

IMPACT OF ARTIFICIAL INTELLIGENCE ON THE INTELLIGENCE - SECURITY AND DEFENSE SECTOR

Sinisa Djukic^{1a}, Slobodan Simic²

¹ Faculty of Security and Protection, Independent University of Banja Luka, Republika
Srpska, Bosnia and Herzegovina, djukic-bs@blic.net

² Security Research Center, Street Sinise Mijatovica 9, Banja Luka, Republic of Srpska,
Bosnia and Herzegovina, slobodansimicss@yahoo.com

Received: 23th July 2024

Accepted: 19th August 2024

Review paper

Abstract: Artificial intelligence in the present, especially in the future, is designed to improve people's quality of life and enable them to perform everyday tasks more efficiently. It will help in the business of many, including those whose activity requires collecting, processing, analyzing and sharing a large amount of information in a really short time. The intelligence-security and defense sector is undoubtedly becoming a consumer of the potential of modern information and communication technologies and models. In this regard, the authors point out that the introduction of artificial intelligence will lead to certain changes in the organizational/functional structure of the intelligence-security and defense sector. Additional and continuous education of intelligence and military personnel, transformation of intelligence capabilities in all phases of the intelligence cycle, the need for accelerated flow and processing of information are just some of the segments that will undergo transformation. The goal of this work is to encourage a more versatile study of the impact of artificial intelligence on the intelligence-security and defense sector with all possible dilemmas and controversies.

Key words: Artificial intelligence, Intelligence-security and defense sector

1. INTRODUCTION

Artificial intelligence (AI) is already involved in many spheres of life and is a permanent thematic unit of many sciences and scientific disciplines. This motoric and imperative momentum of its ultimate limits in many ways also directs the development of various sectors that are directly and indirectly connected to artificial intelligence. The security, defense and protection sectors undoubtedly become consumers of the potential of modern information and communication models, but they are also an incentive to develop artificial intelligence directly for these areas. The set of principles that should be adopted for the use of artificial intelligence in the intelligence-security and defense sector should be in the range of evolutionary expansion

^a ORCID: [0000-0001-8962-4204](https://orcid.org/0000-0001-8962-4204)

to, on the other hand, the limitations of certain ethical and legislative norms. Budgetary development programs, human limitations, increasing risks and threats and increasing the level of information contribute in many ways to the introduction of AI in the intelligence-security and defense sector through various forms with the aim of faster and more purposeful decision-making.

Artificial intelligence is tireless, futuristic and with a visionary scenario, but films are shown showing a single person who receives information from AI and performs different tasks, terminators that perform autonomous data collection and task implementation. Highly developed countries have more developed technical-technological processes and communication systems that surpass smaller and less developed ones and use a wide range of AI usage in the work of the intelligence and defense sectors. Advanced AI capabilities promise improved threat detection, with algorithms analyzing massive data sets in real-time, enabling quick and accurate identification of potential risks. Intelligent monitoring, powered by artificial intelligence, automates monitoring of system logs and network traffic, ensuring proactive anomaly detection. By using historical data, predictive analytics empowers security systems with the ability to predict potential breaches. This predictive ability makes it easier to take preventive actions, effectively reducing risks before they become real threats (<https://zastita.info/hr/novosti/ugradnja-umjetne-inteligencije>).

Intelligence analysis through AI can quickly scan a wider area, identify certain patterns, perform a check with some of the compatible systems and technical solutions and in a short time take action and/or leave that exclusive right to an individual/operator to do it (deliver final data, send strategic analysis, etc.) The acceleration of the ways and approaches of using artificial intelligence was noticed by the great powers, where in a very, relatively short time, the processes and functions of AI were incorporated into the daily work of the intelligence-security and defense services. Strategies, policies and plans are relatively recent, as multivariate ways of using AI in intelligence work are emerging, but there is growing concern about the possible spectrum of negative consequences. In them, modern threats and risks are systematically recognized and the use of AI in the work of intelligence services is determined. Analyzing quantitatively and qualitatively a large number of contents in this contextual level, it can be seen that their genesis lies in the psychological characteristics of human beings that have their own limitations to the need for faster decision-making and the realization of different tasks of the intelligence-security and defense sector. Highly developed countries have virtual operational centers where elements of the operational-intelligence structure are tested in a multi-domain spectrum. The possibilities of such centers multiply with the use of sensor integration, high communication speeds, networking, focus on the execution of intelligence tasks, the connection of operatives in the field with high-tech innovations and the autonomy of systems incorporated in AI. In modern ways of intelligence work, this enables dominance in intelligence activity. It has been established that even in war conflicts in today's world, artificial intelligence is used, which in the conditions of modern warfare enables supremacy on the battlefield through the rapid collection and processing of data and the use of modern weapons by soldiers-decision-makers. (<https://www.theguardian.com/world/2024/apr/03/>).

2. IMPACT OF ARTIFICIAL INTELLIGENCE ON THE INTELLIGENCE-SECURITY AND DEFENSE SECTOR

Numerous security challenges and risks that the intelligence services are facing have caused certain changes in intelligence work. These changes are conditioned by dynamic events in the outside world and the need to accelerate all phases of the intelligence cycle from planning, collection, analysis, processing, sharing and decision-making. The progress of artificial intelligence opens up the possibility of development and wide application in many activities

such as traffic, agriculture, health, art, tourism, etc. The development of this technology and its benefits open up the possibility of application in the security and defense sector as a tool for collecting, processing, analyzing and sharing a large amount of information (Đukic, 2022).

A report by the *Center for Strategic and International Studies (CSIS)* states that new technologies such as artificial intelligence have the potential to transform and empower the intelligence community while simultaneously presenting unprecedented challenges from technologically capable adversaries. These technologies can help expand, automate and sharpen intelligence gathering and processing. They can increase the analyst's ability to produce strategic analysis and value-added insights and enable the intelligence service to more rationally use time, compile and deliver intelligence products to key decision makers. A central issue for success in the intelligence domain will be the adoption and adaptation of new technologies in the way intelligence is collected, analyzed and delivered to decision makers. If intelligence is about providing timely, relevant and accurate insight into foreign actors to provide an advantage in policy formulation, then many new technologies have the potential to reach deeper and wider into the research field.

Data should be delivered in the shortest possible time, volume, and specificity for the user. New technologies are already reshaping the way the intelligence community collects, stores, and processes information, but they are likely to transform all key aspects of the intelligence cycle in the coming decades—from collection to analysis to dissemination. Driving this change is the convergence of four technological trends: the proliferation of networked, multimodal sensors; the enormous growth of "big data", both classified and unclassified/unclassified; improvements to AI algorithms and custom-tailored applications such as computer code and natural language processing; exponential growth of computing power to process data and power AI systems. However, while considering the possibilities provided by new technologies such as AI, it is also important to realize that these technologies are not omnipotent for intelligence tasks and problems, nor independent of a much wider technological ecosystem and human capital. In a world of proliferating sensors and exponential growth in data and computerization, AI can help intelligence gathering organizations automate and streamline the processing of collected data. It can also assist in identifying and prioritizing collection targets in the various "- INTs" - geospatial (GEOINT), signals (SIGINT), human (HUMINT) and open source (OSINT). AI applications can then assist analysts in the way they receive, visualize and leverage that data. AI is particularly suited to more technical means of collection such as geospatial and signalling, helping to process and analyze their vast sensor-derived data sets. For geospatial (GEOINT) AI capabilities such as computer vision can help automate the processing of masses of image data and perform critical, time-intensive activities such as image recognition and categorization at speed and scale. For signals (SIGINT), AI can be similarly useful in automating the processing of electronic signals data (ELINT), while speech to text translation/transcription and other natural language processing capabilities help decipher intercepted communications (COMINT). In addition to the technical, AI tools can also enable a human source on the ground, in the most basic mission of HUMINT, in recruiting and extracting intelligence from foreign agents. Artificial intelligence algorithms can be trained to help "spot and evaluate" potential sources by combing through open source data. Advanced analytics could then help build "digital patterns of life" when recruiting potential sources, helping to predict their activities and verify their access to desired information. These tools could then be used to monitor security and counterintelligence risks before and after deployment. (Katz, 2020). The Report also states that new technologies can also transform and improve the way analysts think about continuously growing data and enable their association with computers/machines to provide timely insights to decision makers.

Previously, there was a principle that the collection of intelligence data and the analysis of that data should be separate processes, while today the exact opposite applies. It has been shown that analysts and intelligence operatives should cooperate closely in so-called operational teams so that the collected and processed data are more usable in the realization of intelligence tasks. This kind of approach can also cause certain problems that are manifested in the first place by the proximity of the analyst to the operational situation, i.e. the carriers and objects of intelligence interest, the assessment of the security problem, the lack of time for quality analysis, etc., but these shortcomings can certainly be eliminated by finding a suitable balance between the phases collection and analysis phases. Regardless of the rapid development of technology, human resources will continue to be an indispensable means of data collection in the field. The speed of flow and processing of information will require in certain cases the speed of portage for human sources. Thus, artificial intelligence algorithms will try to type potential candidates for cooperation using open sources, while analytics would be useful in determining the so-called "digital patterns of life", analysis of targets of intelligence interest, potential recruitment of sources, verification and prediction of their behavior, access to targets of intelligence interest, relevant information, etc. It used to be unthinkable that machines would suggest potential agents, but new technologies will strive to make a breakthrough in that segment as well. It is certain that this segment of intelligence work will continue to be very specific, bearing in mind certain phases of the so-called agent cycle, but the same, in certain situations, will speed up and facilitate work with all possible limitations (Đukic, 2022). Military intelligence services also use different levels of use of artificial intelligence, which now significantly affects the development of strategies for use in military forces (Defence Artificial Strategy, 2022). In this segment are determined:

- Military intelligence services also use different levels of use of artificial intelligence, which now significantly affects the development of strategies for use in military forces (Defence Artificial Strategy, 2022). In this segment are determined:
- Detection and recognition of the target, in which an attempt is made to prevent the activity of the opposing side;
- Monitoring the combat environment and reconnaissance (where drones equipped with artificial intelligence tools are used);
- Participation of artificial intelligence in strategic decision-making;
- Active use of artificial intelligence in command and control (through analytical potential). (Miljkovic, Berisa, Zgonjanin, 2023).

Research in the field of psychology certainly contributes to the assessment of the character of a human being who performs an intelligence assessment of the battlefield, analytically approaches the assessment of the threat of critical infrastructure objects or conducts operational analytical work in the field. Also, the success rate of certain assessments can be assessed with quite high reliability, as well as mathematical proofs can be performed. Intelligence improvements are visible and can be continuously upgraded. New methodologies are being created in training and development, which enhances the development capacities of both individual and collective analytics. However, it has certain limits because internal confrontations in decision-making are characteristics of the human personality. Human nature is inclined to react adequately/inadequately in certain crisis situations, which can lead to incorrect or untimely decisions. In many ways, the introduction of artificial intelligence makes it possible to approach the methods of intelligence work in a more objective way. High-tech crime can be recognized much faster by AI than by the reaction of a human being. Advanced

software allows AI to react without the influence of a human, an intelligence analyst, in order to prevent the leakage of information. After the AI's decision, executive activities are carried out that can be of the highest risk: defense of critical infrastructure, attack on a terrorist cell, fight against the proliferation of weapons, trafficking in people and narcotics, and others.

3. LIMITING FACTORS AND NEGATIVE CONSEQUENCES

The speed of the spread of artificial intelligence, in addition to the benefits it offers, also produces great uncertainty and uncertainty. It can improve the decision-making process, but it can also lead to mistakes. It helps in communication and decision-making, it gives much better quality and content information than humans, but it also depends on humans. Man is the one who should manage the tools of artificial intelligence and use its benefits. The problem arises if artificial intelligence starts to control humans and starts to develop itself (Đukic, 2023).

It is precisely for this reason that man and machine can be "outwitted", so it is necessary to resolve many dilemmas - ethical, legal, security - earlier. The European Union (EU) was among the first to try to establish rules and procedures to deal with the complex challenges arising from the development of artificial intelligence, such as the creation of original content, such as text, video and images. In this regard, in April 2021, the European Commission proposed, as part of its digital strategy, a new Regulation on Artificial Intelligence (Document 52021PC0206, Regulation of the European Parliament, Artificial intelligence Act, com/2021/206 final) with the aim of making the EU the world leader in reliable artificial intelligence. Also, the Council of the European Union, at the beginning of May 2024, confirmed the Act on Artificial Intelligence, the first law in the world that can set a global standard for the regulation of artificial intelligence. The goal of the new law is to encourage the development and acceptance of safe and reliable artificial intelligence systems in the single market of the European Union. At the same time, its goal is to ensure respect for the fundamental rights of EU citizens and encourage investment and innovation in the field of artificial intelligence in Europe. The new law distinguishes four types of artificial intelligence according to the risk it entails. Artificial intelligence systems with a very limited risk, such as video games or spam filters, will only have to meet mild transparency regulations, while high-risk AI systems will have to meet a series of requirements and obligations in order to be approved on the EU market. The law prohibits artificial intelligence systems that socially value and classify individuals into certain categories - by gender, gender identity, race, ethnic origin, migration status, citizenship, political belief, sexual orientation, religion, and the like.

It is important to note that the Law on Artificial Intelligence, the so-called The AI Act applies only to areas covered by EU legislation and provides for exemptions such as systems used exclusively for military and defense purposes, as well as for research purposes. The new law should be published in the Official Journal of the EU in mid-2024. The regulation will start to apply two years after its entry into force, with some exceptions for certain provisions of the law (EU Artificial Intelligence Act).

One of the limiting factors is that communication networks can be vulnerable, which can allow companies that provide the flow of information the ability to monitor, intercept, and possibly influence the collection and processing of information by AI. So, some time ago, the American technology company Meta announced that it wants to use the data of its users in Europe to train artificial intelligence models (<https://www.nezavisne.com/nauka-tehnologija/internet/Meta>).

Because of this, there is a certain concern among the intelligence community about the reliability of information and its sources, as well as the possibility of manipulation of the same. Large computer companies undoubtedly cooperate with intelligence-security and military

agencies of developed countries and develop special software packages of artificial intelligence that will only be at the service of customers. This will also be a special network that will probably be protected multiple times and that will draw basic data from global communications and have significant knowledge about events in the world, primarily of security interest, process them and give them to decision makers. The intelligence-security and defense sector with its analytical capabilities will largely use these opportunities with the need for continuous education of its personnel. Sharing information with partner agencies of the same country or exchanging information with countries handling a joint intelligence/defense operation based on AI-derived data will also require a lot of care and subtlety. Namely, in the first-mentioned segment there will always be a certain rivalry, while in the second one, the question of credibility, principledness, predominance, but also the management and direction of activities by a higher hierarchical level and countries that have a higher level of decision-making can be raised. By itself, artificial intelligence, which is in the function of analytical analysis and assessment, is not immediately dangerous. However, the use of artificial intelligence in a compact unit with certain weapons, in perspective, will require from the intelligence-security and defense sector not only constant monitoring of its use, but also adequate resolution of certain ethical, legal, security, military and other dilemmas and controversies.

4. CONCLUSION

Artificial intelligence is good on the one hand, and bad on the other. Either way, it's a powerful tool. The key question becomes how people should use these technologies. Autonomous weapons are increasingly present as implementers of AI decisions. Evidence of the use of AI in the intelligence, security and defense sectors is increasing. Documentary shows and series are even publicly shown on the possibilities of using different software packages that support AI through machine learning, computer vision and natural language processing. The expediency of using AI for this purpose is multidimensional in data analysis, recognition of possible threats and their bearers, and through the automation of the process of collecting and processing information. In the future, the development path of the use of AI in the work of the intelligence and defense community can be expected in several converging directions - technical-technological development will accelerate the flow of information, management process functions in the intelligence community will be improved according to the possibilities that AI increasingly provides, the decision-making period will be shortened, training and specialization of personnel will be a continuous process, the futuristic vision will include the development of operational intelligence centers with a minimum number of executive bodies where AI will perform a greater number of functions. Certain doubts and ambiguities will still remain and will relate to new and new technical challenges and their potential abuses, violation of privacy, ethical, legal, security, military and other issues. The need for more adequate legal regulation will be a constant imperative and challenge.

REFERENCES

Defence Artificial Strategy, (2022). V 1.0, June 2022, UK Ministry of Defence, <https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy>.

Document 52021PC0206, Regulating of the European Parliament, Artificial Intelligence Act, com/2021/206 final).

Đukic, S. (2022). Obavjestajne sluzbe i nova tehnologija, Banja Luka, *Evropski defendologija centar za naucna, politicka, ekonomska, socijalna, bezbjednosna, socioloska i kriminoloska istrazivanja*.

Đukic, S. (2023). Implikacije vjestacke inteligencije na obavjestajni rad, Banja Luka, *Zbornik radova, Naucna konferencija, Bezbjednosni izazovi, rizici i prijetnje u procesu nastajanja novog svjetskog poretka*, NUBL, Fakultet za bezbjednost i zastitu.

EU Artificial Intelligence Act, (2024), *Available from* <https://artificialintelligenceact.eu/the-act> .

<https://zastita.info/hr/novosti/ugradnja-umjetne-inteligencije-u-sigurnosnu-infrastrukturu-oznacava-strateski,35152.html>) . Accessed 2024-05-29.

Israel-defence-forces-response-to-claims-about-use-of-lavender-ai-database-in-gaza
Available from <https://www.theguardian.com/world/2024/apr/03/>. Accessed 2024-06-13.

Katz, B. (2020), Opportunities and Challenges from Emerging Technologies for U.S Intelligence, *Center for Strategic and International Studies (CSIS)*,1-8.

Miljkovic, M., Berisa, H. i Zgonjanin, S. (2023). Military Application of Artificial Intelligence, In: IX International Scientific Professional Conference Security and Crisis Management-Theory and Practice, Belgrade.

Palo.Alto. (2024). Meta-zeli-da-koristi-podatke-korisnika-u-Evropi-za-obuku-vjestacke-inteligencije/839312. *Available from* <https://www.nezavisne.com/nauka-tehnologija/internet/> Accessed 2024-06-12.