INTEGRATION OF ARTIFICIAL INTELLIGENCE WITHIN INTELLIGENCE STRUCTURES

General (ret) Professor Teodor FRUNZETI, Ph.D*
(Academy of Romanian Scientists, 3 Ilfov, 050044, Bucharest, Romania, email: secretariat@aosr.ro)
Captain Ilie IFTIME, Ph.D Candidate**

Abstract: *One of the main current concerns of the global technology industry and academic environment is the improvement of artificial intelligence (AI) models and their integration into the multiple domains of society. In the case of national and international security, the drive to assimilate AI is also evident within intelligence structures, regardless of their form and specific profile (services, agencies, directorates, etc.), owing to the need to ensure primacy in the exploitation of new information by decision-makers, since „information is the world's most important and contested resource and timely data is the new oil"*[1].

Thus, this article aims to identify a series of capabilities that AI can provide within intelligence structures in an attempt to ensure informational advantage.

Keywords: *artificial intelligence, intelligence structures, intelligence cycle, multiple sources, intelligence analyst, informational advantage.*

DOI 10.56082/annalsarscimilit.2026.2.145

Introduction

The accelerated evolution of new technologies reaches its peak today through artificial intelligence. Although the concept emerged in the relatively distant past (for example, in John McCarthy and others, 1955, paper A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, where the hypothesis was advanced that a detailed description of the processes of intelligence could provide the starting point for simulating autonomous machine learning[2]), its rise in research and development was marked by two long periods of stagnation, or *„AI*

* Entitled Member of the Academy of Romanian Scientists, President of the Military Sciences Section, Doctoral Supervisor at "CAROL I" National Defense University, email: tfunzeti@gmail.com.

** "Carol I" National Defense University, Bucharest, Romania, email: andreiaalbu1@gmail.com.

[1] Rosenbach Eric, Mansted Katherin, *The geopolitics of information*, 2019, available at https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/Rosenbach_Commerce_Testimony_5March19_Final.pdf, p. 1, accessed on 13.06.2026.

[2] *** *A proposal for the darthmouth summer research project on artificial intelligence*, 1955, available at https://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html, accessed on june 13,2026.

winters" (the first from 1950 to 1980 due to the lack of computing power required to train AI models, and the second from 1980 to 2010 due initially to the absence of the internet and subsequently to insufficient digitalization, as the very object of study was missing-digital archives/the concept of Big Data).

At present, however, AI is becoming visible across all sectors of security: political, military, economic, social, and environmental. The appetite for its integration is increasing, from the micro level, where analysts use it to perform routine tasks, to the macro level, where major powers have established national strategies in this field and have even classified it as a national priority-for example, China. This versatile technology can relieve the human factor of a considerable amount of repetitive and administrative tasks, support analytical processes, and provide decision-making support.

Contemporary artificial intelligence is no longer merely at an experimental stage; rather, it is successfully integrated into an increasing number of intelligence systems, or is even updated and improved as new extensions of its capabilities emerge. The advantages of using AI technologies by intelligence structures are multiple: processing huge volumes of data in a very short time, accelerating the intelligence cycle and the OODA loop, enabling the real-time integration of multiple sources, augmenting the capabilities of intelligence officers, increasing the level of early warning by improving the ability to anticipate threats, preventing and countering the rapid evolution of online disinformation and propaganda, improving counterintelligence-specific activities, etc. In what follows, we will argue why these capabilities are important for intelligence structures and will illustrate them through successful models that have already been integrated.

1. Processing much larger volumes of data in a much shorter time (the main advantage of AI systems)

Whereas in the past intelligence services were confronted with a lack of information, today, in addition to the classical process of collecting the necessary data, they are confronted with an excess caused by the proliferation of sources (military and commercial databases, sensors, satellites, digital networks, social platforms, etc.) or by adversaries flooding the information space with false, redundant, duplicate, and other types of information. The analysis, filtering, and selection of the necessary information and its transformation into relevant intelligence products has become an increasingly difficult process to carry out solely by human analysts, regardless of the size of the team. Thus, the integration of certain artificial intelligence models, in order to take over various repetitive tasks, collect data, and conduct its initial processing at a faster pace, has become

more than necessary. The role of the human analyst is thereby redefined around tasks such as verification, interpretation, supplementation, validation, and contextualization.

In this regard, intelligence structures have created and refined various systems based on AI technologies that can operate with huge quantities of data in a very short time. Examples include Maxar and Planet Labs (in the geospatial domain, capable of analyzing terabytes of satellite imagery daily and identifying movements, positions, structures, etc. at the millisecond level)[3], Charlotte AI (in the cybersecurity domain; prevention and countering of attacks through the analysis of characteristics and their comparison with global indicators of compromise, being 75% faster than a specialized human team)[4], Real Time – Regional Gateway (an AI-enhanced system of the U.S. National Security Agency, used by intelligence services to store, integrate, and process billions of dispersed metadata items-calls, e-mails, digital ecosystems-with the purpose of faster target selection)[5], etc.

The processing of large volumes of data in a very short time has direct implications for the main activity of an intelligence structure, namely the conduct of the intelligence cycle by increasing its efficiency. The use of different specific AI systems can thus assist with or take over certain analytical tasks, and *„the stages can be carried out simultaneously, in real time, and not only in a distinct and sequential manner"*[6]. Furthermore, as a subsequent effect of the foregoing, the time required to complete the OODA loop (observe, orient, decide, act), developed by John Boyd, is also shortened. Nevertheless, although the acceleration of warfare and the compression of the decision-making process support the need to integrate AI at this level[7], in this case such integration is much more difficult to achieve than within the intelligence cycle, because the loop requires a

[3] **** Deep learning enables satellite-based monitoring of large populations of terrestrial mammals across heterogeneous landscape,* 2023, available at https://www.nature.com/-articles/s41467-023-38901-y, accessed on june 7, 2026.

[4] **** Accelerate security operations with generative AI*, 2024, available at https://www.-delltechnologies.com/asset/en-us/solutions/business-solutions/technical-support/crowdstrike-charlotte-ai-datasheet.pdf, accessed on 09.06.2026.

[5] Lyons Jessica, *'Four horsemen of cyber' look back on 2008 DoD IT breach that led to US Cyber Command*, 2024, available at https://www.theregister.com/special-features/2024/05/10/four-horsemen-of-cyber-recount-building-us-cyber-command/522406, accessed on 08.06.2026.

[6] Dudley Craig, Lessons from SABLE SPEAR: *The Application of an Artificial Intelligence Methodology in the Business of Intelligence*, published in *Studies in Intelligence*, vol. 65, no. 1, p. 12, available at https://www.cia.gov/resources/csi/static/ArticleSableSpear-ExperimentInAI.pdf, accessed on 06.06.2026.

[7] Johnson James, *Automating the OODA loop in the age of intelligent machines: reaffirming the role of humans in command-and-control decision-making in the digital age*, 2022, available at https://www.tandfonline.com/doi/full/10.1080/14702436.2022.2102486, accessed on 12.06.2026.

stronger presence of the human factor, especially in the last three stages. Strategic interpretation, contextualization, the understanding of ambiguities/uncertainties/non-linear situations and dynamic politico-military arrangements, etc., remain tasks assigned strictly to the human factor, at least for the time being.

2. More efficient integration of multiple sources

Some of the most important information is collected through open sources (OSINT). This section comprises a huge and diverse volume of data: press, mass media, databases from various fields, digital platforms, social networks, satellite imagery, photos/videos provided by CCTV cameras, etc. Analyzing these sources in real time and in a corroborated manner can be an almost impossible task for a team of analysts. In this respect, AI can process all of them in a very short time and, with the help of predefined algorithms, can identify reference elements/patterns.

An example of integration within OSINT is the OSIRIS platform, developed by the CIA's Open Source Enterprise in 2024 for the U.S. Intelligence Community. According to Jennifer Ewbank[8], its main role is not to provide intelligence products, but to help specialists more easily understand immense volumes of open-source data (triage, translation, transcription). With its help, analysis becomes more complex and faster, thinking becomes more refined, assumptions are questioned, and the analysis of alternative scenarios becomes more comprehensive.

The main models involved are Large Language Models (so that as much data generated in various foreign languages as possible can be incorporated), Machine Learning (to understand the context in which the respective information was released, the correlations between it, and to interpret user queries increasingly accurately), and generative AI (to provide the requested product in the desired form).

As illustrated above, artificial intelligence is increasingly used in the analysis of huge volumes of data collected through various methods used by intelligence structures: OSINT, HUMINT, SIGINT, GEOINT, IMINT, etc. Each domain has optimized this process through various AI models. The element of novelty, however, lies in the attempts to generate increasingly comprehensive intelligence products by harmonizing and unifying[9] all these

[8] Ewbank Jennifer, *The Role of Artificial Intelligence in the U.S. Intelligence Community: Current Uses and Future Developments*, 2024, available at https://www.-aspeninstitute.org/wp-content/uploads/2024/10/Ewbank_Role-of-AI-in-USIC_Final.pdf, accessed on 06.06.2026.

[9] Brown Charlotte, *Signal in Sync: OSINT, HUMINT, SIGINT, GEOINT in the modern intelligence environment*, 2025, available at https://mattermost.com/blog/signals-in-sync-modern-intelligence-environment/, accessed on 02.06.2026.

data specific to each domain into comprehensive information capable of highlighting overall, truthful, reliable, and real-time pictures.

Depending on the needs of the beneficiary intelligence structure, various such sources may be combined and unitary architectures may be formed. For example, in the case of maritime monitoring[10], GEOINT-type data (radar satellites that define the type of vessel, direction, and speed), OSINT (data uploaded by vessels/operators to different platforms as a result of traffic obligations), and SIGINT (intercepted radio communications) can be operated by AI software simultaneously and in real time (examples: Palantir Foundry/Gotham Maritime[11]). Thus, *"dark vessel"* actions (the intentional shutdown of a vessel's own localization systems in order to evade tracking by international authorities) can be countered. Another example is the Ukrainian project Eyes on Russia[12], whose AI algorithms integrate IMINT, OSINT, and GEOINT data in order to map the results of the contemporary war in this region.

The final desideratum in integrating multiple data sources is the creation of a mobile and robust AI architecture capable of incorporating all these structures simultaneously in order to respond to queries from various domains. This, however, is limited by the large resources required (especially technological ones), by information systems that are not interconnected across borders (the absence of membership in international organizations/communities), and by actors' internal/external policies (*"closed"* regimes).

3. Augmenting intelligence officers

The evolution of the professional capabilities of intelligence officers at present can also be achieved by assimilating new methods and means of collecting and analyzing information with the help of artificial intelligence. This direction of modernization for intelligence services should be a priority in the current context of the rapid evolution of technologies. AI should not be viewed as a super-technology intended to replace the human factor, but as the most efficient tool currently available. The better the intelligence analyst learns to work with it, the greater the increase in the quality of intelligence products will be.

---

[10] Navulur Kumar, *Data fusion and the future of geospatial intelligence*, 2025, available at https://synspective.com/blogs/2025/kumar_blog1/, accessed on 05.06.2026.

[11] *** *A Brief Analysis of Palantir Gotham: A Collaborative and Interactive Big Data Visualization Analysis Software Based on Dynamic Ontology*, 2024, accessed on 03.06.2026.

[12] Kotaridis Ioannis, *Integrating Earth observation IMINT with OSINT data to create added-value multisource intelligence information: A case study of the Ukraine–Russia war*, 2023, available at https://securityanddefence.pl/Integrating-Earth-observation-IMINT-with-OSINT-data-to-create-added-value-multisource,170901,0,2.html, accessed on 09.06.2026.

The concept of human-AI teaming appears increasingly often in the specialized literature. Perfect synergy between these two entities can be achieved when the technological component reaches considerable algorithmic performance, developed over time on the basis of prior training (integration of multiple sources, understanding of reasoning, intentions, and query formats, etc.). Effective collaboration within this binomial means exceeding any individual human or technological capacity. Why is this binomial necessary? Because the technological component cannot evolve on its own to such a level, since to date the human ethical and moral component has been attributed to it only in certain particular and limited ways. This *"last frontier"*[13] is very difficult to overcome, because AI would have to possess consciousness and a soul.

For the moment, the working spectrum of this hybrid team is limited only by present technological developments. Nevertheless, integration has occurred at all levels of an organization (planning, decision-making, execution, etc.) and can be observed in simple work frameworks (performing repetitive/administrative tasks) or complex ones (strategic analysis, designing scenarios, predictions, and supporting decision-making). If the artificial intelligence system can support the fulfillment of analytical tasks and even decision-making in various ways, the human factor retains a series of attributes that cannot be shared with the technological component: responsibility, ethics, moral intuition, complete contextual judgment, the legitimacy of action, supreme authority (AI can have only procedural authority), meta-coordination (although AI excels at executing structured tasks at scale, the adaptation and coordination of internal actions remain at a low level), and critical decision-making[14].

Some actors on the international stage are already implementing this concept within their own intelligence structures. For example, the United Kingdom's GCHQ (Government Communications Headquarters) introduced the Augmented Intelligence System[15] to support intelligence officers in managing the growing volume and complexity of data and information so as to improve the speed and quality of decisions. Similarly, in the case of Chinese military intelligence, the Generative Artificial Intelligence Large

[13] Siteanu Eugen, Frunzeti Teodor, Coșereanu Liviu, *Artificial Intelligence – From technological hopes to ethical concerns*, 2023, available at https://www.researchgate.net/-publication/367067594_Artificial_Intelligence_-_From_Technological_Hopes_to_Ethical_Concerns, accessed on june 08,2026.

[14] *** *Toward a science of human–AI teaming for decision making: A complementarity framework*, 2026, published in *Oxford Academic – Pnas Nexus*, vol. 5, available at https://academic.oup.com/pnasnexus/article/5/3/pgag030/8490283, accessed on 10.09.2026.

[15] *** *Pioneering a New National Security – The ethics of artificial Intelligence*, 2021, available at https://www.gchq.gov.uk/artificial-intelligence/index.html, accessed on june 04, 2026.

Model Online Monitoring and Early Warning System[16], developed by NORINCO Group (a state-owned company), may be mentioned. It is capable of monitoring large quantities of online data, fusing them with other internal data, analyzing them, and supporting the human factor in validating, interpreting, and integrating the information necessary for the decision-making process. It was developed by training the LLM with a huge amount of data from the "-INT" spectrum (OSINT, GEOINT, HUMINT, etc.). This model provides the analyst with a highly refined AI tool (multi-source information and important historical data).

4. Increasing the level of early warning by improving the ability to anticipate threats

Preventing strategic surprise is one of the objectives of any intelligence structure. In this respect, artificial intelligence plays a particularly important role in drafting situational awareness reports based on continuous scanning of the security environment, identifying indicators specific to threats, determining abnormal situations in the various sectors of security, correlating certain data and information, etc.

The responsibility of intelligence analysts in this case is to evaluate and validate the alerts produced by these AI systems, since errors may occur as a result of insufficient historical data required for prior algorithm training, the emergence of new situations/behaviors that may be misinterpreted, or even adversary interference, either directly (cyberattacks aimed at taking control of and manipulating the system) or indirectly (flooding the online environment with erroneous information, carrying out deceptive maneuvers/diversions in the physical domain) against them. In this case, a situational awareness AI system can eliminate certain human biases (emotional predispositions, support for certain hypotheses while ignoring contrary evidence, failure to integrate all sources, fatigue, pressure, etc.), but it can also create specific biases due to the circumstances mentioned above.

An illustrative example of the above is the implementation of artificial intelligence within the Zero Trust policy proposed by the Office of the Director of National Intelligence (ODNI) in the United States. Within the security architecture, AI is implemented across all processes:[17] joint analysis of the global context, outlining the user's historical behavior,

[16] Haver Zoe, *Artificial Eyes: Generative AI in China's Military Intelligence*, 2025, available at https://assets.recordedfuture.com/insikt-report-pdfs/2025/ta-cn-2025-0617.pdf, accessed on june 04, 2026.

[17] Ajish Deepa, *The significance of artificial intelligence in zero trust technologies: a comprehensive review*, published in *Journal of Electrical System and Inf Technology*, vol. 11, 2024, available at https://link.springer.com/article/10.1186/s43067-024-00155-z, accessed on june 03, 2026.

assessing the operating parameters of the device, calculating the dynamic score, providing decision-making support regarding the granting/blocking of access, etc. Through all these measures and more, the speed of the system increases, as does the efficiency of preventing and countering cyberattacks.

5. Preventing and countering the rapid evolution of online disinformation and propaganda

The digital environment is becoming an increasingly important battlefield for capturing the public's attention and influencing its perceptions, attitudes, and behaviors. Through the phenomenon of radicalization, society becomes polarized, institutional trust declines, and democratic processes are called into question. Certain artificial intelligence models can be exploited in this respect by intelligence structures through their integration into software for monitoring, detecting, and analyzing online social platforms and other digital environments. Coordinated disinformation campaigns conducted by various hostile actors can thus be identified more easily because specific AI technologies can monitor a much broader space and generate alerts in a much shorter time.

The imperative for intelligence structures to assimilate these technologies stems from the fact that adversaries are already operating with them for offensive purposes. Propaganda activities are carried out by these actors on a very large scale, incorporating large language models[18] that adapt content according to the target audience and its characteristics. Thus, similar narratives have been observed spreading across the territories of several states. In this respect, intelligence structures can monitor: the coordination of certain news platforms, the propagation of narrative patterns, the activation of certain account networks and the increase in their activity (anti-EU/NATO, conspiratorial messages) before important events (elections, summits, forums), etc.

An example of an artificial intelligence-based capability that can identify, counter, and attribute coordinated disinformation and propaganda is represented by the SemaFor (Semantic Forensics) technologies[19] developed by the U.S. DARPA (Defense Advanced Research Projects Agency) on the basis of an academic-industrial partnership. The public presentation of the advantages of these technologies took place during the international DEF CON 32 conference in 2024.

Moreover, these software systems may also incorporate a series of automatic rapid response mechanisms that label the fake news in question

[18] *** *LLMs as information warriors? Auditing how LLM-powered chatbots tackle disinformation about Russia's war in Ukraine*, 2024, available at https://arxiv.-org/pdf/2409.10697, accessed on june 02, 2026.

[19] *** *SemaFor program from DARPA,* 2024, available at https://www.semaforprogram.-com/analytic-catalog, accessed on june 11, 2026.

and immediately provide correct information from reliable sources, so that, until the decision-maker adopts certain positions and takes measures, the public is warned that the respective information is erroneous.

6. Improving activities specific to the counterintelligence domain

The phenomenon of digitalization entails, among other things, the storage/migration of data and information into digital databases. Protecting them becomes an increasingly difficult task as their volume and importance grow, and as infrastructure expands and becomes interoperable with that of other actors. In this respect, software based on artificial intelligence can carry out preventive actions by monitoring and signaling unusual behaviors of information networks, atypical migrations of files, the export of data in small quantities but over the long term, suspicious access to databases, the suspicious deletion of documents, increased interest in certain information, amplified communications traffic between various entities, etc.; or it can even undertake countermeasures, for example by blocking cyberattacks and automating the response to the respective IT incident.

Constant supervision of personnel who have access to certain databases and of their activity also remains a very important task. Espionage and sabotage actions are based primarily on the recruitment of sources who have access to these databases. Therefore, security checks carried out with the help of artificial intelligence transform the process from a periodic/occasional and reactive one into a continuous and predictive one. Moreover, many more subjects can be analyzed simultaneously than a classical security team could manage.

Thus, data relating to an individual's profile, relational circle (declared and undeclared), behavioral changes (significant fluctuations in discourse, attitudes, emotions, and actions), and financial risk (a high risk generated by contracted loans, various financial problems, etc., may facilitate corruption and blackmail) can be identified and analyzed automatically and in real time. In this respect, systems enhanced with AI models have been developed, such as UAM (user activity monitoring), responsible for recording, storing, and selecting data, and UEBA (user and entity behavior analytics), used for the analytical component, which compares a predefined *"normal profile/history"* model with each user's subsequent actions. The system identifies precisely those weak indicators that, taken separately, mean nothing, but which, when correlated, signal unusual behavior.

These types of systems are specific to each institution, being trained on the basis of internal rules as well as the classical behavior of an employee (the hours at which the platform is accessed, locations, temporal indicators, the volume and flows of data being operated, usual queries, etc.). In this case as well, the final decision regarding the labeling of a person as a

"security risk" still belongs to the human factor, since *"false positive"* situations may arise (a personal event, such as a death in the family, generating certain negative emotional and behavioral states, may be misinterpreted by AI).

Nevertheless, entities in the intelligence field pay particular attention to these types of systems, integrating and constantly modernizing them, as in the case of the FBI's contracting of the Insider Threat Management Suite for UAM/UEBA Capabilities[20] from the company Everfox in December 2025. The new system supports intelligence activity, the protection of classified information, and counterintelligence.

Conclusions

The migration of data and information from physical media to digital environments, as well as the accelerated increase in the complexity of the relationships among them, have led to the need to process increasingly large volumes of data in the shortest possible time. Within intelligence structures, this capability is sometimes translated into the need to ensure a real-time overall picture based on multiple sources. Informational advantage can be ensured only through complete and timely information, and systems based on artificial intelligence are becoming one of the most reliable tools currently used in this respect.

At the same time, contemporary society is increasingly characterized by a framework suffocated by the multitude of data surrounding us. Identifying the necessary, truthful, and timely information is becoming an increasingly difficult task in a space flooded with redundant information, duplicates in different forms, fake news, and constant disinformation and propaganda campaigns. Artificial intelligence can be used in this respect for both offensive and defensive purposes. Intelligence structures must remain aware of the adversary's intentions and actions and develop/improve capabilities to prevent and counter them.

The spectrum of AI integration is broad, ranging from the automation of simple administrative/repetitive tasks in order to relieve the human factor of simple duties and accelerate the workflow, to the performance of extended analytical processes, and up to the provision of support to the decision-maker through complex information (scenarios, strategies, forecasts, etc.). Within this range, the augmentation of the intelligence officer with these various technological abilities must be a natural (learning/performance) and constant process.

In various domains, the human–AI working binomial appears as one of the most efficient current models of symbiosis. While the technological

[20] **** Contract for the acquisition of "Insider Threat Management Suite for UAM/UEBA Capabilities" by the FBI*, 2025, available at https://www.highergov.com/contract/-15F06726P0000116/, accessed on june 10, 2026.

component represented by artificial intelligence contributes through the unprecedented scale of data analysis and the speed with which this is achieved, the human component completes the structure with exclusive characteristics such as intuition, contextualization, ethical and moral choices, and the capacity to react correctly when unpredictable situations occur, etc.

Therefore, nowadays actors no longer question the efficiency of AI, but rather its immediate yet responsible integration. Nevertheless, the characteristic of responsibility outlines an unfair competitive framework among actors, because the process of collecting, storing, and using data is subject to different legislation when comparing a democratic state with an authoritarian regime. This rivalry is also felt at the level of intelligence structures, which are pressured to deliver quality intelligence products as quickly as possible. Whoever first obtains and exploits certain information can gain significant advantages in an increasingly dynamic, volatile, and competitive security environment. Thus, today we are witnessing an "algorithmic arms race," which is no longer merely a concept situated at the boundary between theory and practice, but a fact.

BIBLIOGRAPHY

*** LLMs as information warriors? Auditing how LLM-powered chatbots tackle disinformation about Russia's war in Ukraine, 2024, available at https://arxiv.org/pdf/2409.10697;

*** SemaFor program from DARPA, 2024, available at https://-www.¬semaforprogram.-com/analytic-catalog;

*** Contract for the acquisition of "Insider Threat Management Suite for UAM/UEBA Capabilities" by the FBI, 2025, available at https://www.highergov.com/contract/15F06726P0000116/;

*** A proposal for the darthmouth summer research project on artificial intelligence, 1955, available at https://www-formal.stanford.edu/-jmc/history/dartmouth/dartmouth.html;

*** *Deep learning enables satellite-based monitoring of large populations of terrestrial mammals across heterogeneous landscape, 2023,* available at https://www.nature.com/articles/s41467-023-38901-y;

*** Accelerate security operations with generative AI, 2024, available at https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/technical-support/crowdstrike-charlotte-ai-datasheet.pdf;

*** A Brief Analysis of Palantir Gotham: A Collaborative and Interactive Big Data Visualization Analysis Software Based on Dynamic Ontology, 2024;

*** Toward a science of human–AI teaming for decision making: A complementarity framework, 2026, published in Oxford Academic – Pnas Nexus, vol. 5, available at https://academic.oup.com/-pnasnexus/article/5/3/pgag030/8490283;

*** Pioneering a New National Security – The ethics of artificial Intelligence, 2021, available at https://www.gchq.gov.uk/artificial-intelligence/index.html;

AJISH D., The significance of artificial intelligence in zero trust technologies: a comprehensive review, published in Journal of Electrical System and Inf Technology, vol. 11, 2024, available at https://link.springer.com/article/10.1186/s43067-024-00155-z;

BROWN C., Signal in Sync: OSINT, HUMINT, SIGINT, GEOINT in the modern intelligence environment, 2025, available at https://mattermost.com/blog/signals-in-sync-modern-intelligence-environment/;

DUDLEY C., Lessons from SABLE SPEAR: The Application of an Artificial Intelligence Methodology in the Business of Intelligence, published in Studies in Intelligence, vol. 65, no. 1, available at https://-www.cia.gov/resources/csi/static/ArticleSableSpearExperimentInAI.pdf;

EWBANK J., The Role of Artificial Intelligence in the U.S. Intelligence Community: Current Uses and Future Developments, 2024, available at https://www.aspeninstitute.org/wp-content/uploads/2024/10/Ewbank_Role-of-AI-in-USIC_Final.pdf;

HAVER Z., Artificial Eyes: Generative AI in China's Military Intelligence, 2025, available at https://assets.recordedfuture.com/insikt-report-pdfs/2025/ta-cn-2025-0617.pdf;

JOHNSON J., Automating the OODA loop in the age of intelligent machines: reaffirming the role of humans in command-and-control decision-making in the digital age, 2022, available at https://www.-tandfonline.com/doi/full/10.1080/14702436.2022.2102486;

KOTARIDIS I., Integrating Earth observation IMINT with OSINT data to create added-value multisource intelligence information: A case study of the Ukraine–Russia war, 2023, available at https://securityanddefence.pl/Integrating-Earth-observation-IMINT-with-OSINT-data-to-create-added-value-multisource,170901,0,2.html;

LYONS J., 'Four horsemen of cyber' look back on 2008 DoD IT breach that led to US Cyber Command, 2024, available at https://www.-

theregister.com/special-features/2024/05/10/four-horsemen-of-cyber-recount-building-us-cyber-command/522406;

NAVULUR K., Data fusion and the future of geospatial intelligence, 2025, available at https://synspective.com/blogs/2025/kumar_blog1/;

ROSENBACH E., MANSTED K., The geopolitics of information, 2019, available at https://www.belfercenter.org/sites/default/files/-pantheon_files/files/publication/Rosenbach_Commerce_-Testimony_5March19_Final.pdf;

SITEANU E., FRUNZETI T., COȘEREANU L., Artificial Intelligence – From technological hopes to ethical concerns, 2023, available at https://www.researchgate.net/publication/367067594_Artificial_Intelligence_-_From_Technological_Hopes_to_Ethical_Concerns;