UDC 355.45:004.8

K. Tkachenko

S. Kravchenko

O. Novykova

APPLICATION OF ARTIFICIAL INTELLIGENCE IN INTELLIGENCE ACTIVITIES UNDER MODERN WARFARE CONDITIONS

The article examines the role of artificial intelligence (AI) in intelligence activities under modern warfare conditions. The capabilities of AI in the collection, processing, and analysis of intelligence information are analyzed, as well as its impact on decision-making processes in hybrid conflicts. Particular attention is paid to the application of machine learning algorithms and neural networks in tasks related to pattern recognition, threat forecasting, and the identification of correlations within large data sets. The main challenges associated with the implementation of AI in intelligence activities are highlighted, including issues of cybersecurity, resilience to information manipulation, and integration with electronic warfare systems. The necessity of a systematic approach to the use of AI in intelligence activities to ensure information superiority is substantiated.

Keywords: *intelligence, artificial intelligence, machine learning, intelligence data, data analysis, military intelligence.*

Statement of the problem. Modern armed conflicts are characterized by an information-saturated environment, high dynamics, and the extensive use of electronic warfare technologies and asymmetric threats. Intelligence operations, which play a key role in ensuring information superiority, face new challenges – the growing volume of data to be analyzed, the accelerating pace of decision-making, and the need to integrate intelligence results with command and control systems.

Traditional methods of information analysis no longer provide the necessary speed and efficiency for real-time decision-making. The use of artificial intelligence (AI) opens new possibilities for automating the processes of intelligence data collection and processing, improving the accuracy of enemy action forecasting, and developing intelligent decision-support systems for commanders. However, the process of implementing AI may also encounter a number of challenges – ranging from technical ones, such as algorithm resilience under interference, to ethical and legal issues related to the use of autonomous systems.

Given the rapid evolution of technologies and their growing impact on modern conflicts, there is a clear need for a systematic analysis not only of the opportunities that arise from the use of AI in intelligence operations, but also of the potential problems related to it. In this context, it is particularly relevant to study the practical experience of applying such technologies in contemporary wars, especially in light of events of recent years.

Analysis of recent research and publications. The issue of applying artificial intelligence in the military domain has been actively examined by both domestic and foreign researchers. Article [1] substantiates the feasibility of using machine learning algorithms to enhance the accuracy and speed of military data processing.

In study [2], the authors emphasize the risks and threats associated with the integration of intelligent technologies into military systems, particularly ethical and legal aspects.

Foreign research devotes significant attention to the practical aspects of AI implementation. Article [3] published on the IEEE Xplore platform analyzes U.S. and EU defense projects in which AI is employed for intelligence data processing and threat forecasting.

Article [4] explores the transformation of strategies and tactics under the influence of AI, highlighting the risks of dual-use technologies and the need for close cooperation between the military and civilian sectors.

Particular attention should be paid to the analytical report [5], which examines the development of Ukrainian systems featuring autonomous capabilities, primarily in the fields of unmanned technologies and situational awareness.

The authors of publication [6] analyze current trends in the use of AI for automating target recognition, image processing, and the integration of intelligence data streams – areas directly related to the information support of combat operations.

A separate line of research addresses the role of AI in military communications. Article [7] discusses the prospects for employing machine learning algorithms in tactical networks, particularly for adaptive communication channel management and enhancing the resilience of information exchange.

Theoretical foundations of the organizational and ethical challenges of using AI in combat systems are presented in study [8], where the authors examine the balance between algorithmic autonomy and human control.

Thus, contemporary Ukrainian and foreign studies demonstrate a wide range of approaches to exploring the military applications of AI – from technical and legal aspects to analyses of specific defense projects and ethical constraints. However, none of the reviewed works provide a systematic examination of AI application specifically in intelligence activities under modern warfare conditions, which defines the relevance of the present article.

The purpose of the article is to conduct a comprehensive study of the role of artificial intelligence in intelligence operations during modern warfare.

Summary of the main material. Intelligence activity has always been one of the key elements in supporting military operations; however, in the 21st century, its significance has risen to the level of a strategic factor that directly determines the success or failure of armed confrontation for either side. Whereas the primary goal of intelligence used to be obtaining information about the enemy's forces and intentions for operational planning, modern wars, particularly those of a hybrid nature, require multidimensional, continuous, and highly accurate information support.

A distinctive feature of contemporary armed conflicts is the dramatic increase in data volume arriving from diverse sources – technical sensors, satellite systems, unmanned aerial vehicles (UAVs), electronic intelligence, open-source information (OSINT), and human intelligence networks. This creates the problem of "information overload," where the amount of incoming data far exceeds human capacity for timely analysis.

At the same time, the nature of modern warfare is characterized by rapid change: the tactical situation on the battlefield can shift within minutes. This demands that intelligence not only collect information but also process it swiftly and produce conclusions in real time. Traditional methods based on manual analytical work lose efficiency under such conditions, as they do not ensure the timeliness of decision-making.

Moreover, modern intelligence faces an adversary that actively employs a wide range of camouflage, deception, and electronic warfare measures. This complicates the detection of key indicators of enemy activity, increases demands on the accuracy of analytical assessments, and challenges the resilience of intelligence systems in the information environment.

Thus, intelligence as a whole becomes a highly complex, integrated system that cannot function effectively without automation of information collection and analysis processes. Under these conditions, the possibility of using artificial intelligence (AI) becomes increasingly relevant to ensure the speed, accuracy, and adaptability of intelligence activities.

Modern intelligence is characterized by the multichannel nature of its information sources, among which technical surveillance means play a leading role. The use of AI significantly expands data collection capabilities, allowing for automation of signal, image, and text processing and improving the efficiency of early-warning and threat-detection systems.

One of the key areas of AI application is the processing of satellite imagery and aerial photographs from unmanned aerial vehicles (UAVs). Today, computer vision algorithms can automatically detect military equipment, fortifications, troop movements, and other objects of interest – even under conditions of partial concealment or low image quality. This substantially reduces the time between data acquisition and its use in the decision-making process.

Equally important is the use of AI in the field of signals intelligence (SIGINT) and electronic intelligence. Deep learning algorithms can identify various signal types, distinguish characteristic patterns in the enemy's communication systems, and detect atypical activities in the spectrum. This provides the basis for rapid localization of emission sources and potential identification of enemy command-and-control network structures.

Another important area is the automation of information collection from open sources (OSINT – Open Source Intelligence). AI makes it possible to analyze large volumes of text, photo, and video content from social networks, news portals, and other open resources in real time. The use of classification algorithms and natural language processing (NLP) allows for the detection of changes in the information environment, assessment of message reliability, and identification of potential sources of information leaks.

A crucial task for modern armed forces is creating distributed sensor networks that make it possible to integrate diverse information sources – from satellites and UAVs to ground-based sensors and cyber intelligence. In such systems, AI serves as a "filter" that reduces data redundancy, extracts relevant information, and transmits it to command centers for further analysis.

The application of AI in intelligence data collection significantly enhances the operational effectiveness of intelligence operations by reducing the time between object detection and analytical interpretation, decreasing the cognitive load on analysts, and improving the accuracy of threat detection.

However, the most valuable capability of AI lies not only in minimizing redundancy, thereby accelerating the detection of objects of interest, but also in processing and analyzing intelligence data. At this stage, command gains access to advanced technological tools that enable rapid and well-grounded decision-making.

Machine learning methods are among the most important tools, enabling data classification, pattern recognition, and information clustering. For example, algorithms can automatically identify groups of signals belonging to a single enemy communication system or establish correlations between equipment movement and changes in radio exchange patterns.

Neural networks and deep learning algorithms are used for image, voice, and text recognition. This enables, in particular, the tracking of unit movements from photo and video materials, the identification of key individuals in intercepted radio communications, and the analysis of informational content in social media posts.

A special role is played by the integration of heterogeneous information sources. Under modern conditions, the work of intelligence agencies relies on the comprehensive use of data from HUMINT (human intelligence), SIGINT (signals intelligence), GEOINT (geospatial intelligence), MASINT (measurement and signature intelligence), and OSINT (open-source intelligence). AI can integrate these datasets into a unified system, automatically eliminating duplication, identifying inconsistencies, and generating a coherent operational picture.

The use of natural language processing (NLP) algorithms opens new opportunities for working with large volumes of text data – from intercepted messages to vast collections of social media posts. This makes it possible not only to identify key topics and sentiments but also to detect indicators of enemy information and psychological operations.

Another promising area is the use of anomaly detection algorithms. These allow automatic identification of deviations from typical enemy behavior patterns – for example, sudden changes in supply routes or atypical activity in the radio spectrum. Such signals can serve as early indicators of operational preparation or the deployment of new capabilities.

Thus, AI serves as a powerful enabler in the field of intelligence data processing and analysis: it does not replace the analyst but significantly enhances analytical performance – particularly the ability to quickly identify key threats and make informed decisions. In this context, the importance of human–machine interaction increases: algorithms handle routine tasks, allowing decision-makers to focus on strategic interpretation of results. This, in turn, directly influences the quality of decisions made by the command.

Regarding AI application in forecasting and decision support, one of its most critical areas is predicting possible enemy actions and assisting commanders in decision-making. In modern warfare, where situations evolve rapidly, the timely anticipation of enemy intentions becomes crucial.

Through predictive analytics algorithms, AI can model potential scenarios of combat operations by combining historical and current intelligence data. This makes it possible to determine likely routes of enemy unit movements, forecast their logistical activities, and assess the probability of specific weapon employment under given conditions.

In intelligence operations, systems for modeling the operational environment are gaining increasing importance. These systems integrate data from various sources (SIGINT, GEOINT, OSINT, etc.) to create a comprehensive operational picture of the battlefield. AI algorithms in such systems can automatically identify vulnerabilities in enemy formations, predict the consequences of their tactical maneuvers, and suggest possible courses of action.

The use of multi-agent systems, in which virtual “agents” simulate the behavior of military units under different scenarios, allows for rapid assessment of the effectiveness of potential decisions and the determination of the optimal strategy in a specific operational environment.

Decision Support Systems (DSS) based on AI play a distinct role by providing commanders and staff with analytical insights in a clear and visualized format. This reduces time for situation assessment, minimizes the risk of human error, and enables proactive action.

It is important to emphasize that AI in forecasting and decision support does not replace the military commander; rather, it functions as an intelligent assistant. It offers courses of action, but the final decision remains with the human, ensuring a balance between the speed of algorithmic analysis and the commander’s responsibility for combat outcomes.

Thus, the use of AI in forecasting and decision support provides a significant advantage in modern warfare, where analysis and response time are often measured in minutes – or even seconds.

However, despite its evident advantages, the use of AI in military operations may be accompanied by a number of challenges and limitations that must be addressed before its integration into combat practice. Examples of such challenges are outlined below.

Technical challenges and algorithm reliability. In real conditions, data are often incomplete, noisy, or deliberately distorted by the adversary. Machine learning algorithms that demonstrate high accuracy in laboratory settings may produce errors in combat environments. The reliability of AI performance directly depends on the quality of training datasets and the adaptability of models to unpredictable situations.

Vulnerability to information manipulation. The adversary may deliberately introduce disinformation into the information space or manipulate sensor inputs. This creates the risk of “data poisoning”, where the algorithm generates false conclusions. Additionally, adversarial attacks can be employed to deceive neural networks even through minimal alterations in input data.

Cybersecurity and system protection. The integration of AI into intelligence complexes requires a high level of cybersecurity. Attacks on the computing infrastructure may disrupt the operation of intelligence systems or lead to leaks of critical information. Therefore, the security of algorithms and communication channels is a top priority.

Ethical and legal aspects. The use of autonomous systems capable of making decisions without direct human involvement raises complex moral and legal issues. The question of accountability for the consequences of AI-assisted decisions remains open. There is also a risk of excessive automation, which could reduce the level of oversight by responsible personnel.

Dependence on the technological capacity of the state and its partners. Developing and implementing advanced AI-based systems requires significant resources, scientific and technical potential, and access to computing infrastructure. Countries lacking domestic developments in this field risk becoming dependent on external suppliers.

Thus, the integration of AI into military intelligence is a complex process that involves technical, organizational, legal, and ethical challenges. Overcoming these limitations is essential for the effective application of intelligent technologies in modern armed conflicts.

The future of military intelligence is directly linked to the further integration of AI technologies. Development trends indicate that in the coming years, AI will gradually become an integral part of multi-level data collection and analysis systems, forming the foundation for new forms of information warfare.

A promising direction involves the development of systems in which AI algorithms can not only analyze information on electromagnetic activity but also adaptively counteract enemy actions. In the field of cyber intelligence, AI can automatically detect anomalies in network traffic and forecast cyberattacks before they occur.

The intelligence of the future will involve the creation of unified information environments that integrate data from satellites, UAVs, sensor networks, social media, and cyberspace. AI will play a central role in this integration, ensuring automatic validation, cleansing, and unification of information.

International experience shows that the military structures of the United States, NATO, Israel, and other countries are actively developing directions for the application of AI in intelligence. For Ukraine, it is important to study this experience while simultaneously developing its own technologies adapted to the conditions of hybrid warfare and resource constraints. Particular importance should be given to strengthening cooperation with partners in data sharing, establishing joint research programs, and training qualified personnel.

Further research should address the resilience of algorithms to information attacks, the development of Explainable AI methods to enhance trust in such systems, as well as the creation of standards for security and ethical use of AI in the military domain.

Thus, future prospects point to the transformation of military intelligence into an integrated intelligent system, where humans and machines operate in close interaction. AI will become not merely a tool of automation but a key element in achieving information superiority in modern and future wars.

Conclusions

Intelligence activity in modern warfare is acquiring strategic significance, determining the ability of the armed forces to act proactively and ensure information superiority. Under these conditions, the use of artificial intelligence opens up new opportunities for data collection, processing, and analysis, threat forecasting, and decision-making support.

An analysis of scientific publications has shown that although the issue of implementing AI in the military domain is being actively studied, most works focus on general technical, legal, and ethical aspects. The specific area of applying AI in intelligence activities during modern armed conflicts remains insufficiently explored.

The main findings of the study indicate that AI can significantly enhance data collection efficiency through automated analysis of satellite and aerial imagery, communication signals, and open-source information.

The use of machine learning algorithms and neural networks makes it possible to integrate diverse information flows, thus forming a comprehensive picture of the operational situation.

In the field of forecasting and decision support, AI serves as an intelligent assistant capable of modeling enemy courses of action and proposing optimal response strategies.

At the same time, there are significant challenges: the technical reliability of algorithms, the risk of information manipulation, the need for cybersecurity, as well as legal and ethical issues related to the use of autonomous systems.

A promising direction for further research is the development of scientifically grounded approaches to the comprehensive implementation of artificial intelligence technologies within the military intelligence system. It is particularly advisable to explore the potential for integrating AI with automated command and control systems, electronic warfare, and cyber intelligence to create a unified information environment for situational awareness. Of special importance is the development of mathematical models for predicting enemy actions and assessing the intelligence situation using cognitive and hybrid machine learning approaches. For Ukraine, a crucial task is the advancement of domestic technologies in this field and the training of specialists capable of effectively employing intelligent systems in military intelligence.

Thus, the application of artificial intelligence in intelligence activities during modern warfare is not merely a technical innovation but a fundamental factor in transforming the entire system of military command and ensuring battlefield superiority.

References

1. Trofimenko O., Loginiva N., Sokolov A., Chikunov P., Ahmamatieva G. (2025). *Shtuchnyi intelekt u viiskovii sferi* [Artificial intelligence in the military sphere]. *Cybersecurity and Computer Technologies.* Borys Grinchenko Kyiv University. Retrieved from: https://surl.li/lsbdzc (accessed 10 July 2025) [in Ukrainian].

2. Gurjii S. (2025). *Tendentsii zastosuvannia tekhnolohii shtuchnoho intelektu u viiskovo-tekhnichnii sferi* [Trends in the use of artificial intelligence technologies in the military-technical field]. *Institute of Information Society Problems.* Retrieved from: https://surl.li/uhscoq (accessed 12 July 2025) [in Ukrainian].

3. Zhang Y., Dai Z., Zhang L., Wang Z., Chen L., and Zhou Y. (2021). *Application of Artificial Intelligence in Military: From Projects View.* IEEE Xplore Digital Library. Retrieved from: https://surl.li/epzoix (accessed 25 August 2025) [in English].

4. Atkinson R. (2024). Artificial Intelligence in Modern Warfare. Military Review. *U.S. Army University Press.* Retrieved from: https://surl.li/uahqij (accessed 5 June 2025) [in English].

5. Bondar K. (2024). Ukraine's Future Vision and Current Capabilities for AI-Enabled Autonomous Warfare. *Center for Strategic and International Studies (CSIS)*. Retrieved from: https://surl.li/kzyuct (accessed 17 May 2025) [in English].

6. Pusztaszeri A., Harding E. (2024). Technological Evolution on the Battlefield. *Center for Strategic and International Studies (CSIS).* Retrieved from: https://surl.li/igzrlt (accessed 20 August 2025) [in English].

7. Baeza V.M., Parada R., Salor L.C., Monzo C. (2025). AI-Driven Tactical Communications and Networking for Defense: A Survey and Emerging Trends. *arXiv.org.* Retrieved from: https://surl.li/yqjyxa (accessed 14 September 2025) [in English].

8. Feldman P., Dant A., Dreany H. (2024). War Elephants: Rethinking Combat AI and Human Oversight. *arXiv.org.* Retrieved from: https://surl.li/lrroel (accessed 3 September 2025) [in English].

The article was submitted to the editorial office on 26 September 2025

УДК 355.45:004.8

К. М. Ткаченко, С. О. Кравченко, О. О. Новикова

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У РОЗВІДУВАЛЬНІЙ ДІЯЛЬНОСТІ В УМОВАХ СУЧАСНОЇ ВІЙНИ

У статті досліджується роль штучного інтелекту (ШІ) у розвідувальній діяльності в умовах сучасної війни. Обґрунтовується, що стрімкий розвиток інформаційних технологій, зростання обсягів інформації і підвищена складність збройних конфліктів зумовлюють необхідність інтеграції алгоритмів машинного навчання та нейронних мереж у процеси збору, обробки й аналізу розвідувальної інформації. У дослідженні показано, що сучасна розвідка стикається з проблемою інформаційного перевантаження та потребою своєчасної інтерпретації різнорідних джерел даних – від супутникових знімків і сигналів радіоелектронної розвідки до відкритих джерел інформації та соціальних мереж. Застосування ШІ забезпечує автоматизоване виявлення об’єктів, класифікацію сигналів, аналіз текстових даних, а також інтеграцію інформації з різних напрямів розвідки (HUMINT, SIGINT, GEOINT, OSINT) у єдину оперативну картину. Особливу увагу приділено використанню предиктивної аналітики та мультиагентних моделей, які підтримують командирів у процесі ухвалення рішень, зокрема під час прогнозування дій противника. У статті окреслено основні виклики, що стримують широке впровадження ШІ: технічна надійність алгоритмів, ризики маніпуляцій і дезінформації, загрози кібербезпеці, а також правові та етичні обмеження. Підкреслено перспективи подальших досліджень у сфері розробки когнітивних систем, інтеграції ШІ із засобами радіоелектронної боротьби та кіберрозвідки, а також розвитку національних технологічних рішень в Україні. Наукова новизна дослідження полягає у зосередженні уваги саме на використанні ШІ у військовій розвідці, що дозволяє обґрунтувати його роль як вирішального інструмента досягнення інформаційної переваги в умовах сучасних війн. Практичне значення дослідження визначається створенням основ для розвитку інтелектуальних систем, які підвищують аналітичні спроможності військових структур і забезпечують ефективне управління військами в умовах високої динаміки бойових дій.

Ключові слова: *штучний інтелект, військова розвідка, сучасна війна, аналіз даних, прогнозування загроз, інформаційна перевага.*

Tkachenko Kyrylo – PhD, Deputy Head of the Department of Military Communications and Informatization, National Academy of the National Guard of Ukraine
https://orcid.org/ 0000-0001-7678-0363

Kravchenko Serhii – Candidate of Military Sciences, Associate Professor, Associate Professor of the Department of Land Forces, National University of Defense of Ukraine
https://orcid.org/0000-0001-8188-3113

Novykova Olena – Candidate of Technical Sciences, Associate Professor, Professor of the Department of Military Communications and Informatization, National Academy of the National Guard of Ukraine
https://orcid.org/0000-0003-3557-5210