# Application of artificial intelligence in modern weapon systems - opportunities and threats in armed conflicts

Zbigniew Małodobry[1], Karolina Nastaj-Sałek[2], Katarzyna Cyrkun[3], Wojciech Jakubiec[4]

[1]University of Rzeszów
*Poland*

[2]State Vocational University of prof. Stanisław Tarnowski in Tarnobrzeg
*Poland*

[3]Military University of Technology
*Poland*

[4]Bielsko-Biala University of Applied Sciences
*Poland*

*Abstract*— **The aim of the work is to analyze the role of artificial intelligence in modern weapon systems, taking into account its potential, threats and ethical challenges. The main objective of the article is to assess the impact of AI on the effectiveness of military operations, security, as well as the potential in the context of weapon autonomy and international regulations. Research problems focus on questions about the impact of AI on decisions made during armed conflicts, threats related to autonomous weapon systems and ethical and legal challenges related to their use. Research hypotheses assume that the implementation of AI can increase the precision and effectiveness of military operations, but at the same time lead to serious challenges in terms of responsibility and the risk of conflict escalation. The research was conducted using the qualitative method, based on the analysis of the literature on the subject and reports on the use of AI in the armies of various countries. The research tool was a review of case studies and analysis of international documents. The conclusions emphasize the need to create international legal regulations regarding the use of AI in weapons to ensure responsible and safe implementation of this technology in the army.**

**Keywords— artificial intelligence, autonomous weapon systems, modern weapon systems, new technologies.**

## I. INTRODUCTION

The modern world is undergoing a dynamic technological revolution, of which artificial intelligence has become one of the most important pillars. Artificial intelligence is entering almost every sphere of life - from medicine, through education, to industry and entertainment. In particular, its application in the defense sector causes both excitement related to new possibilities and serious concerns about potential threats. Military weapon systems based on AI are opening a completely new chapter in the history of military operations. With the ability to process huge amounts of data and make decisions in fractions of seconds, AI is becoming a tool that can significantly affect the way wars are fought. From precision drones to autonomous combat vehicles - new technologies offer the potential to increase the effectiveness of military operations, minimize human losses and optimize costs. However, along with these possibilities, questions also arise about the limits of its application. What are the ethical and legal consequences of entrusting machines with life and death decisions? Can we be sure that these systems will always act in accordance with the intentions of their creators? Moreover, the development of autonomous combat technologies contributes to a new arms race, in which the stakes are global military superiority. The possibility of using artificial intelligence in modern weapons poses one of the greatest challenges of modern civilization. Therefore, it is worth considering whether it will be possible to use this technology in a responsible manner, in accordance with the principles of law and ethics, or will it become the cause of uncontrolled development of autonomous weapons with catastrophic consequences for humanity? This article attempts

**ASEJ** - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 28, No 4 (2024), pages 5
https://doi.org/10.19192/wsfip.sj4.2024.8
Received: September 2024, Accepted: December 2024,
Published: December 2024

to understand both the potential and the risks associated with the development of AI in the military sector, and analyzes the need for international cooperation in the regulation of this technology.

## II. Machine learning and artificial intelligence

Artificial intelligence (AI), also known as AI, has yet to be clearly defined. It is most often described as “intelligence displayed by machines, as opposed to the natural intelligence observed in humans and animals.” To better understand this concept, it is worth distinguishing two main types of AI: the so-called strong AI and weak AI. Strong AI usually brings to mind the image of AI that appears in the imagination of most people. In turn, weak AI refers to advanced algorithms that have been designed to perform specific tasks in clearly defined domains. Although strong AI remains theoretical for now, the development of weak AI has accelerated in recent years thanks to technological progress, including research on machine learning (ML) and data engineering (M. Nowakowski, 2023, p. 26).

It is worth mentioning that machine learning, which is an important element of building intelligent systems, is already a well-known process. Instead of creating a computer program based on a mathematical model, a data system is developed that, thanks to processing numerous examples, can generate its own models and classifiers. In this case, huge amounts of data replace the traditional mathematical model. For example, a few kilobytes of code in a modern programming language are enough to implement basic arithmetic operations such as addition, subtraction, multiplication or division. Meanwhile, an ML system would need billions of parameters or data to obtain correct results in the same range (M. Nowakowski, 2023, pp. 27-28).

It is worth mentioning that although arithmetic can be relatively easily modeled mathematically, tasks such as facial, voice or emotion recognition go beyond the capabilities of standard branches of mathematics such as algebra, analysis or geometry. For example, speech recognition systems require processing over 500 billion parameters. In such cases, ML models show a significant advantage. The type of model plays an extremely important role in machine learning. It is the model that determines how the AI learns, the type of data it can process, and the type of questions it can answer for itself. Designing and selecting appropriate models for specific problems is one of the most important challenges in data engineering. Models must be advanced enough to capture complex relationships and structures, but at the same time simple enough to be implemented effectively (B. Fischer, A. Pązik, M. Świerczyński, 2023, p. 256).

On the other hand, NN neural networks are a type of machine learning model that is modeled on the structure of neurons in the brain, which allows for performing calculations and predicting results. Neurons in networks are arranged in layers, each of which performs a set of simple calculations and sends the result to the next layer. Thanks to this organization of layers, it is possible to perform more complex calculations. A simple network with several layers of neurons is enough to reproduce basic classification functions ( V. Matlach, 2023, p. 114).

Deep neural networks DNN are more complex structures that consist of dozens or even hundreds of layers. Such networks are able to create very advanced models that can learn complex dependencies without the need for humans to define them. This allows the development of algorithms capable of solving various problems. An important aspect of neural networks is the training process. The "memory" of the model is a set of numerical parameters that determine how to generate answers to the questions asked. Model training involves adjusting these parameters to obtain the best results (S. Nikiel, 2022, p.7).

In turn, the data used to train neural networks can include millions of examples, both correct and incorrect. There is no single analytical solution to this process. However, you can start with a simple neural network model and then improve it by making incremental corrections. One of the tools supporting this process is the evaluation of classifiers and the use of so-called "scores". The extremely large variety of machine learning models is based on this concept. The most difficult challenge is to develop an effective "score" for training the network. One very effective way to train neural networks is to use another neural network. This technique, known as generative adversarial networks (GANN), involves using two cooperating networks. The first network generates data randomly, while the second, trained, tries to distinguish real from fake data using examples of real data. These two networks compete with each other. In turn, the generative network aims to create convincing fakes, while the discriminative network tries to distinguish authentic data from fabricated ones. This technology has gained enormous popularity in recent years and is used in projects such as GPT-3 (Open AI), AlphaGo and DeepMind (S.Nikiel, 2022, pp. 7-9).

Similar solutions were developed by the Pentagon as part of the Maven project, which aimed to create image recognition systems for military drones. However, in 2018, after numerous protests and opposition from employees, Google withdrew from this project. This situation sparked a heated debate on human rights and the morality associated with the development of AI for military purposes. Although the controversy surrounding the Maven project has died down over time, calls for increased use of AI in defense have become increasingly loud in recent years (C. Demarest, 2022, p. 45). It is worth mentioning that in order to reduce concerns, the US Department of Defense has developed guidelines for the so-called responsible AI, which require AI developers to comply with ethical principles. NATO has also implemented an AI strategy, which includes voluntary ethical guidelines for its members. All the documents described above encourage the use of AI in a lawful, responsible, reliable and traceable manner, while trying to eliminate biases built into algorithms (R. Kopeć 2017, p. 76).

## III. Advantages of using AI in weapons

The use of artificial intelligence (AI) in weapons brings a number of benefits that significantly change the face of modern warfare. The introduction of modern AI-based technologies increases the efficiency of military operations, reduces the risk to personnel and allows for better use of available resources.

In turn, one of the most important advantages is the increased precision and effectiveness of operations. AI algorithms are able to analyze huge amounts of data in real time, which allows for quick identification of targets and making accurate operational decisions. This minimizes side effects, such as civilian casualties or damage to infrastructure. The accuracy of AI-based combat systems contributes to increased safety of both soldiers and bystanders (K. Kowalczewska, 2021, p. 35).

Artificial intelligence significantly affects the speed of decision-making. In situations where every minute counts, systems based on AI exceed the capabilities of human command. An example is missile defense systems that analyze the trajectories of enemy missiles and immediately initiate appropriate actions before the threat has time to materialize. Another advantage is the reduction of risk for military personnel. The use of autonomous combat systems, such as robots, allows operations to be carried out in difficult and dangerous conditions without endangering the lives of soldiers. Thanks to this, the armed forces can carry out complex missions in conflict zones that would previously have been unattainable or would have involved high risk. The introduction of AI to armament also contributes to the optimization of costs and efficiency of military operations. Although the development and implementation of systems based on artificial intelligence is associated with high initial costs, in the long term their use allows for reducing expenses. AI supports resource management, improves logistics and reduces the need to engage large military contingents, which significantly reduces operating costs (K. Cyrkun, 2023, p. 9).

The ability to learn on their own is another advantage of technologies using AI. These systems can adapt their activities to changing conditions, constantly analyzing new data and modifying their strategies. As a result, they become more effective with each subsequent use, which is a significant advantage in dynamic combat environments. In summary, artificial intelligence enables the prediction and prevention of threats. Analytical algorithms are able to identify patterns in intelligence data, which allows for earlier detection of potential attacks or enemy actions. This type of forecasting can play a key role in preventing conflicts and improving security at the strategic level (M. Górka, 2018, p. 12).

## IV. Threats related to the autonomy of combat systems

Autonomous combat systems, although they offer many advantages, also carry a number of major threats that raise concerns both in the technological and ethical sphere. One of the greatest challenges is the limited control over the operations of such systems. Autonomous algorithms, based on data and previously programmed rules, can unexpectedly make decisions that are not in line with the intentions of their creators or operators. In dynamic combat conditions, where situations are often unusual and unpredictable, such errors can lead to tragic consequences (K. Anderson 2013, p. 111).

The possibility of unauthorized entities, such as hackers or terrorist groups, taking control of autonomous systems is no less dangerous. Cyberattacks on weapon systems can lead to their misuse or directing them against one's own armed forces. In response to this, ensuring a high level of cybersecurity and constant monitoring of autonomous systems in order to prevent such incidents is a key challenge (K. Boruszak 2019, p. 24).

It is worth mentioning that there are also significant threats related to the arms race in the field of autonomous weapons. Countries that invest heavily in the development of technologies such as the United States, China or Russia may contribute to the destabilization of global security. The development of autonomous weapons without international regulations may lead to the escalation of conflicts, where decisions made by machines will be difficult to predict or control. The ethical aspects of the autonomy of combat systems also cannot be ignored. The decision to use lethal force should belong solely to humans, but fully autonomous systems can perform their tasks without human interference. This raises questions about the responsibility for the actions of such systems and their compliance with international humanitarian law. An example would be a situation in which an autonomous drone hits a target, causing accidental civilian casualties - who is then responsible? (I. Oleksiewicz, 2019, p. 68).

## V. Ethical dilemmas

The use of artificial intelligence (AI) in modern weapons systems raises numerous ethical dilemmas, which concern both the issue of responsibility for decisions made by machines and the risks associated with weapon autonomy. As technologies for the military use of AI become increasingly advanced, questions arise about the moral, social and legal consequences of using such systems on the battlefield (K. Nastaj-Sałek 2023, p. 6).

One of the important issues is the issue of responsibility. Traditionally, people, not machines, are responsible for making decisions regarding the use of force, including possible violations of international law. In the case of autonomous weapons that use AI to make decisions about attacks, the question arises: who is responsible when the system makes a mistake, leading to civilian casualties or violating the principles of proportionality? This is a fundamental challenge, because in the case of autonomous systems, decisions are made by algorithms, not by humans, which makes it difficult to assign responsibility (K. Kowalczewska, 2021 p. 150).

Another dilemma is the issue of the morality of decisions made by AI. According to international law, all military actions must be proportionate to the threat and, importantly, aimed solely at military objectives. The use of artificial intelligence in weapons systems that can make decisions on the use of force independently raises concerns about whether the machine will be able to accurately assess what constitutes a military objective and what is a civilian one. In conflict situations, where this distinction can be difficult, autonomous systems may not be able to meet the requirements of the law of war, which creates a risk of unintended casualties among the civilian population (W. Niewiadomski 2019, p. 87).

An additional problem is the potential escalation of conflicts. The introduction of autonomous weapons may lead to an arms race, as states may strive to develop increasingly advanced technologies to maintain the advantage of military autonomy. This may lead to a situation in which the use of AI in war becomes the norm, and thus the risk of international escalation increases. In addition, easier access to autonomous weapons technology may increase the threat from terrorist organizations or other non-state actors who will use these technologies to achieve their own goals, which poses a serious threat to global security (A. Żebrowski 2017, p. 71).

Another key dilemma is the loss of control over decisions made by autonomous systems. Although initially the technology may be programmed to operate in a strictly defined manner, over time there may be a risk that these systems will be able to modify their algorithms and make decisions beyond the reach of human control. In a situation where autonomous systems operate unpredictably or outside the programmed rules, control over the conflict becomes extremely difficult, and responsibility for unintended consequences becomes even more unclear.

An extremely important issue is the transparency and supervision of AI-based weapon systems. Since many countries treat the development of autonomous weapons as a matter of national security, details about these technologies often remain classified. This raises the question of whether there are sufficient international oversight mechanisms to ensure that autonomous weapons are used in accordance with international law of war and ethical standards. Inadequate or non-transparent management of such technologies can lead to human rights violations or deepening inequalities between countries (E.D. Denning 2002, p.150).

From an international perspective, the use of AI in weapons systems also raises questions about compliance with existing conventions and treaties. Although there are some international norms governing the use of weapons in armed conflict, technology is developing rapidly and legal provisions often fail to keep up with new threats. The lack of global consensus on ethical and regulatory norms in the context of AI in weapons systems can lead to serious international tensions. Finally, one cannot forget the complex moral issues related to the very purpose of war. AI in weapon systems can be used to precisely attack targets, which can reduce casualties, but the question of whether war should be fought using technology in which human control is minimized remains unanswered. In the long term, it may turn out that the development of autonomous weapons will eventually transform the very rules of warfare, turning it into a more dehumanized and technological process (J. Wrona 2020, p. 206).

## VI. CONCLUSIONS

In the context of the development of military technologies, such as autonomous weapon systems, questions also arise about the long-term effects on the global balance of power. Without clear regulations and a transparent framework, countries may try to maintain a technological advantage, leading to the risk of an arms race. In such a scenario, not only states but also irregular military groups could gain access to this technology, which increases the risk of global crises and increasing instability. A key aspect that is still not fully resolved is the creation of international regulations that could set boundaries for the use of artificial intelligence in military weapons. International organizations such as the UN can play an important role in creating standards to monitor the use of these technologies. Traditionally, war has been determined by human decisions, but as technologies become increasingly autonomous, it is necessary to introduce control mechanisms that ensure compliance with international law and ethics. Taking joint action to control and regulate AI in the defense sector can help reduce the risk of escalation of armed conflicts and prevent potential abuses related to autonomy in making life-and-death decisions. Examples of such initiatives as NATO or the US Department of Defense guidelines on the responsible use of AI are a step in the right direction, but require further development and expansion to the global level. The use of AI in modern weapon systems opens up a number of new opportunities for humanity, but also serious threats. On the one hand, this technology allows for increased precision, efficiency and safety of military operations, as well as optimization of resources and rapid decision-making in crisis situations. On the other hand, autonomous combat systems can lead to unpredictable effects, uncontrolled escalation of conflicts, and also pose a threat to the basic principles of international law and ethics. Without appropriate regulations and international cooperation, AI in weapons can become a tool of destabilization, which on the one hand brings benefits, and on the other - creates the risk of irreversible consequences for all of humanity. Only through a responsible approach and transparency will it be possible to minimize the risks associated with these modern technologies, and their use in a manner consistent with the principles of law and ethics can contribute to greater global security.

## VII. REFERENCES

Anderson K., M.C. Waxman, (2013), Law and Ethics for Autonomous Weapon Systems: Why a Ban Won’t Work and How the Law of a War Can, Columbia Law School, New York.

Boruszak K., (2019), Cybersecurity of Poland in the Context of the Security Strategy of the European Union, Adam Marszałek Publishing House, Toruń.

Cyrkun K. (2023), International Practice of Using Innovative Weapon Systems in the Armed Forces in the 21st Century, [in:] K. Śmiałek, W swobodek, (eds.), Armed Forces Facing New Challenges and Threats, FNCE, Poznań.

Demarest C. (2022), Pentagon’s AI, data office fully operational as leadership posts filled, Pentagon.

Denning E.D., (2002) Information Warfare and Information Security, WNT Publishing House, Warsaw. Fischer B., Pązik A. (2023), Świerczyński M., Law of Artificial Intelligence and New Technologies 2, Wolters Kluwer, Warsaw.

Górka M. (2018), Cybersecurity as a Challenge for the Modern State and Society, in: T. Dębowski, Cybersecurity as a Challenge of the 21st Century, Archeae-Graph, Łódź-Warsaw.

Kopeć R. (2017), Codes of Ethics of Combat Robots, in: War/Peace – Humanities in the Face of the Challenges of Modernity, ed. R. Sapeńko, P. Pochały, Zielona Góra.

Kowalczewska K. (2021), Artificial Intelligence at War, Wydawnictwo Nauowe Schoolar, Warsaw.

Matlach V. (2023), Introduction to Data Processing 1, Palacký University Olomouc, Olomouc.

Nastaj-Sałek K. (2023), Legal aspects of the use of artificial intelligence in military armament in the 21st century, [in:] K. Śmiałek, W swobodek, (ed.), Armed forces facing new challenges and threats, FNCE, Poznań.

Niewiadomski W. (2019), Cyber threats to the European Union, University of Economics Publishing House, Katowice.

Nikiel S. (2020), Artificial Intelligence in war - Autonomous Weapon Systems, [in:] International Journal of Slavic Studies, no. 4

Nowakowski M. (2023), Artificial intelligence. A practical guide for the financial innovation sector, Wolters Kluwer, Warsaw.

Oleksiewicz I. (2019), Outline of the cybersecurity policy of the European Union. The case of Poland and the Federal Republic of Germany, Elipsa Dom Wydawczy publishing house, Warsaw.

Wrona J. (2020), Cyberspace and international law. Status Quo and Perspectives, Wolters Kluwer, Warsaw.

Żebrowski A. (2017), Determinants of Information Warfare, UP, Kraków.