DOI: 10.53477/1842-9904-25-36

THE IMPACT OF EMERGING TECHNOLOGIES ON INTELLIGENCE ANALYSIS

Răzvan-Georgian ZMĂDU*

Intelligence agencies have aligned with armed forces through the adoption of emerging technologies in their current operations. However, there is limited understanding of how artificial intelligence (AI) and Big Data modify the intelligence cycle and analytical process, particularly the redefinition of the human analyst's role in the context of technology integration. This article adopts a socio-technical perspective to examine the interaction between emerging technologies and intelligence analysis, by addressing how technology use reconfigures the human analyst's role through their repositioning within hybrid human-machine teams as the dominant working model.

Through the use of bibliometric analysis and systematic literature review, research trends were examined and findings regarding the technological impact on the analytical process and the interaction between technology and human operators within it were synthesised. The research results show that emerging technologies are leading to complex, comprehensive data automation and patter detection, but human judgment remains essential in the decision-making process.

The future of the intelligence analysis depends on the partnership between humans and machines, and achieving this will reconfigure analytical workflows, update doctrinal frameworks and operating procedures, and develop new skills to facilitate the effective integration of technical capabilities with human expertise.

Keywords: *intelligence analysis; artificial intelligence; intelligence services; technology; Human-Machine Teaming.*

* ***Răzvan-Georgian ZMĂDU is a PhD Student at the National Defence University "Carol I", Bucharest, Romania. He is deeply interested in artificial intelligence, machine learning, communication and computer networking. His main field of research is the influence of emerging technologies on military actions. E-mail: zmadu@hotmail.com***

Introduction

The current security environment is characterised by profound transformations, with state and non-state actors contesting informational supremacy by exploiting emerging technologies. In this context, AI, Big Data, and more recently LLMs (Large Language Models) have provoked a paradigm shift in intelligence analysis by creating opportunities offered by specific tools to process the increasingly large volume of available data, but also to adapt the analytical component to new security challenges, such as the capacity to extract relevant information in a very short time or the integration of multiple intelligence collection disciplines, specifically multiple sources of data and information.

The proposed article is based on the hypothesis that the integration of the emerging technologies, with primary focus on AI, generates fundamental transformation in the process of intelligence analysis and leads to the reconfiguration of the intelligence cycle, through the redefinition of the human analyst's role within a synergistic human-machine interaction framework. From a methodological perspective, the study relies on a narrative review of the literature, complemented by a bibliometric analysis of academic and institutional sources relevant to the scientific inquiry.

The exponential volume of digital data generated by new information and computing technologies has reduced the efficiency of traditional analysis methods. Consequently, intelligence analysis will be shaped by the powerful and potentially disruptive effects of AI, big data, and machine learning on what has long been an intimately scaled human endeavor. Furthermore, by utilising emerging technologies, we can project a scenario in which intelligence analysis is performed by digital assistants using AI-equipped systems and integrated data infrastructures, while analysts only verify and concentrate on tasks located at superior execution and command levels. Thus, through human-machine teams, processing and detection capacity is extended, while ethics and responsibility at the level of the decision-making process are ensured (Gartin 2019).

Intelligence analysis is a cognitive activity carried out by human operators, whereas artificial intelligence represents a set of computational systems and algorithms used to process large volumes of data and information, in short time, detect patterns, and support or automate specific analytical tasks. The evolution of emerging technologies, and implicitly of artificial intelligence, will favour the development and efficiency of cognitive tools that will facilitate and modify the analyst's role. Traditionally, the analyst is at the center of the analysis process, receiving information, deciding what is important and what is redundant, using acquired knowledge, and generating an intelligence product for the political decision-maker. The traditional model will be replaced by one in which automated storage and analysis processes generate the intelligence product based on beneficiary

requirements and interactions, and the analyst will intervene only when the situation is too complex, insufficiently measurable by autonomous systems, or the decision is novel or less understood (Hare and Peter Coghill 2016, 8-12).

The transformation of intelligence analysis offers a relevant conceptual framework for understanding how emerging technologies are integrated into analytical practice. With the explosion of data volume, the capacity of traditional intelligence analysis methods has been surpassed, and the manner of implementing and integrating artificial intelligence, machine learning, and cloud computing will be decisive for maintaining the decision-making advantage at the strategic level. Technology will take over repetitive tasks and those requiring a large volume of data and information; thus, the cognitive activity of analysts is used to add value to the intelligence product through hypothesis formulation and testing, critical thinking, and strategic communication. However, constraints related to algorithm limitations regarding human reasoning, analysts' competencies and resistance to change, as well as the need for organisational reform, professional training, and new doctrinal and legal frameworks to produce a transformation at the level of intelligence analysis must be recalled (Katz 2020).

In 1989, shortly before the fall of the Berlin Wall and the Iron Curtain, American President Ronald Reagan made a statement asserting that "The Goliath of totalitarian control will rapidly be brought down by the David of the microchip" and that "the biggest of Big Brothers is increasingly helpless against communications technology.... Information is the oxygen of the modern age.... It seeps through the walls topped with barbed wire. It wafts across the electrified borders and traps..." (Harari 2024, 9). Through this statement, Ronald Reagan captures, among other things, a turning point within intelligence services in non-democratic regimes, in the sense that technological evolution would limit their capacity to control, filter, and block information flows. Thus, the historical moment that ended the Cold War represented a transformation of political power toward structures capable of managing and capitalising on the informational explosion generated by technology.

Emerging technologies are already utilised within systems that support the decision-making process through intelligence analysis products. Thus, the subject proposed for this paper is of interest to a wide range of specialists in various fields, from different countries, especially within intelligence structures and armed forces in NATO and the European Union (EU), but also in the defence industry or in the field of research and development of new dual-use technologies.

Therefore, the present study aims to contribute to the understanding of how emerging technologies, particularly AI and LLMs, reconfigure the relationship between the analyst's cognition and the mathematical processing of algorithms within intelligence analysis. By an examination of the current trends, the scientific endeavour seeks to contribute to the debate on how technological evolution and

digital transformation redefine the architecture of intelligence analysis within a geopolitical framework characterised by increasing complexity of security threats and by a reconfiguration of political and diplomatic approaches.

1. The Evolution from Information Analysis to Intelligence Analysis

The North Atlantic Treaty Organization defines analysis as "the study of a whole by examining its parts and their interactions" (The NATO Joint Analysis and Lessons Learned Centre 2024). In this context, analysis is not new to the military system, which has used analysis to support decision-making and to streamline the impact of military capabilities on the enemy. Analysis represents an essential cognitive mechanism for building knowledge, but also a specialised epistemic endeavour applied within the field of national security. By employing specific analytical methods and techniques, it enables the transformation of raw data into actionable intelligence. Ultimately, this cognitive process serves to support and optimise the decision-making process up to the highest politico-military level of a state (Nițu 2011, 15-16). Seen from a different perspective, namely law enforcement and maintaining public order and safety, intelligence analysis is conceptualised by referring to the techniques used, but also to the intelligence products generated at various operational levels. Thus, while at the tactical level, intelligence products assess immediate risks and current activities, at the strategic level, they provide an integrated perspective on the dynamics of activities, facilitating local policies and future action planning (Cope 2003, 404-410).

The term *intelligence analysis* is also conceptualised within intelligence services. For example, the Romanian Intelligence Service (SRI) defines intelligence analysis as a "highly complex refinement process that involves both the intelligence, critical thinking and creativity of the intelligence analyst, as well as a very good knowledge of the field being analyzed" (Serviciul Român de Informații 2025). This definition highlights the multidimensional nature of intelligence analysis, which is an approach based on knowledge, judgement, but also practical skills to synthesise information and evaluate it meaningfully.

However, technological developments have left their mark on the traditional methods of intelligence analysis used by intelligence agencies and structures, through the use of specific tools to process the ever-increasing volume of available data, but also to adapt the analytical component to new security challenges, such as the ability to extract relevant information in a very short time or the integration of several disciplines of information gathering, respectively several sources of data and information.

The First World War was a turning point in the development of information gathering, analysis and dissemination capabilities, especially as intelligence services

played an important role in the evolution and conduct of the conflict. Thus, intelligence services evolved from lone agents to networks of spies and informants, but also to communications interception techniques, aerial photography and reconnaissance flights. Cryptography also developed during this period to secure information transmitted through telegraph and telephone networks, but also to decrypt the secure information of adversaries (Ferris 2019, 1). A well-known event that changed the course of the war, through the entry of the United States into the conflict, but also through the fact that the information was obtained without the intervention of agents in the field, was the interception of a telegram sent by the German Foreign Minister, Arthur Zimmermann, on 16 January 1917, to the ambassador in Mexico, Heinrich von Eckardt, by British intelligence services, when Germany offered Mexico an alliance against the US (Gathen 2007, 2-3).

In this context, the methods used in intelligence analysis evolved to integrate data and information from multiple sources into the products disseminated to decision-makers, but also to assess their credibility. The US Army also developed a doctrine that provided for the production and dissemination of intelligence products to military commanders on the battlefield. Although the US Expeditionary Force did not have intelligence structures in place at the beginning of its military operations, once they arrived in France, they adapted and understood the importance of radio interceptions and photographs from the battlefield, which proved to be a real advantage later in World War II (Smoot n.d.).

The Second World War was an important moment for intelligence analysis, due to the very large volume of data and information from several geographical areas where military actions were taking place at the same time. The field of cryptanalysis underwent significant development, with notable successes, including the decryption of the Enigma machine code, a project on which 10,000 people worked at one point, the code used by Japanese embassies, called "Purple", and the Lorenz code (Mowry 2014, 1-8). The naval victory at Midway in 1942, as well as the success of the Normandy landings, were largely due to the interception and decryption of Axis messages, but also to the determination of political and military leaders who took their content into account.

Technology played an important role in this new type of analysis, with the Colossus computer, the first fully electronic computing machine, being built and used to break the Lorenz code used by the German army in its strategic communications, including with the political leadership. These were first intercepted in 1941, and their exploitation and analysis demonstrated that information obtained from enemy communications provided decisive advantages in supporting decision-making and achieving superiority on the battlefield (National Security Agency 2024).

The Soviet Union demonstrated its progress in technological development during World War II as early as 1945, when an official delegation presented the

American ambassador in Moscow, Averell Harriman, a wooden replica of the Great Seal of the United States, inside which was concealed a passive listening device, later known as "The Thing". The device was designed as a passive cavity resonator and activated by a radio frequency beam emitted from outside the embassy. It allowed conversations in the ambassador's office to be captured by modulating the reflected signal, making it extremely difficult to detect with the technical means available at the time. It was not discovered until 1952, and its public disclosure brought to light both the technological ingenuity of the device and the major vulnerabilities of information protection in the diplomatic environment (Wilson 2025).

In 1951, the Technical Services Staff was established within the CIA, whose main mission was to provide technical support for the agency's operations by developing specialised equipment. This section evolved and was reorganised in 1960 under the name Technical Services Division, at a time when the complexity of the agency's activities required deeper integration of technology (Central Intelligence Agency 2007). In 1952, the NSA (National Security Agency) was established, a leader in the field of cryptology, radio communications interception and electromagnetic emissions from non-communications equipment (SIGINT - Signals Intelligence). More than a decade later, in 1963, the CIA established The Directorate of Science & Technology, a structure dedicated to science and technology, whose main mission is to provide technical support for the agency's actions through research, development and scientific analysis programmers, while maintaining a permanent link between government and private research (Central Intelligence Agency n.d).

It can be seen that the post-war period was marked by the creation of modern intelligence services, given that the conventional warfare waged in the Second World War turned into the Cold War, where the victorious powers became enemies. The term Cold War was first used by English writer George Orwell in an essay published in 1945, entitled "You and the Atomic Bomb", to define a "peace that is not peace" (Foundation 1945). This period also saw some of the greatest failures of intelligence analysis, such as in 1950, the start of the Korean War, the Cuban missile crisis in 1962, the Tet offensive in Vietnam in 1968, and the 1979 revolution in Iran (Lock 2010, 129, 177-178, 276, 368).

Throughout this period, intelligence analysis focused more on discovering the adversary's intentions and military capabilities, especially nuclear ones. The Cuban missile crisis highlighted the importance of imagery intelligence (IMINT - information obtained from the collection and analysis of visual data from a range of sources, including satellites, reconnaissance aircraft, drones and ground cameras) (Caddell 2017), but also of information obtained from signals and electronic systems used by foreign targets, such as communications systems, radars and weapons systems, which provide information on the capabilities, actions and intentions of foreign adversaries (Government Communications Headquarters 2016). In this

context, intelligence services have adapted from tactical and operational intelligence, specific to the Second World War, to strategic intelligence and long-term analysis.

The impact of technology on intelligence gathering was reflected in aerial reconnaissance, where, starting in 1956, the U-2 reconnaissance aircraft managed to allay the fears of American leaders about the Soviet intercontinental ballistic missile (ICBM) development programme. By the time the Soviets developed a missile capable of shooting down this aircraft in 1960, the Americans, at the initiative of President Eisenhower, had a satellite surveillance programme called Corona. This technology thus allowed them to "cross borders" to gather essential information for political and military decision-makers, especially since the communist bloc was a closed one that did not allow secret agents to be sent into the field (Lock 2010, 129).

In 1970, Edgar F. Codd published the paper "A relational model of data for large shared data banks", which introduced the concept of a relational data model and the interconnection of data through logical relationships rather than hierarchical structures. Although initially met with skepticism, including from the industry itself, such as IBM (International Business Machine), the relational model became an international standard for data storage and management. In 1979, the first commercial product called Oracle V2 appeared. All these developments brought Edgar F. Codd's concepts to the fore, which represented an analytical revolution for information communities, allowing rapid data correlation, reduction of information redundancy, and more efficient searches in increasingly complex databases.

During the same period, encryption-enabled telephones and electric typewriters were gradually introduced, and the first word processing applications appeared, all of which facilitated the work of analysts. Later, analysts in the intelligence community installed capabilities for reading, writing, storing, and transmitting information in electronic format through secure communication channels, which improved the flow of information and, implicitly, the quality of intelligence products. At the same time, the interconnection of local networks facilitated access to databases, and increased transfer speeds enabled the rapid exchange of information between intelligence communities (Clift 2003).

After the Second World War, in the era of the so-called Cold War, which was in fact a rivalry between the United States and the Soviet Union, but also their allies, the intelligence services had as their priority mission the provision of information and intelligence products to prevent a new armed conflict between the great powers, a third world war. Thus, the emphasis remained on collection, as a stage in the intelligence cycle, and less on processing, exploitation and, implicitly, analysis. The period was marked by the continued use of traditional, analyst-centered methods, where the analyst's expertise, judgement and skills were advantages in complex situations with many uncertainties. Moreover, after the official dissolution of the Soviet Union on 26 December 1991, there were voices of well-known politicians

who called for the abolition of intelligence services, given the democratisation of the East and the end of the bipolar world dominated by the former USSR and the USA (McGarr 2015, 291).

After 1990, with the emergence and development of the internet, personal computers and technical equipment, there was also a revolution in information analysis, which facilitated the exchange of information between partner structures. The World Wide Web provided methods of personal, commercial and governmental communication, and the development of public key encryption enabled online monetary transactions and the development of online messaging applications (e.g. Skype, FaceTime) that used the internet as a communication channel (Lowenthal 2017). The era of the internet brought about a paradigm shift in the analytical process, which adapted to open sources through the discipline of information gathering, OSINT (Open Source Intelligence), alongside information from human and technical sources (SIGINT – Signal Intelligence).

In the new post-Cold War era, intelligence services shifted their focus from the military threat posed by the Soviet Union and its ideological expansion to new threats to national security, predominantly non-state actors such as terrorist groups, which became their main mission. The terrorist attacks of 11 September 2001 marked a turning point for intelligence services wordwide, not just for those in the United States. The official investigative report highlighted major shortcomings in interagency cooperation, as well as significant limitations in the analytical capacity, despite the existence of indications suggesting the possibility of a terrorist attack (The National Commission on Terrorist Attacks Upon the United States 2004). The post-September 11 period was marked by profound changes in intelligence services, with an emphasis on information sharing, modernisation of IT capabilities, a shift away from the "need to know" mentality, and changes in analysis methods and techniques. Furthermore, institutional changes took place with the creation in 2004 of the position of Director of National Intelligence, a role designed to integrate and coordinate analytical efforts within the US intelligence community in order to prevent a repeat of their failure to ensure national security.

At the same time, the technological revolution has also left its mark on collection and analysis techniques and methods, and political decisions have begun to take the information obtained into account. Moreover, intelligence activities have moved beyond the classified realm and have become public in some areas, with major implications for political and military decision-makers, as well as the general population. Technology has become a catalyst for analytical resources, enabling the transition to new methods through the use of modern tools.

The NSA's 2012 SIGINT collection discipline strategy highlighted the fact that intelligence services have consistently used data and information collected by equipment specific to this discipline in their products and, due to their high degree of

accuracy, have guided the actions of political and military decision-makers (National Security Agency 2012). At the same time, the development of digital infrastructure and the virtual environment has led to the emergence of two other distinct areas of collection and analysis, namely CYBERINT and OSINT, which together provide complete coverage of cyberspace.

Technological evolution and paradigm shift within intelligence structures have facilitated their adoption of the latest tools, fundamentally transforming the way data is collected, analysed and processed to anticipate threats and support strategic decisions. The exponential growth in computing power, the emergence of computers and computer applications, and the explosion in the volume of digital data have brought about transformations in the analytical process. Under these circumstances, where intelligence services are faced with information overload and the inability to analyse data using traditional methods and human effort alone, the need to transition to technical solutions using emerging technologies is becoming increasingly apparent.

2. The Future of Intelligence Analysis

In this context, over the last decade, the current technological revolution has significantly transformed information gathering capabilities, as well as the ability of analysts to extract important information from an ever-increasing volume of data collected by sensors and stored on different systems. The World Economic Forum estimates that by 2020, there will be 44 zettabytes of digital data, approximately 40 times more bytes than there are stars in the observable universe (The World Economic Forum 2019). The Director of the National Geospatial-Intelligence Agency (NGA) has publicly estimated that at the current rate of data and information collection, eight million image analysts will be needed by 2037 to process all the data (Office of the Director of National Intelligence 2019). Through artificial intelligence, the large volume of information collected, Big Data, is processed and analysed, and the information products are disseminated to political and military decision-makers. At the same time, by taking over tasks with artificial intelligence tools, human analysts can focus more on the needs of the beneficiary, on validating results, on preparing products, but also on horizontal and vertical communication.

One of the limitations that intelligence services may face is that, although they have an artificial intelligence tool at their disposal, it is not provided with sufficient data for machine learning. In this context, the analytical component will be limited and will create dissatisfaction among workers, as it is well known that the success of the mission depends on their perception of change. The principle in computer science "GIGO - Garbage in, garbage out" applies very well to AI and its components Machine learning or Deep learning.

Recent research by the Technical University of Munich and the University of Hamburg has shown that ChatGPT has a "pro-environmental and left-wing libertarian orientation". Political bias is not unusual, as it is present in all people, but the results of intelligence analysis must remain objective in order to support the actual decision-making process at the political and military levels. This is a key reason that demonstrates the crucial role of the analyst, who must carefully examine the results of algorithms, identify biases, and ensure an informative product that meets the quality standards of the beneficiaries (Insight Forward 2024). In this context, we draw attention to algorithm audit mechanisms, as well as ongoing and multiple human verification, to prevent AI from taking on human biases and amplifying them. The normative dimension has also evolved. The United Nations General Assembly adopted Resolution 79/239 on 24 December 2024, which clearly states that international humanitarian law applies "throughout all stages of the life-cycle of artificial intelligence in the military domain", clearly mentioning the need for human control in the decision-making process. This international position at the highest level argues that AI should amplify, not replace, human responsibility and judgement in decision-making at all operational levels.

Consequently, the human-machine connection, materialised through AI systems, demonstrates relevance in the field of military action, including the informational dimension of the operational environment. Technological integration excels precisely because it combines human cognitive abilities with the computing power of artificial systems, so that humans, analysts, have genuine qualities in terms of critical thinking and analytical intuition, while AI excels in processing and analysing very large volumes of data.

Among the relevant models of interaction between analysts and artificial systems, we highlight the following types of interactions:

- Human-in-the-loop (HITL), where the analyst will verify and validate information discovered by the system based on keywords (Wilcox 2023, 88);
- Human-on-the-loop (HOTL), where the system runs autonomously, but the analyst monitors and can intervene if necessary (Tschider 2024, 59-65);
- Human-out-of-the-loop (HOOTL), where the system will make decisions without any human intervention, with the proviso that there may be verification or supervision after the decision (Endsley 2016, 18).

To highlight the levels of interaction between humans and machines, in this case with AI, we have designed Figure no. 1, which highlights the compromise between human control, AI and the processing speed of the data entered. In the case of HITL, human control over information products, generically referred to as intelligence, is present, while in the case of HOTL, human control and AI share responsibilities. Last but not least, when we consider HOOTL, human control does not exist, the artificial intelligence system has complete access to inputs and outputs, and the analyst becomes a mere observer.

In this context of developing interaction between AI and human intelligence, we can evolve towards much more advanced concepts, such as "Human-Machine Teaming – HMT", which will allow analysts and autonomous systems to work as partners or colleagues (NATO Science & Technology Organization 2023). An example of such a system, which allows collaboration between a human operator and AI, is AI Felix (Artificial Intelligence Front End Learning Information Execution), developed by NATO's Allied Command Transformation (ACT) since 2019, which is a "knowledge agent" with a clearly defined objective, "is to automate the extraction of metadata and the distribution of this information across the organization". Although the use of the system will only reduce the number of employees by 40, it is connected to classified networks that are not connected to the internet "with an average processing time of 27 seconds per document compared to the 5 to 10 minutes required."

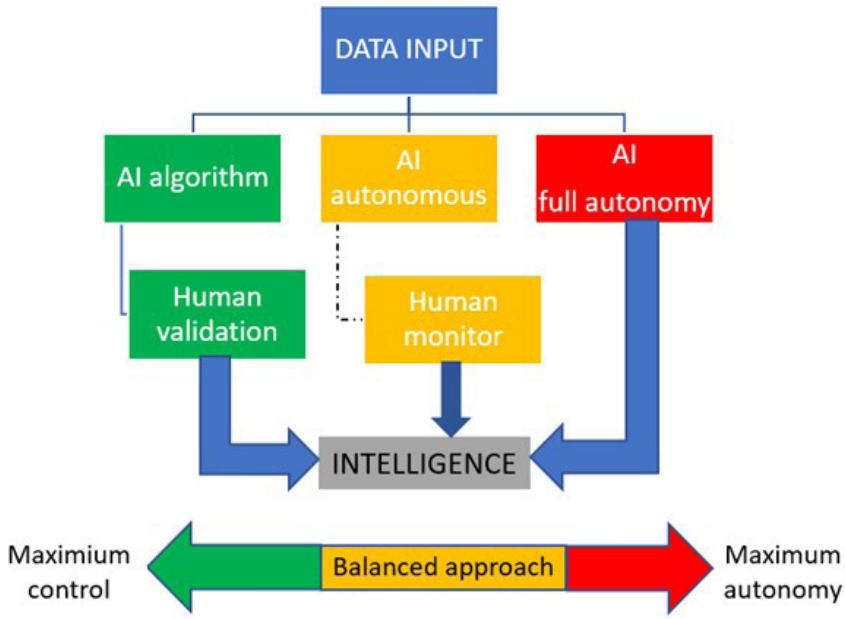

Figure no. 1: Human-AI interaction: Autonomy spectrum in decision-making system

North Atlantic Treaty Organization, an emerging capability called AI CLAIRE (Content Linking and Artificial Intelligence for Rapid Exploitation) has been developed, which is tasked with semantic search and intelligent content navigation, thus enabling rapid access to critical knowledge and providing support in strategic decision-making (Command 2025). With changes in the European and global security environment, which contains a large amount of increasingly complex information,

NATO, as a political-military alliance, has set itself the goal of maintaining an advantage at all operational levels, with an emphasis on the strategic level, by developing intelligence capabilities, with a focus on the collection, processing, exploitation, analysis and integration of data from open sources, through the OSINT collection discipline, but also from images, through the IMINT collection discipline. In this way, the Alliance maintains its cognitive edge, which will allow it to retain the ability to make decisions faster and more efficiently than potential enemies.

We are witnessing an emerging transformation in which the analyst will not be replaced by technology, but only augmented by it, and for this model to work, digital training of personnel is necessary, including hybrid skills, both cognitive and technical, such as mechanisms for verifying and understanding algorithms. Although the HMT concept is a vision of the future where human and artificial capabilities function as an integrated entity, the enthusiasm for the potential of emerging technologies and, implicitly, AI must be analysed and tempered by an understanding of the limitations and risks, and the professional redefinition of intelligence analysts is not the only issue. There is an assumed risk that AI will consume more time and resources (e.g., electricity), and that the results of intelligence analyses will generate a false sense of efficiency and overconfidence. Thus, intelligence services, and in general organisations that choose to use AI, must clearly define the tasks it is to perform, with the integration of emerging tools into existing processes. In fact, constant monitoring of the technology is required in order to obtain a real response to the performance or failure generated by the complexity of existing processes.

Intelligence analysis is more than just answering one or more questions: Who? What? When? Where? Why?, and How? It refers to an iterative process of examining, interpreting, evaluating and

validating data from multiple sources, formulating and testing alternative hypotheses to produce actionable knowledge. Intelligence analysis does not stop there, because its primary goal is to anticipate future events by generating scenarios, defining and explaining uncertainties, and transforming big data into information that provides opportunities for decision-makers and ensures national security and the promotion of national interests and values. Moreover, the information space has undergone profound changes due to the evolution of technology towards the digital age, and we can now appreciate that one of the determining factors in intelligence analysis is the democratisation of sources and the transition from secret sources – CLOSEINT – to open sources – OPENINT. In this context, the discipline of OSINT information gathering has become the core of intelligence analysis, but also a tool through which every citizen is transformed into a potential observer.

The emergence of new technologies has revolutionised the operational environment, radically transforming the information dimension, while the phrase "information is power" has returned in the current security environment, marked

by profound transformations that are unpredictable even for the most experienced analysts. The value of analytical products made available to political and military decision-makers depends to a large extent on the technology available at all stages of the intelligence cycle. Information has become a new weapon both in conventional conflicts, where military actions win campaigns, battles, fights and clashes, and especially in hybrid and asymmetric conflicts, where state and non-state actors achieve strategic victories with small forces.

In his work *Intelligence Analysis – An Approach from the Perspective of Change Theories*, 2nd revised and expanded edition, Ionel Nițu presents the "4P" model, in which the first "3Ps come from the categories/domains involved in defining national security intelligence analysis, namely: process, personnel, product and public" (Niţu 2011, 142), and the fourth "P", comes "from another coordinate of the producer and consumer relationship" (Nițu 2018, 192). In the current context of the technological revolution that has also penetrated the field of intelligence services and, with it, intelligence analysis, it can be said that the "4P" model can be transformed into a "4P+T" model, where the "4P" are the elements presented above, and the "T" represents the technology that supports the process, personnel, product and audience.

Conclusions

The future of intelligence analysis will be a deeply technologically augmented process, and within the decision-making process, the human factor remains responsible and involved. Under these conditions, with an exponential increase in the volume of data and information and with the increasingly accelerated integration of AI into the intelligence cycle, the value of intelligence products will depend on the quality of the interaction between humans and machines, but also on the ability of intelligence services to use algorithms in a well-defined operational framework, in line with their missions. In this context, the use of emerging technologies, especially AI, involves not only revolutionising data processing capabilities, but also designing safety and risk assessment mechanisms to ensure that the decisions taken by the human-machine duo are within the scope of the objectives at all operational levels, but especially at the strategic level.

A future is emerging in which intelligence analysis will be fundamentally transformed by the technological and digital revolution, where AI-integrated analysis capabilities will extend the automation capabilities of high-e data processing tasks, thus freeing up time for activities that require human judgement, anticipation and decision support. It is precisely the balance between the human and technological factors that will strengthen trust and ensure the validation of intelligence products.

The proposed emerging "4P+T" model synthesises a new paradigm in which technology has become a catalyst for analytical process efficiency, however without replacing the critical role of the analyst, and the human-machine binomial describes

an increasingly imminent future, in fact a symbiosis between the analyst and AI-managed algorithms, with the role of transforming data into intelligence.

The success of intelligence analysis in an operational environment characterised by dynamism, technological competition and big data will depend on the ability of state actors to responsibly integrate emerging technologies while preserving human reason.

BIBLIOGRAPHY:

American Civil Liberties Union. 2012 "SIGINT Strategy." Accessed November 30, 2025. https://www.aclu.org/sites/default/files/assets/u_sigint_strategy.pdf

Alford, Stephen. 2011. "Some Elizabethan Spies in the Office of Sir Francis Walsingham. Diplomacy and Early Modern Culture", 46-62. https://doi.org/10.1057/9780230298125_4

Bode, Ingvild. 2024. "Falling under the radar: the problem of algorithmic bias and military applications of AI." International Committee of the Red Cross. Accessed November 11, 2025. https://blogs.icrc.org/law-and-policy/2024/03/14/falling-under-the-radar-the-problem-of-algorithmic-bias-and-military-applications-of-ai/

Caddell, Joseph . 2017. "Discovering Soviet Missiles in Cuba: How Intelligence Collection Relates to Analysis and Policy." War on the Rocks. Accessed November 11, 2025. https://warontherocks.com/2017/10/discovering-soviet-missiles-in-cuba-intelligence-collection-and-its-relationship-with-analysis-and-policy/

Center for Strategic and International Studies. 2020 "The Intelligence Edge: Opportunities and Challenges from Emerging Technologies for U.S. Intelligence.". Accessed November 30, 2025. https://www.csis.org/analysis/intelligence-edge-opportunities-and-challenges-emerging-technologies-us-intelligence

Central Intelligence Agency - CIA. 2025. "CORONA: America's First Imaging Satellite Program. Retrieved from Central Intelligence Agency." Accessed November 10, 2025. https://www.cia.gov/legacy/museum/exhibit/corona-americas-first-imaging-satellite-program/

Central Intelligence Agency - CIA. 2007. "Office of Tehnical Service - 50 Years Supporting Operations." Central Intelligence Agency. Accessed November 15, 2025. https://www.cia.gov/readingroom/docs/DOC_0001225679.pdf

Central Intelligence Agency - CIA. 2025. "Directorate of Science and Technology. Retrieved from Central Intelligence Agency." Accessed November 5, 2025. https://www.cia.gov/about/organization/directorate-of-science-and-technology/

Clark, J. Ransom. 2007. Intelligence and National Security: A Reference Handbook (Contemporary Military, Strategic, and Security Issues). London: Praeger.

Clift, Denis A. 2003. "Intelligence in the Internet Era - From Semaphore to Predator." Central Intelligence Agency. Accessed November 30, 2025. https://www.cia.gov/resources/csi/static/Intel-in-Internet-Era.pdf

Command, NATO's Strategic Warfare Development. 2025. Harnessing Artificial Intelligence: Allied Command Transformation at the Forefront of NATO Innovation. Accessed November 30, 2025. https://www.act.nato.int/article/harnessing-artificial-intelligence/

Cope, Nina. 2003 "Crime Analysis: Principles and Practice." În Handbook of Policing, de Tim Newburn, 340-362. Portland: Willan Publishing.

Deloitte Insights. 2019. "The future of intelligence analysis - A task-level view of the impact of artificial intelligence on intel analysis." Accessed November 1, 2025. https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/artificial-intelligence-impact-on-future-intelligence-analysis.html

EMDYN. 2025. "Imagery Intelligence. Retrieved from EMDYN." Accessed November 2, 2025. https://www.emdyn.com/solutions/imagery-intelligence

ETH Zurich. 2000. "The Cuban missile crisis." Accessed November 3, 2025. https://www.files.ethz.ch/isn/6858/doc_6860_290_en.pdf

Ferris, John Robert. "The War Trade Intelligence Department and British Economic Warfare during the First World War." British World Policy and the Projection of Global Power (Cambridge University Press), 2019: 24-45.

Foundation, The Orwell. The Orwell Foundation. 1945. Accessed November 3, 2025. https://www.orwellfoundation.com/the-orwell-foundation/orwell/essays-and-other-works/you-and-the-atom-bomb/

Gallagher, Brian. 2020. "The amount of data in the world doubles every two years." Accessed November 10, 2025. https://medium.com/callforcode/the-amount-of-data-in-the-world-doubles-every-two-years-3c0be9263eb1

Gartin, Joseph W. 2019 "The Future of Analysis." Center for the Study of Intelligence. Accessed November 30, 2025.. https://www.cia.gov/resources/csi/static/Future-of-Analysis.pdf

Gathen, Joachim von zur. 2007"Zimmermann Telegram: The Original Draft." *Cryptologia 31*: 2-37. https://doi.org/ 0.1080/01611190600921165

Government Communications Headquarters - UK. 2016. A short history of SIGINT in Scarborough. Accessed November 30, 2025. https://www.gchq.gov.uk/information/short-history-sigint-scarborough

Harari, Yuval Noah. 2024 A Brief History of Information Networks from the Stone Age to AI. New York: Random House.

Hare, Nick, și Peter Coghill. "The Future of the Intelligence Analysis Task." *Intelligence and National Security* 6 (2016): 858–870 https//:dor.org/10.1080/02684527.2015.1115238

Horowitz, Michael C. 2020. "Do Emerging Military Technologies Matter for International Politics?." Annual Review of Political Science. https://doi.org/10.1146/annurev-polisci-050718-032725

Insight Forward. 2024. "Emerging Technology and Intelligence Analysis." Accessed November 10, 2025. https://www.insightforward.co.uk/wp-content/uploads/

go-x/u/f0af2c7a-66bd-4e86-9488-d1fef3599589/Emerging-Technology-and-Intelligence-Analysis.pdf

Iordanou, Ioanna. 2022. "The secret service of Renaissance Venice: intelligence organisation in the sixteenth century." Journal of Intelligence History, 21(3), 251-267. https://doi.org/10.1080/16161262.2022.2141976

Johnson, James. 2019. "Artificial intelligence & future warfare: implications for international security." Defense and Security Analysis. 35(2), 147–169. https://doi.org/10.1080/14751798.2019.1600800.

Katz, Brian. 2020 "The Analytic Edge: Leveraging Emerging Technologies to Transform Intelligence Analysis." Center for Strategic and International Studies. Accessed November 30, 2025 https://www.csis.org/analysis/analytic-edge-leveraging-emerging-technologies-transform-intelligence-analysi

Khachatryan, Davit. 2025. "Military AI Challenges Human Accountability." Accessed November 7, 2025. https://internationalpolicy.org/publications/military-ai-challenges-human-accountability/

Klaus, Matthias. 2024. "Transcending weapon systems: the ethical challenges of AI in military decision support systems." Accessed November 7, 2025. https://blogs.icrc.org/law-and-policy/2024/09/24/transcending-weapon-systems-the-ethical-challenges-of-ai-in-military-decision-support-systems/

Kramer, Roderick M. 2012. "Institutional Trust Failures: Insights and Lessons from the 9/11 Intelligence Failures." *Restoring Trust in Organizations and Leaders: Enduring Challenges and Emerging Answers*. 69-91. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199756087.003.0005

Lane, Chris. 2024. "Bias in AI amplifies our own biases." Accessed November 7, 2025. https://www.ucl.ac.uk/news/2024/dec/bias-ai-amplifies-our-own-biases

Lock, Johnson. The Oxford handbook of national security intelligence. New York: Oxford University Press,, 2010.

Lowenthal, Mark M. Intelligence : from secrets to policy 7th Edition. 2015 Los Angeles: CQ Press, 2017.

McGarr, Paul. 2015. "Do We Still Need the CIA?' Daniel Patrick Moynihan, the Central Intelligence Agency and US Foreign Policy." History (Wiley) 2, nr. 340 (2015): 275-292. http://www.jstor.org/stable/24809573

Mitchell, Taylor. 2021. "Algorithmic Bias in Health Care Exacerbates Social Inequities-How to Prevent It." Accessed November 7, 2025. https://hsph.harvard.edu/exec-ed/news/algorithmic-bias-in-health-care-exacerbates-social-inequities-how-to-prevent-it/

Mowry, David P. 2014 German Cipher Machines of World War II. Fort George G. Meade: Center for Cryptologic History – NSA. Accessed November 30, 2025. https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/wwii/german_cipher.pdf

National Security Agency. 2024. History Today: The role of signals intelligence or 'ULTRA' on D-Day. Accessed November 30, 2025. https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3790238/history-today-june-6-the-role-of-signals-intelligence-or-ultra-on-d-day/

National Security Agency-Central Security Service. 2025. "Signals Intelligence Overview." Accessed November 12, 2025. https://www.nsa.gov/Signals-Intelligence/Overview/

NATO. 2019. "Artificial Intelligence Front End Learning Information." Accessed November7,2025.https://www.act.nato.int/wp-content/uploads/2023/05/2019_ai-felix.pdf

NATO Allied Command Transformation. 2019. "Artificial Intelligence Front End Learning Information." Accessed November 7, 2025. https://www.act.nato.int/wp-content/uploads/2023/05/2019_ai-felix.pdf

NATO Science & Technology Organization. 2023. "Science & Technology Trends 2023-2043-volume 1: Overview." Accessed November 4, 2025. https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf

NATO. 2024. "Summary of NATO's revised Artificial Intelligence (AI) strategy." Accessed November 7, 2025. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy

NATO Joint Analysis and Lessons Learned Centre. 2024. Accessed November 27, 2025.Analysis Handbook. https://nllp.jallc.nato.int/news/Documents/JALLC_Analysis_Handbook_2024.pdf

NATO's Strategic Warfare Development Command. 2025. "Harnessing Artificial Intelligence: Allied Command Transformation at the Forefront of NATO Innovation." Accessed November 5, 2025 https://www.act.nato.int/article/harnessing-artificial-intelligence/

NATO Command Transformation at the Forefront of Innovation. 2025. Accessed November 29, 2025 https://www.act.nato.int/article/harnessing-artificial-intelligence/

NATO's Strategic Warfare Development Command. 2025. Harnessing Artificial Intelligence: Allied Command Transformation at the Forefront of NATO Innovation. Accessed November 30, 2025. https://www.act.nato.int/article/harnessing-artificial-intelligence/

Nițu, Ionel. 2018. "Analiza de intelligence – O abordare din perspectiva teoriilor schimbării", ed. a 2-a revăzută și adăugită. București, România: RAO.

Nițu, Ionel. 2011. Ghidul analistului de intelligence - Compendiu pentru analiştii debutanţi. 2011.Editura Academiei Naţionale de Informaţii - Mihai Viteazul, 2011.

Office of the Director of National Intelligence. 2019. "The Aim Initiative: A Strategy for Augmenting Intelligence Using Machine". Accessed November 12, 2025.

https://www.govinfo.gov/content/pkg/GOVPUB-PREX28-PURL-gpo115186/pdf/GOVPUB-PREX28-PURL-gpo115186.pdf

Romanian Intelligence Service. 2025. "Intelligence Analysis". Accessed November 8, 2025. https://www.sri.ro/analiza-de-intelligence

Smoot, Betsy Rohaly . "Chut, J'ecoute: The U.S. Army's Use of Radio Intelligence in World War I." The Army Historical Foundation, n.d. Accessed November 28, 2025. https://armyhistory.org/chut-jecoute-the-u-s-armys-use-of-radio-intelligence-in-world-war-i/

The Department of Homeland Security. 2024. "The impact of Artificial Intelligence on traditional human analysis". Accessed November 8, 2025. https://www.dhs.gov/sites/default/files/2024-09/2024aepimpactofaiontraditionalhumananalysis.pdf

The National Commission on Terrorist Attacks Upon the United States. 2004 "The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States." 9/11 Commission Report.

The Orwell Foundation. 1945. "You and the Atomic Bomb." Accessed November 10, 2025. https://www.orwellfoundation.com/the-orwell-foundation/orwell/essays-and-other-works/you-and-the-atom-bomb/

The World Economic Forum. 2019. "How much data is generated each day?." Accessed November 10, 2025. https://www.weforum.org/stories/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/

Tschider, Charlotte A. 2024. "Humans Outside the Loop." Yale Journal of Law & Technology 26. Accessed November 27, 2025. https://yjolt.org/humans-outside-loop

United Nations. 2024. "Artificial intelligence in the military domain and its implications for international peace and security". Accessed November 7, 2025. https://digitallibrary.un.org/record/4071348?ln=en&v=pdf

Warner, Michael. 2009. "Building a theory of intelligence systems. In G. F. Treverton, & Wilhelm Agrell, National Intelligence Systems - Current Research and Future Prospects (pp. 11-37). Cambridge. Cambridge University Press.

Wilcox, Lauren. 2023. "No Humans in the Loop: Killer Robots, Race, and AI." *Feminist AI: Critical Perspectives on Algorithms, Data, and Intelligent Machines.* Edited by de Jude Browne, Stephen Cave, Eleanor Drage și Kerry McInerney, 83-100. Oxford University Press.

Wilson, Matt. 2025 "'The most ingenious stunt since the Trojan Horse': The Soviet artwork that spied on the US." The British Broadcasting Corporation. Accessed November 30, 2025. https://www.bbc.com/culture/article/20250826-the-soviet-artwork-that-spied-on-the-us