THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE DEFENSE SECTOR

Stefaniya Mircheska

Summary: *A general-purpose technology called artificial intelligence (AI) has the ability to transform every aspect of defence, from back-office enterprise services to delivering military effect. In the integrated review, at a time when the geostrategic landscape is increasingly complex and challenging, AI technologies are evolving rapidly and becoming more widely available to allies and potential adversaries alike. We cannot avoid the reality that conflicts - both in the physical and virtual realms - will be enabled by AI. Each country should introduce and make the best use of these. At this time, we are required to use these technologies safely and responsibly, in accordance with our legal commitments and the values and standards of the society we serve. All uses of AI to improve defense processes; systems or military capabilities are guided by our AI Ethical Principles.*

Key words: *AI definition, benefits, challenges, AI ethical principles, defense*

INTRODUCTION

The process of defending someone or anything against an aggressive attack is known as defense. Any nation's top priority when it comes to sustaining its existence is defense. Countries must always be vigilant against all threats, hazards, and attacks that could arise from both the inside and the outside. This justification is important enough to permit the nation to allocate a sizable portion of its budget to defense needs. Advanced weaponry and ammunition are provided to the armed forces of a country. These forces must constantly maintain the highest standards of alertness, readiness, and vigilance. The majority of the defense forces' responsibilities are made simpler by technology. Innovative concepts in this area facilitate efficient and quick development.

In order for a new technology to be effectively applied, it is necessary for the governments of each country to create conditions for their implementation and use. Globally, citizens' trust in government is at a very low level. (Stoykov, 2022). For this purpose, it is necessary for every government to work effectively to create trust in its citizens.

Over the past two decades, data, computing power, and machine learning advancements have all contributed to the global advancement of artificial intelligence (AI), which has been progressively getting better. As a result, AI is being applied more and more in a variety of industries' daily operations. Speech recognition, biometric authentication, mobile mapping, navigational systems, manufacturing, supply chain management, data collecting, transportation and traffic control, and targeted internet marketing are just a few of the numerous applications for this technology.

The worldwide defense and security landscape is evolving due to artificial intelligence (AI). It presents a once-in-a-lifetime chance to bolster our technical advantage, but it will also quicken the pace at which the challenges we confront materialize. The complete range of actions carried out by the Alliance in support of its three primary missions - cooperative security, crisis management, and collective defense - will probably be impacted by this underlying technology. AI is a broad term that refers to computer systems designed to mimic human intelligence. It can be programmed to learn, reason, problem-solve, perceive, and even interpret language. Two prominent subsets of AI are machine learning, where systems learn from data to improve their performance, and deep learning, a more complex form of machine learning modeled on the human brain. AI's potential in defense is vast. It can streamline operations, enhance decision-making and increase the accuracy and effectiveness of military missions. Drones and autonomous vehicles can perform missions that are dangerous or impossible for humans. By anticipating and recognizing dangers, analytics driven by artificial intelligence can offer strategic benefits. According to experts, artificial intelligence is a production component that could bring forth new opportunities for expansion and alter how various businesses carry out their operations. By 2035, artificial intelligence is predicted to boost the world economy by $15.7 trillion. Nearly 70% of the worldwide impact of the impending AI boom is expected to come from China and the US.

As the scientific field of "artificial intelligence" began to take shape in 1956, the term AI also refers to the technological phenomenon of contemporary intelligent systems that examine their surroundings and, to a certain extent, act independently to complete their given tasks. Essentially, artificial intelligence (AI) is defined as "a collection of technologies that combine data, algorithms, and computing power that has the potential to transform major sectors of industry, services, and society as a whole."

A key element in the realization that intelligent system implementation and the financial gains from data processing will become more and more important for Europe's well-being and sustainable economic growth is the continent's expanding computing infrastructure and the emergence of numerous large volumes of data.

The application of AI technologies, however, carries a number of potential risks, including lack of transparency in the decision-making process, invasions of privacy, illicit use, or just plain non-acceptance and rejection by the populace because of the need for ever-higher qualifications or apprehension about changes in the job market. The European Commission (EC) is dedicated to supporting scientific advancements, safeguarding the EU's technological leadership, and ensuring that new technologies will benefit all Europeans in a way that upholds their rights, all in the context of a global competition for a leading position in the development and application of AI. The European Commission extends an invitation to all member states to participate in creating a European "ecosystem" for AI development and utilization, all the while upholding people' rights and values.

The present approach to the development and application of AI is distinguished by a distinctive vision: technological advancement should be accompanied by a framework of laws and morality that ensures citizens' rights and security, as well as by actions taken to collect easily accessible data of the highest caliber, disseminate information widely, and provide equal access to the advantages of AI technologies. Additionally, a number of nations, including China, the United States, Russia, and Europe, want to lead the world in "trustworthy AI," which refers to AI applications that abide by moral standards and do not intentionally or unintentionally cause harm, even when used by non-technical individuals. In addition to encouraging business to provide goods and services where dependability is a competitive advantage, this would boost public confidence in European AI that has been developed in a special "ecosystem of trust." Innovation in AI, scientific discoveries, and fresh research will all be sparked by ethical standards. All nations will be able to create international AI standards in this way.

The ethical principles and related values that must be honored in the creation, implementation, and use of AI systems are stated as follows: protecting people's autonomy, preventing harm, fairness, and explainability. This is due to the rapidly accelerating global development of AI. In this context, the following essential standards have been specified for AI applications to meet in order to be trusted:

- human factor and supervision, AI-powered systems that don't affect a person's autonomy or have any negative side effects;
- each component of every site configuration should be reviewed for technical stability and safety, as well as for physical and mental safety on AI-powered devices
- data management and privacy; data must not reflect social biases and must be free of errors or inconsistencies;
- transparency and simplicity, in recording and registering the judgments made by the AI systems as well as the complete process that resulted in these decisions;
- monitoring of the social impact of artificial intelligence (AI) and the sustainability and environmental responsibility of AI systems, as well as the well-being of society and the environment;

responsibility, to guarantee accountability for AI systems and their outcomes and to reduce any potential harmful effects;

A number of guidelines and particular requirements are established with regard to the technical stability and safety of AI systems in relation to new species risks and vulnerabilities. These include potential hidden attacks through data manipulation and decision mechanisms, as well as misuses of the "black box" effect resulting from the application of machine learning and big data. The primary distinction between "traditional" information and management systems and artificial intelligence (AI) systems is that the former can oftennot explain why a certain model produced a particular result or conclusion or what combination of input components contributed to it. In these situations, the algorithms are compared to "black boxes," and it is suggested that they adhere to the "explainability" criterion, which is directly tied to the "transparency" requirement and is necessary to establish and preserve public confidence in AI applications. Procedures ought to be clear, AI systems' purposes and capabilities ought to be freely discussed, and decisions ought to be as fully explained as possible to people who may be impacted by them, whether directly or indirectly.

Other measures of explainability are also proposed (traceability, auditability and transparent communication about the capabilities of the system). The Self-Assessment Approach to AI Systems according to the seven key requirements is also based on a risk assessment in depending on the degree of criticality when using the AI systems and the solutions offered by them, the dependence on their correctness and the possible ones' harmful consequences.

1. DEFINITION AND REGULATION OF AI

The dynamic approach and speed of development of artificial intelligence leaves no possibility for a clear definition and research of the possibilities provided by these technological solutions. In scientific academia, there are different definitions regarding artificial intelligence and its applications. In its broadest definition, AI equates to algorithms. However, this is not a particularly useful approach for defining a new technology that is not entirely clear. Algorithms predate AI and have been widely used outside of the field.

“In order to accomplish a complex goal, artificial intelligence (AI) systems are software (and possibly hardware) systems created by humans that perceive their environment through data acquisition, interpret the structured or unstructured data that has been gathered, reason using the knowledge or process the information derived from this data, and determine the best course of action to take. Artificial intelligence (AI) systems can learn a numerical model or employ symbolic rules. They can also modify their behavior by examining the effects of their past choices on the surrounding environment.

Artificial Intelligence (AI) is a scientific field that encompasses various methods and approaches, including machine learning (deep learning and reinforcement learning are two examples), machine reasoning (planning, scheduling, knowledge representation and reasoning, search, and optimization), robotics (control, perception, sensors, and actuators, as well as the integration of all other techniques into cyber-physical systems), and optimization).[1]"

NATO regulation of AI – In October 2021, NATO Defense Ministers endorsed the NATO Artificial Intelligence (AI) Strategy, setting out how the Alliance seeks to adapt AI to meet operational requirements and accelerate and deploy the safe and reliable integration of AI across a range of Alliance capabilities. The AI Strategy is centered on the principles of the responsible use of AI in defence, with twin pillars of activities that will help the Alliance promote the development and adoption of AI, as well as defend against threats arising from this technology (Cullen, 2018). Also, in October 2022, NATO Defense Ministers approved the next set of policies to continue the implementation of the comprehensive Emerging and disruptive technologies **(**EDT's) strategy, including the establishment of the NATO Data and Artificial Intelligence Review Board and the NATO Autonomy Implementation Plan. The AI and Data Review Board serves to operationalize NATO's principles for the responsible use of AI as outlined in the NATO AI Strategy. The Autonomy Implementation Plan provides a coherent approach to NATO's efforts to protect and develop autonomy in accordance with the Alliance's norms, values and commitment to international law. Effective and accountable governance, in keeping with common values and international commitments, is necessary for the adoption of AI in the context of defense and security.

By developing and considering the deployment of AI applications, Allies and NATO make sure that these six principles are upheld:

- Legality: AI applications will be created and implemented in compliance with applicable national and international legislation, including human rights and international humanitarian law;

- Accountability and Responsibility: Appropriate judgment and care will be utilized in the development and deployment of AI applications; accountability is ensured by applying a defined human responsibility framework;

- Clarity and traceability: AI applications will employ suitable transparency and understandability, including the utilization of review

[1] For additional information: OECD. (2024). *Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449*. OECD Legal Instruments. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

processes, sources, and procedures. This covers national and/or NATO-level verification, evaluation, and validation procedures;

- Reliability: Use cases for AI applications will be precise and well-defined. Throughout these use cases, testing and verification of the safety, security, and resilience of such capabilities will be conducted, including through existing NATO and/or national level certification procedures;

- Controllability: Artificial intelligence (AI) applications will be created and utilized in compliance with their intended purposes. They will facilitate proper human-machine interaction, the capacity to recognize and prevent unintended outcomes, and the ability to take action, such as turning off or disabling systems, when they display undesired behavior.

European regulation of AI - After the definition of artificial intelligence at the global level, this technology and its applications have to be legally regulated in every European country. In 2023, the member states of the European Union were the first to start introducing a legislative framework with principles and rules for the use of this technology and the protection of human rights. Part of the EU's strategy for the development of the digital economy is the drive to regulate artificial intelligence. The aim is to simultaneously create suitable conditions for the development of technology and to protect consumers.

In April 2021, the European Commission proposed the first regulatory framework for artificial intelligence. It envisages assessing and classifying systems using the technology into groups according to the risk to which users are exposed. Higher risk systems will be subject to stricter regulations. The European Parliament's priority is that artificial intelligence systems in the EU are safe, with clear rules and a clear origin, do not discriminate against certain groups of people and do not harm the environment. Technology should be subject to human control, not automatic systems.

Parliament also wants to establish a single definition of artificial intelligence that is not tied to a specific technology and can also be applied to future systems. In that way, Parliament charts the EU's path to global leadership, and is defined as a global force in terms of the development of artificial intelligence. In this way, a favorable environment is ensured through the regulation of artificial intelligence. Currently, EU and national legislation is fragmented, decisions are taken slowly and there is a lack of legal clarity. In order to support innovation in this area and avoid imposing an excessive regulatory burden, only high-risk applications should be subject to regulation.

The main guidelines adopted by the European Parliament regarding the use of artificial intelligence for military purposes are the following:

- Artificial intelligence cannot replace either human decision-making or human contact;

- An EU strategy against lethal autonomous weapons systems is needed;

- Call for a ban on "highly intrusive social scoring apps" by public authorities; concern about "deep-fakes".

In addition to these basic guidelines, there are clearly spelled out rules where the basic premise is that artificial intelligence must be subject to human control, allowing humans to correct or disable it in case of unintended behavior. The fundamental tenet of artificial intelligence is that human rights and dignity must be upheld in all EU defense-related endeavors.

Artificial intelligence (AI)-enabled systems must provide people substantial control over them so they may accept responsibilities for their use. All nations are urged to engage with the UN and the international community to develop and advance a global framework that prohibits the use of AI for military objectives.

2. THE MAIN TECHNOLOGICAL SOLUTIONS IN DEFENSE SECTOR USED BY AI

The technological solutions used are defined as having to be useful for AI to be applicable. Its true value can only be realized when it provides useful insights. If we think about AI from the perspective of the human brain, then AI technologies are essential technological solutions that allow people's ideas to be implemented. Below in Figure 1 are some of the most widely used and rapidly developing AI technologies that find use in defense.

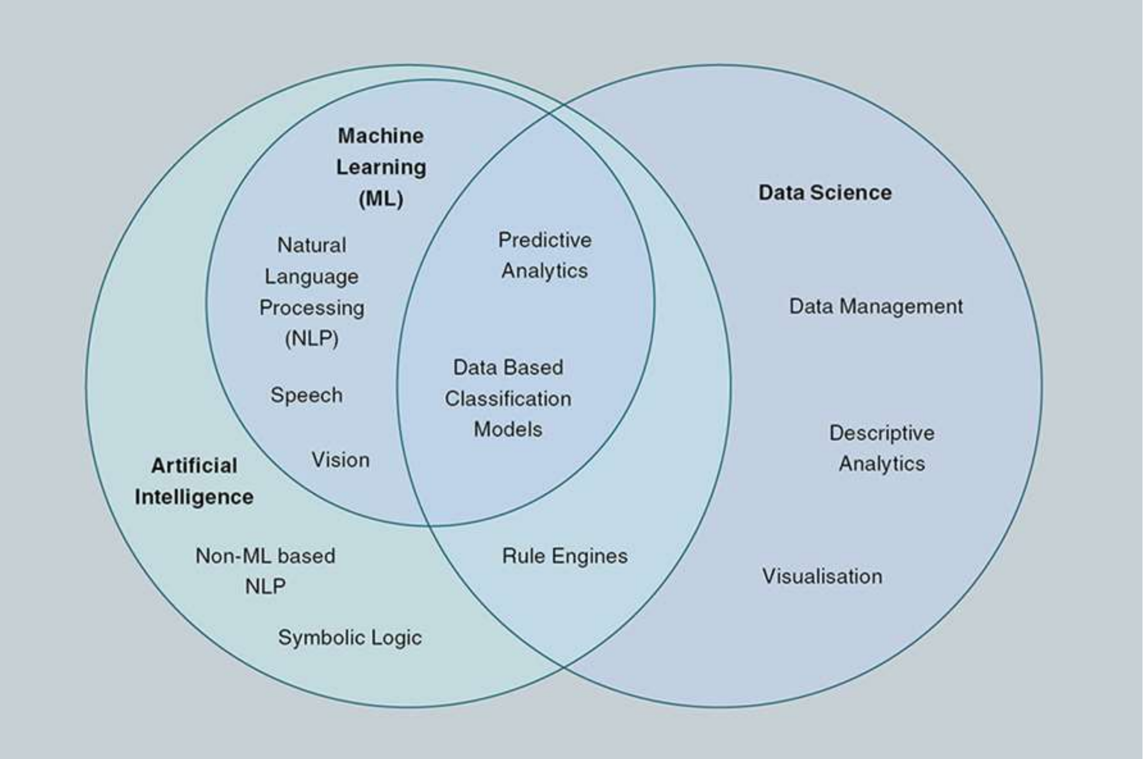

Figure 1. Main technological solutions. (*Source*: Szabadföldi, 2021)

Figure 1 shows the three main technological solutions on which artificial intelligence in defense is based.

1. The first is data science, which overlaps with the second and comprises predictive analytics, rule machines, data management, descriptive analysis, and models of data-based classification. One of the main applications of artificial intelligence is data processing. AI processing includes image recognition, deep learning, machine learning, and other techniques. These technologies' algorithms can be accessed by a third-party API, installed on a public or private cloud, found in a data lake, data center, or at the location of data collecting. These algorithms distinguish the current wave of AI from the previous one by being strong, adaptable, and capable of self-learning. The increase in raw power can be attributed to the implementation of graphics processing units (GPUs). Their aptitude for mathematics makes them an excellent option for data crunchers. Another exponential increase in AI performance is coming soon thanks to a new generation of processor units made especially for AI-related workloads.

2. Artificial intelligence, which includes symbolic logic, rule engines, and non-ML based natural language processing. The goal of the AI branch of machine learning is to replicate intelligent human behavior in order to carry out difficult tasks similar to human problem-solving. Machine learning relies on data, which encompasses text, numbers, and images. To give the machine learning model with training data, data is gathered and stored. The application performs better the more data it has. When the data is prepared, programmers select a machine-learning model to feed the data into, and the model learns to recognize patterns or forecast future events on its own. Over time, the programmer can adjust the model's parameters to help it generate more accurate results. To assess the model's accuracy when it is exposed to fresh data, some data is set apart from the training set. In the future, the model can be applied to different data sets. Three categories of machine learning exist (Das et al., 2015):

- Labeled data sets are used to train supervised machine learning models, which helps them accumulate knowledge and improve accuracy over time. To enable an algorithm to recognize dogs on its own, it may be trained with pictures of dogs and other items. Among the applications of supervised machine learning are spam detection and image categorization. Right now, this is the most often used kind of machine learning model.

- Unsupervised machine learning can identify trends and patterns in unlabeled data that consumers aren't actively looking for. An unsupervised machine-learning software that analyzes online sales data to distinguish between various customers who make purchases is an example of this. Additional examples of unsupervised machine learning applications are clustering and anomaly detection.

- By establishing a reward system, reinforcement machine learning teaches robots to make the best decisions through trial and error. Models are trained to play games and autonomous vehicles are trained to drive using reinforcement learning. By informing the machine when it has made the correct choice, it can gradually learn what steps to do. Among the applications of reinforcement machine learning include gaming and robotics control.

3. Machine learning, the third circle, completely fits inside the second circle and crosses over into it (Mason et al., 2012). Natural language processing, speech, vision, data-driven categorization models, and predictive analytics are all included in machine learning. A subfield of computer science called natural language processing, or NLP, aims to make computers comprehend spoken and written language in the same way that humans do. Deep learning, machine learning, statistics, and computational linguistics' rule-based modeling of human language are all combined in natural language processing (NLP). These technological advancements enable computers to fully comprehend human text and voice data. Natural language processing (NLP) is the field of computer programs that can translate text quickly between languages, understand spoken commands, and swiftly summarize enormous amounts of text in real time. It's conceivable that digital assistants and voice-activated GPS units have encountered you in NLP interactions. Additionally, NLP plays a significant role in enterprise solutions, which serve to simplify mission-critical business procedures, increase staff productivity, and streamline business operations. NLP activities deconstruct text and audio data to enable computers to comprehend what they are consuming.

3. BENEFITS OF AI IN DEFENSE SECTOR

Artificial Intelligence is a quickly evolving technology that, like computers, nuclear weapons, and airplanes, will transform military technology. The way artificial intelligence (AI) transforms defense technology will be directly reflected in the abilities of scientists and engineers to develop and construct new technologies and applications. Our vast data base is essential for creating and improving technical solutions. These data are gathered via the regular use of different military vehicles, ships, and airplanes. War games, digital simulation, and real-world defensive exercises and training can also produce AI data.

All accessible data, including all significant inputs and the methods and conclusions made, must be used to train the AI system. Data from a military field can be gathered and then put together to create an AI system. This can, in fact, preserve an accurate record of friendly forces and increase the safety of officers and other non-defense people. The use of AI is becoming essential to ensuring future security. It turns out that a country's ability to control military technology is crucial for retaining power over possible enemies.

AI has several important advantages for military operations, including (Johnson, 2020):

- Artificial intelligence is capable of compiling all the information gathered from several satellites and sensors and presenting findings. The defense personnel may be further empowered to decide what associated steps to conduct as a result.

- Currently, ships fitted with sonar are frequently employed to find mines beneath the surface of the ocean. However, as AI develops, submersible boats and other vehicles will be able to use AI to identify mines. Mine detection would happen more quickly. It would examine the object, recognize it, and make the appropriate choice.

- Artificially intelligent military robots may be able to perform operations or tasks all by themselves, perhaps saving human lives.

- The number of unmanned vehicles – such as battle tanks and airplanes – will undoubtedly increase. This will reduce costs, speed up decision-making, and remove an officer from potentially dangerous situations.

- Some of the land-based combat vehicles will integrate AI and machine learning in order to improve their targeting capabilities.

- Artificial intelligence (AI) can operate a drone on its own and help it take off and land without human assistance.

4. CHALLENGES OF AI IN DEFENSE SECTOR

AI has the potential to cause global instability and chaos in the defense sector, which has long been a driving force behind global development. AI in the defense can be a double-edged sword. It can also be a problem if it is not regularly checked by the relevant moderators and raters. The military of any country can be brought dangerously close to collapse by a small mistake or act of carelessness, which can cause international unrest or a dire situation that no one has foreseen.

The main risks, uncertainties and difficulties associated with artificial intelligence (AI) in the context of military applications and deployments are as follows:

- Ethical issues: Using AI in the military presents a number of ethical issues, one of which is the possibility that autonomous weapon systems may decide between life and death without human intervention. Making sure AI is used in military applications in accordance with moral norms and values is crucial.

- Reliability: Ensuring the reliability of AI in military applications is one of the major concerns. The quality and quantity of data used for training have a significant impact on the accuracy of AI models, and bias and errors in the data are a constant risk. Any errors in an AI system's output could have serious repercussions, especially in military operations.

- Cybersecurity: Because military AI systems are frequently networked with other systems, they are susceptible to hackers. The military's operations, personnel, and infrastructure could all be seriously harmed by the malevolent application of AI. Furthermore, it can be challenging to identify and stop cyberattacks driven by AI.
- Adversary attacks: These can cause AI systems to provide erroneous results by manipulating the input data. An AI system may be forced by adversarial attacks to identify targets incorrectly or provide misleading information in a military context.
- Public conception and perception: People are worried about the employment of AI in the military because they think it will replace human soldiers, reduce accountability, and put civilians at greater risk of damage.

Finally, while the integrity of AI augmentation and processing systems is a long-standing intelligence and strategic concern that predates the cyber age, it is especially susceptible to fraud. The disruptive consequences of disinformation campaigns could be significantly worsened by the combination of AI use and hostile actors' technology exploitation. Governments should take the lead in developing legal frameworks that specify how emerging technologies combine with the arsenal of misinformation weapons that they now possess, including social media. Although there was not enough time to conduct a more comprehensive analysis of an AI system's vulnerability, there were several signs and concerns of AI-related espionage throughout the tabletop exercise.

CONCLUSION

Artificial intelligence advancements will open up new possibilities for defense technology. In addition to improving military unit effectiveness, using artificial intelligence in military operations can increase the likelihood of winning a war. AI is being used by many countries throughout the world to improve defense force performance. Undoubtedly, AI is creating new opportunities for defense technologies. Although there are great hopes for the use of AI techniques in various military domains, there are still challenges and unanswered questions that need to be addressed in order for future research to live up to the hype.

Together with military prowess, artificial intelligence (AI) holds the greatest potential to profoundly impact the evolution and advancement of contemporary society. AI technology is currently going through a new phase of fast development. AI is the technology that has the greatest potential to change the disruptive technology landscape in the future, according to a number of governments and digital giants. Moreover, using them to improve national strategies and resources—like military applications - has become the norm. Progress is what we expect and what motivates our AI-assisted improvements.

The potential and applications of AI in the military are described, discussed, and evaluated. These applications include autonomous vehicles, cyber security, homeland security surveillance, autonomous weapons and target recognition, cybersecurity, surveillance, military transportation and logistics, and combat training and simulation. However, when utilizing AI in the military, the following challenges need to be taken into account:

- Vulnerabilities that could seriously impair the system's performance;
- Openness to ensure that the model operates in accordance with military requirements;
- Insufficient training data for machine learning (ML);
- Impact of AI on nuclear danger and international strategic stability.

All things considered, artificial intelligence (AI) has the potential to become a double-edged sword that could harm rather than aid a country if it is not applied appropriately in the military with the assistance of the right hand. Nevertheless, a more extensive needs assessment is required to fully comprehend the utilization. Legislative restrictions, risk, and data quality can all vary significantly for the military, and some elements of transparency might not even be relevant. Before we can decide how AI will be used in the military and what other uses it might have, more information and research are required. To make AI more understandable in military contexts and to fully enhance its capabilities, more research is needed.

BIBLIOGRAPHY:

Стойков, С. (2022). Дилема на (не)сигурността и добавената стойност на образованието за сигурност. *Сигурност и отбрана,* (2), 58-81. https://institute.nvu.bg/sites/default/files/inline-files/2022-2-04-stoykov.pdf // Stoykov, S. (2022). Dilema na (ne)sigurnostta i dobavenata stoynost na obrazovanieto za sigurnost. *Sigurnost i otbrana*, (2), 58-81. https://institute.nvu.bg/sites/default/files/inline-files/2022-2-04-stoykov.pdf

Cullen, P. J. (2018). *Hybrid Threats as a New'wicked Problem'for Early Warning*. Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-2018-8-Cullen.pdf

Das, S., Dey, A., Pal, A., & Roy, N. (2015). Applications of Artificial Intelligence in Machine Learning: Review and Prospect. *International Journal of Computer Application, 115*(9), 31-41. DOI=10.5120/20182-2402. https://research.ijcaonline.org/volume115/number9/pxc3902402.pdf

Johnson, J. S. (2020). Artificial Intelligence: A Threat to Strategic Stability. *Strategic Studies Quarterly, 14*(1), 16-39.

https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-14_Issue-1/Johnson.pdf

Mason, R., McInnis, B., & Dalal, S. (2012). Machine learning for the automatic identification of terrorist incidents in worldwide news media. *2012 IEEE International Conference on Intelligence and Security Informatics* (pp. 84-89). Washington, DC: IEEE. doi: 10.1109/ISI.2012.6284096

NATO Allied Command Transformation Operational Experimentation. (2020). *Military Uses of Artificial Intelligence, Automation, and Robotics (MUAAR).* Retrieved March 19, 2021, from https://www.act.nato.int/wp-content/uploads/2023/05/2020_mcdc-muaar.pdf

NATO Science & Technology Organization. (2020). *Science & Technology Trends 2020-2040*. Retrieved March 19, 2021, from https://www.sto.nato.int/pages/tech-trends.aspx

OECD. (2024). *Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449*. OECD Legal Instruments. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Szabadföldi,I. (2021). Artificial Intelligence in Military Application – Opportunities and Challenges. *Land Forces Academy Review, 26*(2), 157-165. https://doi.org/10.2478/raft-2021-0022