution of these systems, enabling the analysis of large volumes of data and the generation of valuable insights for management decision-making. The use of AI technologies in intelligence analysis facilitates the identification of potential threats, the mapping of adversary activities, and the assessment of the geopolitical situation, thereby enabling rapid and informed decision-making.

The main advantages of AI-based data analysis in intelligence include enhanced situational awareness, improved forecasting capabilities, and more accurate threat assessment. Defence intelligence systems can employ cognitive AI to support decision-making by military leadership, assisting in complex strategic planning and risk assessment. Cognitive computing can be applied in military intelligence in the following areas:

- natural language processing (NLP) — NLP algorithms can process textual data, enabling defence intelligence systems to extract information from large volumes of unstructured documents;
- artificial intelligence — AI-based virtual assistants help military leaders organize information, formulate queries, and make decisions in real time, saving valuable time in critical situations;
- scenario simulation — AI cognitive systems analyze various parameters and simulate the implementation of different scenarios, helping the Armed Forces predict outcomes and develop effective strategies.

The integration of AI with autonomous systems and robotics is leading to significant changes in intelligence activities. Among the most important advantages of introducing AI into autonomous systems are the following:

- they conduct visual surveillance, collect, and analyze data much more efficiently, minimizing risks to personnel;
- these systems can detect, track, and identify potential targets with greater accuracy, reducing the likelihood of unintended damage to civilian infrastructure;
- autonomous systems equipped with AI optimize logistics and supply chains, ensuring the timely delivery of resources to the battlefield.

2. Cooperation with the private sector and the use of social networks.

Today, new technologies allow non-state actors and individuals to collect and analyze intelligence sometimes more effectively and faster than government agencies. Commercial entities launch hundreds of satellites every year. More than half of the world's population is online, producing and receiving open-source intelligence, often without being aware of it. According to a 2019 World Economic Forum report, Internet users post about 500 million tweets on Twitter and 350 million photos on Facebook every day (Private eyes in the sky; Spies, lies, and algorithms).

In particular, the CIA has established a unit focused on building partnerships with the private (non-governmental) sector in order to obtain innovations that provide a competitive advantage.

In addition, social networks are actively used. Thus, as part of countering Russia, U.S. intelligence services have intensified their recruitment efforts (in particular, through the use of the Telegram platform) among Russian citizens dissatisfied with the Kremlin's policies.

3. Controlled disclosure of sensitive information.

"Strategic declassification" — the deliberate public disclosure of certain secrets in order to undermine competitors and rally allies — has become a powerful political tool. Its use does not imply reckless endangerment of sources or methods of obtaining intelligence information but rather a deliberate resistance to the reflexive desire to keep everything secret.

4. Partnerships and personal contacts with representatives of intelligence services of other countries.

Personal contacts and partnerships represent a form of "intelligence diplomacy" that contributes to bringing interests closer together and supports the efforts of politicians and diplomats in achieving desired outcomes.

These meetings are an important means of preventing unnecessary misunderstandings and unintended clashes, and they complement and support policy-making channels, including contacts between heads of state.

5. Investment in human capital (personnel of the intelligence community).

Professional training of personnel is becoming increasingly important in modern conditions and is a key factor in enhancing the effectiveness of intelligence agencies.

It is necessary to attract and retain technological talent, improve compensation systems, and encourage more flexible career models that allow officers to move to the private sector and return.

It should be noted that, according to the Office of the Director of National Intelligence, of more than 165 vacancies (as of autumn 2024), a significant number (with the exception of doctors, lawyers, and translators) were oriented toward specialists capable of working directly in the intelligence field. A detailed analysis of positions and corresponding responsibilities defined by the CIA makes it possible to outline the requirements for candidates, including:

- possession of knowledge, abilities, and skills across various fields;
- lawyers must work "at the intersection of law and advanced technologies";
- methodologist-analysts must be able to develop methods for improving the accuracy of intelligence data analysis and collection using statistical, econometric, and mathematical

- techniques, as well as perform geospatial modeling;
- for certain professions (accountants, cartographers, polygraph examiners, case officers), a bachelor's degree is sufficient;
 - for higher-level positions, a master's or doctoral degree is required (including for analysts, biotechnologists, and lawyers with a Juris Doctor degree);
 - certain positions require a PhD;
 - multidisciplinary competencies (ability to collect data from multiple systems and develop analytical solutions);
 - analytical capabilities (a wide range of analytical positions);
 - strong scientific background;
 - proficiency in cutting-edge technologies (AI, augmented reality, etc.).

6. Budget.

Priorities are not realistic without adequate financial support.

Despite the revolution in digital technologies and the rapid development of technical intelligence, human intelligence (HUMINT) remains a priority, as there are always secrets that can only be obtained through human sources. This requires intelligence officers to undergo intensive training, work as a team, and possess significant creativity and a willingness to take risks.

These provisions are closely aligned with the U.S. National Intelligence Strategy (2023), which defines six key areas of development for the intelligence community.

Conclusions

The war in Ukraine has far-reaching consequences that not only transform the security architecture of Europe but also affect global geopolitics and geo-economics. The geostrategic position of the Russian Federation is deteriorating, as the war has prompted two previously non-aligned states—Finland and Sweden—to join NATO. The Russian invasion of Ukraine has clearly demonstrated that the risk of a large-scale war in Europe is increasing.

Analytical discourse and direct intelligence practices in Western countries indicate that modern intelligence is conceived as a complex, multidisciplinary, science-intensive process that requires the continuous transformation of “intelligence pedagogy” in order to train effective multidisciplinary specialists who are psychologically and physically resilient, scientifically and professionally capable of collecting, understanding, integrating, and transmitting data from multiple sources, as well as conducting strategic intelligence and forecasting (taking into account future challenges), relying on the multi-use capabilities of artificial intelligence, etc.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

References

- Vinci, A. (2020). *The coming revolution in intelligence*. *Foreign Affairs*. <https://www.foreignaffairs.com/articles/north-america/2020-08-31/coming-revolution-intelligence>
- Stenslie, S., Haugom, L., & Vaage, H. (Eds.). (2021). *Intelligence analysis in the digital age*. Routledge.
- Hammond-Errey, M. (2024). *Big data, emerging technologies and intelligence: National security disrupted*. Routledge.

Private eyes in the sky: How commercial satellites are transforming intelligence. (n.d.). *Foreign Affairs*. <https://www.foreignaffairs.com/world/private-eyes-sky>

Spies, lies, and algorithms: Why U.S. intelligence agencies must adapt or fail. (n.d.). *Foreign Affairs*. <https://www.foreignaffairs.com/united-states/spies-lies-and-algorithms>

Office of the Director of National Intelligence. (2023). *National intelligence strategy 2023*. <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2023/3713-2023-national-intelligence-strategy>