Artificial intelligence, its application and development prospects in the context of state security

Igor Britchenko [*] [1] [A]; Krzysztof Chochowski [2] [B]

*Corresponding author: [1] Dr, Prof., Professor of the Department, e-mail: ibritchenko@gmail.com, ORCID: 0000-0002-9196-8740
[2] Dr, prof., Professor, e-mail: krzysztof.chochowski@onet.pl, ORCID: 0000-0003-3198-9619

[A] University of Security Management in Košice, Slovakia
[B] State Higher Vocational School Memorial of Prof. Stanislaw Tarnowski, Poland

Received: September 2, 2022 | Revised: September 20, 2022 | Accepted: September 30, 2022

DOI: 10.5281/zenodo.7128906

Abstract

Today, we observe the process of the constant expansion of the list of countries using AI in order to ensure the state of security, although depending on the system in force in them, its intensity and depth of interference in the sphere of rights and freedoms of an individual are different.
The purpose of this article is to define what is AI, which is applicable in the area of state security, and to indicate the prospects for the development of AI. The historical method was used as the leading one in the research process, supported by the comparative method and the dogmatic method.

Key words: intelligence, security, development, system.

Introduction

Security was, is and will be one of the basic human needs. The state is naturally predestined to satisfy it. Various authorities and its structures perform a number of functions and tasks in the area of security, while increasingly using ICT and artificial intelligence (hereinafter referred to as AI for short).

Results and Discussion

What is Artificial Intelligence (AI)

Artificial intelligence is used not only in the scientific discourse, but also in the mass media and colloquial conversations. Often it is done automatically and without reflection, so it often happens that the interlocutors when using this term do not mean the same. This creates communication problems and is a factor that hinders an effective approach to solving various types of problems and challenges related to artificial intelligence. For this reason, it seems reasonable to present the genesis and some basic definitions of AI.

It is commonly assumed that the "father" of AI is the British scientist, mathematician and cryptologist A. Turing, who in the article *Computing Machinery and Intelligence* asked the question whether machines can think and presented a test to answer it, later called the Touring test. (Touring, 1950, pp. 433-460). As emphasized by I. Szpotakowski and M. Kalinowski, this scientist should be associated primarily with the Touring machine and the mentioned Touring test, whose task is to test the intelligence of a given software and qualify it as intelligent or not. (Szpotakowski, Kalinowski, 2021, p. 50).

The English term (Artificial Intelligence) was introduced into the scientific circuit in 1956 by J. McCarthy during the conference in Dartmouth, describing it as the science and engineering of creating intelligent machines. In turn, W. Furmanek believes that the concept of artificial intelligence should be understood as a branch of computer science, within which remote computers can perform activities that are usually the domain of people, especially those requiring the use of human intellect

or logic (Furmanek, 2018, p. 277). N.J. Nilsson, on the other hand, believes that artificial intelligence (AI) is a field of computer science that tries to build improved intelligence into computer systems (Nilsson, 2010).

In OECD and EU documents, we can also find attempts to define the concept of *artificial intelligence*. Well, in the communication of the European Commission to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions of April 25, 2018 *Artificial Intelligence for Europe* , it was stated that the term artificial intelligence refers to systems that demonstrate intelligent behavior by analyzing the environment and taking action to some extent autonomously to achieve specific goals. (communication from the commission to the European parliament, the European council, the European economic and social committee and the committee of the regions artificial intelligence for Europe – publications office of the EU (europa.eu)). In turn, in the OECD Council Recommendation on Artificial Intelligence OECD / LEGAL / 0449, the OECD defines an artificial intelligence (AI) system as: a machine-based system that can, for a specific set of human-defined goals, make forecasts, recommendations, or make decisions affecting real or virtual environments. (OECD Legal Instruments).

As you can see, no single, universal and universal definition of AI has been developed. We should therefore share the thesis of W. Fehler, A. Araucz-Boruc, A. Dan and A. Lasota -Kapczuk that "Artificial intelligence has been the subject of research for over 50 years, but so far no uniform and generally accepted definition of it has been developed". (Fehler, Araucz-Boruc, Dana, Lasota-Kapczuk, 2021, p. 278). A convergent view is presented by M. Rojszczak, who states that "Despite the multitude of publications and research on the issue of AI, so far no universally accepted definition of the term" artificial intelligence "has been introduced. In practice, this concept covers a number of different applications, often related to machine learning (ML) systems. Machine learning, however, is a broader term than artificial intelligence and covers all solutions based on algorithms capable of building their own conclusions based on available information. (...) However, it would be a mistake to try to equate machine learning systems with artificial intelligence systems. The latter are seen as the next stage of evolution after machine learning. As the characteristic of ML systems is the ability to discover knowledge, the distinguishing feature of AI systems is the ability to make independent decisions". (Rojszczak, 2019, p. 3).

K. Kowalczewska therefore rightly points out that "The numerous functional definitions of artificial intelligence can be broadly divided into those that focus on the possibility of mapping (simulating) rational (human) reasoning (thinking) or rational (human) behavior". (Kowalczewska, 2021, p. 30).

It is also worth quoting the Ethics Guidelines for Trustworthy Artificial Intelligence, formulated by an independent group of experts on April 8, 2019. According to them, "Trustworthy artificial intelligence has three features that must characterize the system equipped with it throughout its life cycle: a) it should be legal, i.e. comply with all applicable laws and regulations, b) it should be ethical, ensuring compliance with ethical principles and values, and c) it should be sound both technically and socially, as AI systems can cause unintended harm even when used in good faith". (Ethics guidelines for trustworthy AI Shaping Europe's digital future (europa.eu) p. 2).

Experts then state that "The development, implementation and use of AI systems should be ensured in accordance with the requirements for trustworthy artificial intelligence: 1) human leadership and supervisory role, 2) technical reliability and security, 3) privacy protection and data management, 4) transparency, 5) diversity, non-discrimination and justice, 6) social and environmental well-being, and 7) responsibility". (Ethics guidelines for trustworthy AI Shaping Europe's digital future (europa.eu) p. 3).

The above-presented exemplary definitions of AI do not exhaust this broad and complex issue. The author, however, agrees with the OECD definition, according to which AI is a machine-based system that can, for a specific set of human-defined goals, make forecasts, recommendations, or make decisions affecting real or virtual environments. However, it is important to bear in mind also the issues raised by the group of experts of the European Commission regarding the creation of

trustworthy AI. In this way, it is possible to avoid the use of AI to achieve unethical and non-humanitarian goals. (For more on this, see e.g. Haugeland 1985; Luger & Stubblefield, 1993; Świerczyński, Więckowski, 2021).

Application of artificial intelligence (AI)

Artificial intelligence has its application both in the military and non-military dimension of security. Regarding the non-military use of AI in the sphere of security, it should be noted that one of its main areas is the control and management of both land and sea traffic. Traffic light systems in large cities or AI-controlled ship traffic management systems directly translate into an increase in the level of security.

AI is also used to forecast the development of fires, which makes it easier to contain and extinguish them, or to prevent and combat infectious diseases, which was particularly evidenced by the COVID-19 pandemic. and the judiciary. AI is also used to control and supervise the condition and efficiency of critical infrastructure, with the help of drones controlled by it. AI is also useful in conducting rescue operations and removing the effects of natural disasters, or in the process of training uniformed services. These are just some examples of the non-military use of AI in the security sphere.

The military use of AI covers many different planes, ranging from reconnaissance and identification systems, through support for military logistics management, to direct combat management.

The use of AI enables the integration and faster analysis of data and information collected by the reconnaissance complex (HUMINT, OSNIT, INTEL, etc.). Intelligence, surveillance and reconnaissance – this is the nervous system of every modern army. (For more see e.g. Matela, 2021, p. 238 ff.). This is important for maintaining the continuity of the decision loop and for leaders (decision makers, commanders) to make optimal decisions at a given moment. A convergent view is presented by W. Fehler, A. Araucz-Boruc, A. Dana, A. Lasota-Kapczuk, who claim that "AI systems, due to the speed and scale of the processed data, can provide information support for decision-makers. Also, integrated command support systems (Battlefield Management Systems, BMS), applied at various levels, are becoming more and more common". (Fehler, Araucz-Boruc, Dana, Lasota-Kapczuk, 2021, p. 283.).

Artificial Intelligence is playing and will continue to play an increasingly important role in the military use of space. Satellite constellations, including AI-managed microsatellites, will play a key role in defense systems against hypersonic weapons, the dynamic development of which we are currently observing. AI will also be used for the economic exploitation of space, in particular in the context of obtaining energy, thus ensuring the energy security of a given country or bloc of countries, e.g. by obtaining Hel_3 resources from the Moon.

The use of AI in space will increase, because already today there are hundreds of satellites (some inactive) enabling, for example, precise navigation and guidance of precision weapons (GPS). Therefore, they are the source of the advantage of the side of the conflict that has them. For this reason, fearing the cosmic Pearl Harbor, it is expected to use AI to minimize the possibility of carrying out such an attack and its possible consequences. (Bartosiak, Friedman, 2021, p. 179 et seq.).

Artificial Intelligence is used in information warfare, using it, for example, to identify agents of influence, overlaying the narrative of the hostile center of power on their own statements, while analyzing the degree of coherence and convergence of the message. It is also possible to identify the most active "resonance boxes", which often unknowingly engage in hostile propaganda messages, which in turn makes it possible to take appropriate educational and preventive measures against them. Such actions can be observed during the ongoing war in Ukraine, where Ukrainian special services – in particular the SBU – track, identify and eliminate entire networks of agents working for Russia, and cleanse their own ranks of traitors. Moreover, in the ongoing struggle for the hearts and minds of Ukrainian society and the sympathy of the international public opinion, thanks to AI it became possible to identify extras pretending to be the Ukrainian population or Ukrainian soldiers who act for the needs of Kremlin propaganda and take part in staged scenes, recorded and then disseminated

primarily in the Russian media. It is also used to define the identity of war criminals who murder civilians and captured Ukrainian soldiers and representatives of other uniformed formations.

AI is also used, on the one hand, in creating, and on the other, pointing to the deep fake. As indicated by A.K. Olech and A. Lis, "The term" deep fake "is used to" refer to realistic photos, audio, video and other fakes generated using artificial intelligence technology "and was first used in 2017. Mostly deep fakes are created through the use of machine learning techniques, in particular generative opposing networks. In the process of competition between two different machine learning systems, one of them (generator) creates a kind of output data (audio recordings, photos, video material), and the other (discriminator) learns to identify the false effects of the generator's work. "Competition" lasts as long as the generator perfects its work to the point where the discriminator is unable to distinguish between false and true content" (Olech, Lis, 2021, p. 97.).

By way of example, mention should be made of a fake recording in which the President of Ukraine, V. Zelensky, urges his countrymen to surrender to the Russian invaders. (Deepfake video of Volodymyr Zelensky surrendering surfaces on social media – YouTube). Deep fake is therefore a prospective tool for conducting psychological operations, the effectiveness of which largely depends on AI.

AI is therefore an effective weapon in the field of fake news or deep fake, it can be used to create and disseminate compromising scene leaders, false messages, orders, calls to surrender, causing disinformation of the opponent and decaying his morale, which may determine the outcome of the fight.

Artificial Intelligence is also used in cryptography, as exemplified by learning cipher neural networks or networks supporting intrusion detection systems. Therefore, the thesis of P. Kotlarz and Z. Kotulski should be shared, that "The solution currently used in practice is the use of neural networks to support intrusion detection systems. IDS systems (Intrusion the Detection System essentially works by gathering so-called user profiles on the network. They characterize typical behaviors for a given user. If suddenly the nature of the traffic generated by a given user differs from the created profile, it is an alarm signal for the IDS system" (Kotlarz, Kotulski, 2005, pp. 186 and 187).

Another application of AI is its use in radio-electronic warfare. "Such solutions were noticed during the Russian involvement in Syria and Ukraine, where several" Murmansk-BN "radio-electronic warfare units were deployed. Their goal was, among others gathering information on electronic signals from Western military equipment within a radius of up to 5,000 km. Then the collected data was processed by advanced learning algorithms, which allowed for the marking of Western military equipment with appropriate signatures, in order to ultimately improve Russian defense capabilities". (Kumalski, 2020, p. 80).

The use of AI also includes, for example, supporting the pilot in difficult weather conditions, optimizing supply chains and improving logistics efficiency, recognizing sonar signals, conducting a number of various training courses using trainers and simulators, or steering a drone or a swarm of drones. Regarding the latter form of using AI, it is worth noting that we are already dealing with a confirmed combat use of a drone that attacked a person on its own, possibly leading to his death. According to the UN report S / 2021/229 in Libya, the Turkish Kargu-2 drone was used in the clashes between the GNA and HAF forces, which attacked the retreating enemy forces, doing it independently through the use of deadly, autonomous weapon systems. (N2103772.pdf (un.org), p. 17).

When concluding the considerations on the use of AI in the sphere of security, it is worth mentioning the Chinese social credit system, which is in essence a system of social control. As M. Bieroński points out, "Its idea is to evaluate people in terms of compliance with social norms and rights". (Bieroński, 2020, p. 11.). These standards are set de facto by the Communist Party of China, headed by its Secretary General and the President of the People's Republic of China, Xi Jinping. Their observance and evaluation of the behavior of the citizens of the Middle Kingdom are supervised by, among others, AI. This state is very similar to the Orwellian utopia described in the novels *1984* or *Animal Farm.* As you can see, what was not so long ago the sphere of SF, is slowly becoming reality – not necessarily positive and optimistic.

Conclusions

The development of AI in the field of security is inevitable.

There is a danger of the uncontrolled development of AI and its alienation.

AI will be transferred into space, enabling man to exploit it economically.

It is necessary to take steps to enact legal regulations, including international ones, which will cover the methods and scope of AI use in the sphere of both military and non-military security.

References

Bartosiak J., Friedman G., Wojna w kosmosie. Przewrót w geopolityce, Warszawa, 2021.

Bieroński M., Etyczne i moralne wyzwania związane ze stosowaniem Sztucznej Inteligencji, "Kieleckie Studia Teologiczne" 2020 nr 19.

Deepfake video of Volodymyr Zelensky surrendering surfaces on social media – YouTube. Available from : https://www.youtube.com/watch?v=X17yrEV5sl4

Ethics guidelines for trustworthy AI | Shaping Europe's digital future. Available from : https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Fehler W., Araucz-Boruc A., Dana A., Lasota-Kapczuk A., Systemy sztucznej inteligencji jako wyzwanie dla sfery bezpieczeństwa i obronności RP, "Zeszyty Prawnicze BAS" 2021, №2(70).