UDC 327.56::351.88(497.11)
DOI:10.5937/nint48-49980
Original Scientific paper

НАЦИОНАЛНИ ИНТЕРЕС
NATIONAL INTEREST
Година XX, vol. 48
Број 2/2024
стр. 53-75

Aleksandar Pavić*
University of Defense Belgrade, National Defense School

Hatidža Beriša**
University of Defense Belgrade, Military Academy

ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY STRATEGY DEVELOPMENT – CHALLENGES AND PERSPECTIVES

Abstract

As a rule, the directions of development of the national security strategy are always aligned with vital national interests and modern achievements of society, which are imbued with modern challenges, risks and threats and available instruments of power. Monitoring global trends and the use of an adequate methodological approach enables the strategy to reflect a clear definition of national interests, ways of achieving them and the state's ability to achieve those interests using instruments of national power. Artificial intelligence through various forms of manifestation will significantly influence the development of future society. The implementation methodology will depend primarily on the needs and capabilities of the state. The goal of this work is to bring artificial intelligence closer to the professional public and to somehow place it in the focus of future considerations in the field of security and defense. Technology, which every day is becoming more and more present in all spheres of life, must find its role and place in strategic and doctrinal documents related to the defense of the state. Artificial intelligence must be integrated and operationalized as one of the starting points for creating a modern national security strategy, which is also the thesis of this expert work. The thesis clearly implies that the future national security strategy cannot be conceived without the concept

* aleksandar.pavic@mod.gov.rs; ORCID: https://orcid.org/0009-0005-6737-0094.
** hatidza.berisa@mod.gov.rs; ORCID: https://orcid.org/0000-0002-9432-5273.

of using artificial intelligence. The theoretical foundation of artificial intelligence is imbued in various scientific fields that primarily deal with automation and autonomous use of systems. Practical application found its basis in the gradual but comprehensive digitization of all spheres of life and society as a whole. From the point of view of national security, it is especially important to consider the impact in the development of autonomous weapon systems, the perspective of their use and the way they will shape modern armed conflicts.

Keywords: artificial intelligence, national security strategy, autonomous armed systems.

INTRODUCTION

When we talk about the concept of intelligence, it is mostly related to the mental ability of a person. Attributing such an ability to an object or subject that is not the embodiment of a human brings us into the domain of artificial intelligence. The earliest known writings about non-human intelligence appear in the Greek myths of Hephaestus[1] and Daedalus[2] which included the idea of "intelligent robots" and artificial beings like Pandora[3]. These "automatic" beings such as Talos[4] had the role of protecting Crete from invaders. The ancient Greeks also talked about the idea of "biotechnics", and how biological phenomena such as ageing can be changed with human technology. However, the first real concept of AI was formulated by the German philosopher and mathematician Gottfried Wilhelm Leibniz[5]. According to his theory it was possible for a machine to automatically generate ideas. He said that, human thoughts, in any form, can be measured and can be reduced to a

1 Hephaestus – god of fire and blacksmithing, one of the sons of Zeus and Hera in Greek mythology.

2 Daedalus (Greek: Δαίδαλος, Latin: Daedalus) is the greatest Greek sculptor, painter, builder and inventor in Greek mythology.

3 Pandora (Greek: Πανδώρα, Latin: Pandora) in Greek mythology is the wife of the titan Epimetheus. Pandora is a woman who brought evil and suffering into the world.

4 Tal or Talos (Greek: Τάλως) was a bronze man in Greek mythology, the guardian of Crete.

5 Gottfried Wilhelm Freiherr (Baron) von Leibniz, (German: Gottfried Wilhelm Freiherr (Baron) von Leibniz; Leipzig, July 1, 1646 – Hanover, November 14, 1716) was a German polymath.

refined combination of fundamental concepts. Because of this, Leibniz assumed that this combination could be repeated to enable a machine to do the same thing as a human. Leibniz called this theoretical mechanism "a great instrument of reason", which, in his opinion, could answer all the questions put to it. However, the idea of a thinking machine has come under fire. Many believed that human thought was an inimitable form of expression, not something reducible to scientific principles, a view still held by some today. That "great instrument of reason" was never successfully created, and we have yet to see a machine that could answer any question (Milosavljević 2015).

The paper is divided into six units, in which the possibilities and potentials of artificial intelligence as an element of national security are analyzed, with reference to the challenges and perspectives of the use of autonomous armed systems. In the first part, the concept and definition of artificial intelligence is pointed out. The second part analyzes the challenges of using autonomous weapons systems. In the third part, some commonly known facts related to the concept of AI and the perspectives of further application are discussed. The fourth unit presents the normative legal basis and readiness of the system for the application of artificial intelligence in the Republic of Serbia and the areas in which potential projects could be developed. The directions and experiences in the implementation of the Artificial Intelligence Strategy in defense are shown in the example of United Kingdom of Great Britain and Northern Ireland in the fifth unit. Finally, in the last unit, some of the concepts of autonomous weapon systems are discussed through examples and planning for further development.

TERM AND DEFINITION

The term AI appeared for the first time in 1956. in the United States of America in the city of Dartmouth, at a gathering of researchers interested in the topics of intelligence, neural networks and automata theory (Solomonoff 1956). The meeting brought together the most eminent experts in the field of automation and computing, as well as the mathematical elite of that time, where the foundations of the concept were created and the path for further development of AI was laid out. Alan Turing[6] had previously published an article in 1950 entitled "Computers

[6] Alan Mathison Turing (London, June 23, 1912 – Cheshire, June 7, 1954) was an English mathematician, logician and cryptographer.

and Intelligence", in which he talks about the concept of AI and lays the foundations of a type of test, through which it would be determined whether a certain computer system behaves in accordance with what is meant by AI, or not. Later, this type of test will be called the Turing test. The aforementioned facts tell us that thinking about giving non-human entities human intelligent features has existed since the beginning of the first developed human thoughts and continues to this day (Turing 1950).

The search for a definition of AI is a complex problem, so according to (Russell and Norvig 2010) there is no generally accepted definition. The constant expansion of possibilities and the sphere of use contribute to the fact that the definition is constantly refined and adapted to new and changed circumstances. What is acceptable from the point of view of the Republic of Serbia is the definition from the "Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020 – 2025". Within the mentioned strategy, the widely accepted definition of the European Commission is used, with the view that: "Artificial intelligence refers to systems that show reasonable, intelligent behavior based on the analysis of their environment and make decisions – with a certain degree of autonomy – to achieve specific goals. Systems based on artificial intelligence can be based exclusively on software and operate in the virtual world (for example, virtual assistants, photo analysis software, Internet browsers, speech and face recognition systems) or they can be embedded in devices – hardware (for example, advanced robots, autonomous vehicles, drones and the like)." (Government of the Republic of Serbia, 96/2019-5).

THE CHALLENGE OF AUTONOMOUS ARMAMENT

The issue of autonomous weapons is a classic example of the discrepancy between modern technological progress and the moral principles the modern world rests on. A large number of authors deal with attempts at legalization, moral acceptability and analysis of the place and role of AI in contemporary society. If we add to this fact the use within the operations of military structures, then it acquires a new dimension because it is directly related to national security. And when there is a threat to the security and survival of the nation, then all other aspects are minimized because survival has no price and it is a natural characteristic of every living being, including man, to fight for the same. Defining an autonomous weapon system (AWS) is as difficult as defining

an AI, especially due to ethical, political and strategic sensitivities. Taddeo and Blanchard gave one of the acceptable and declaratively neutral definitions. They defined AWS as an artificial agent that is able to change its own internal properties in order to achieve a goal or a set of goals, within the dynamics of its operational environment and without direct interventions of another agent (Taddeo and Blanchard 2022). It may be capable of changing its own transition rules without the intervention of another agent for exerting kinetic force against a physical entity (either an object or a human). In order to identify, select and attack a target without the intervention of another entity. When implemented, AWS can be used with or without human control, with a human in the loop or out of the decision loop. Autonomous weapon systems that are lethal deserve special attention. The debate on AWS is shaped by strategic, political and ethical considerations. Different interests and values contribute to the polarization of the debate, while politically charged definitions of AWS undermine efforts to identify legitimate uses and to define relevant regulations (Sheikh, Prins and Schrijvers 2023; Scharre 2019).

Regardless of the different views, the Ministry of Defense of the United Kingdom of Great Britain and Northern Ireland defined in its AI Defense Strategy that the ultimate goal of the use is profiling in a "scientific and technological superpower" by 2030 (UK MoD). The importance and actuality of the topic in terms of security in itself dictates that it must be considered in the broadest view from the point of view of the challenges faced by human society. The risks and threats arising from the use of AI are more and more present every day, both in the form of new combat autonomous platforms and in cyberspace.

In order to answer the question of the challenge of using AI, it is first necessary to define who manages the system and to delimit the concepts of automated and autonomous systems in the defense and security system. Conceptually, management is often equated with control. However, the environment in which security and defense are considered certainly rests on governance. Cybernetics is a science that deals with the study of system management, and as such essentially defines that management is reflected in the translation from one state to another state of the system, so that in each subsequent phase, greater efficiency of the system's functioning is ensured (Čubura 1977; Wiener 1965). The study of information connection theory, the development of communication models, the study of feedback loops and control mechanisms of information transmission, and the management of cybernetics as a scientific discipline gave rise to informatics and artificial intelligence.

Learning and decision making in artificially intelligent autonomous control systems is an essential question that needs to be answered. Neural networks and machine learning are part of the framework in which we can find the answer to how AI learns. The ability to learn and upgrade knowledge is the basis of intelligent systems. However, the answer to the question of how AI manages, thinks and makes decisions is much more complex. The feedback mechanism and the OODA loop could play a significant role in the way the autonomous system works. The feedback mechanism, within the defined parameters, performs the assigned action with constant correction in order to make the output result as high quality as possible. On the other hand, John Boyd[7], which is the creator of the OODA loop[8], perhaps best describes the management and decision-making process in such advanced systems. As (Osinga 2006) and (Hammond 2001) in their deliberations state that this is his greatest achievement, which has a wide application in the decision-making process and timely action in various fields, among other things in the security system. The OODA loop consists of a decision-making circle whose elements are observation, orientation, deciding and action. The cycle defined in this way is the basis of the functioning of autonomous armed systems based on artificial intelligence (Čolić 2022).

The interaction of cognitive, geopolitical and organizational factors dictates that the line between machines that analyze, generate information, predict future events and inform decision makers. To clearly define the continuum and separate the decision-making process between humans and machines will greatly contribute to the automation of the OODA loop.

By analyzing the challenges of using the AI, you should definitely clearly define the difference between a directed, automated and autonomous process. The relationship between the three different processes is, in practice, the boundary that defines a system that is declared intelligent versus one that is not. Autonomy is the highest level that can be related to the operation of a single system, machine-robot. Autonomy gives the intelligent system the distinction of making a decision on its own based on the available data and the situation it is located.

---

7 John Richard Boyd (January 23, 1927 – March 9, 1997) was a United States Air Force fighter pilot and Pentagon consultant during the second half of the 20th century. His theories were very influential in military, business and judicial strategies and planning.

8 OODA – Observe-Orient-Decide-Act.

The modern concept of living, which is constantly based on technological accessories, without which comfort would be significantly reduced and redacted, unequivocally states that it is necessary that further considerations be directed to the important aspects of the application of AI and they be seen, described and discussed. First of all, in order to get closer to the common man who expects modern technology to be a loyal service and enable the optimization of life and work. Certainly, it is necessary that any technology that can potentially equal the power of man in the process of making a distinction or in the distant future be in supremacy over the same be thoroughly considered and socially accepted within the framework that does not infringe on universal human rights. Wide acceptability of the AI is a necessary condition for its application and implementation in the national security strategy. It is also a big challenge for future decision-makers who will have to define a place in the role of AI in the normative legal security system of the state between ethics and necessity.

AI FACTS AND APPLICATION PERSPECTIVES

Ancient philosopher Parmenides[9] emphasized in his speech "being is, non-being is not". From a philosophical point of view, the interaction of man as a being and a machine that possesses all the elements of advanced artificial intelligence always places the human being as superior both by nature and by right. The views and facts related to AI cannot be considered only from the point of view of the scientific aspect, but also from the point of view of the common person who needs to accept and exploit the products of the new technological era.

The starting point is that AI is all around us even though we do not see robots or different machines materialized in our environment as much as we might want. It is necessary to start with the device that everyone owns, which is the smartphone. It is the point at which almost every person has a direct connection with AI, even though they may not think about it. Namely, the various virtual assistants that are used via mobile smart devices are actually representations of AI in its basic fundamental form. Voice assistants, i.e. applications, such as Google Assistant, Siri, Cortana or Alexa are some of the examples that can be

[9] Parmenides of Elea (Greek: Παρμενίδης ὁ Ἐλεάτης, born around 515 AD, died around 450 AD) was a Greek philosopher, born in Elea, a Greek city on the southern coast of Italy.

found in public sources, which probably most people have used and seen the possibility of their practical application. Another accessible area is industry, or engineering, where one can directly see a robot materialized and functional within limited and strictly controlled conditions. Since 2011, there has been a terminological definition of "Industry 4.0", which is the natural successor of the previous industrial revolutions. About "Industry 4.0" various authors said that it is the future of global production that unites existing ideas and new values in a chain that plays a key role in transforming the entire value of the life cycle of goods in one innovative form, resulting in greater productivity and flexibility of engineering integration (Tay et al. 2018).

Another interesting fact is that AI already talks a lot with us. In the basic human sense, it is perhaps the most important element of interaction between man as a conscious being, "homo sapiens[10]"and a machine that is intelligent. The level at which a conversation can be held with a machine is something that can bring a man and a machine closer together, because by nature man has to communicate, and it is certainly easiest when he does it directly. As one of the examples of what was written above, we can take the system "ChatGPT", presented in November 2022 by the company "OpenAI". The system is only one of several offered, but it actually communicates with humans and constantly improves its behavior and learns along with us and from us.

The third important fact is that people are afraid of AI. The fear of integrity being taken over by machines is certainly rational. Also this can be seen as fear of the unknown and uncertainty brought by some new intention, which can threaten some of the basic human rights. Although we talk a lot about AI, it is still a very inaccessible area for the ordinary, that is, the average person, which is what various authors talk about and talk about in their works (Russell and Norvig 2010; Scharre 2019; Taddeo and Blanchard 2022).

The last, but not the last, fact that should be taken into account is that AI is not perfect, that is, it is currently far from perfect. But if we take into account the evolution of man, it may not be appropriate to compare it with machine or virtual systems, but we can certainly draw a parallel between the development and evolution of man from the beginning to the present day. If we take into account that the term AI

[10] Man or homo sapiens (lat. Homo sapiens – "wise man", primarily a subspecies of Homo sapiens sapiens), a living being that has a highly developed brain capable of thinking, speaking, solving problems, self-observation, etc.

was defined in 1956, it can be concluded that it is very young, but also that it is developing faster than the thoughts of man himself. Imperfection can especially manifest negative aspects in autonomous weapon systems, where the human is on the other side of the machine as the target, but behind the machine as the governing body.

The areas in which AI is applied cannot be rounded off, because the dynamics of development and interaction with different areas is expanding every day. However, the areas of defense and security are certainly among the most innovative and, as a rule, are always the initiator of new technologies that are later used in various spheres of life. It is important to list the areas of security and defense where implementation will be significant, especially in times to come. Analyzing a large number of authors and publicly available literature, several areas and projects can be singled out that will shape the future of the use of AI in the security and defense segment, namely: autonomous armed systems, systems for strategic data processing, analysis and decision-making, battlefield simulations and training, recognition threats, drone swarms and cyber security.

Why it is important and necessary to consider the use of AI in the security and defense system can best be considered through the development of war as the basis of an armed conflict between two or more opposing parties. The national security strategy considers how national interests can be realized or preserved if they are threatened, as well as the means necessary to achieve this. AI and its rapid development are certainly one of the mechanisms that in the future will significantly influence instruments and mechanisms that will show the technological-technical component of the development of a country and certainly use it as an element of deterrence or an element of active action in the realization of national interests together with other factors.

LEGAL FOUNDATION AND POSSIBILITIES OF IMPLEMENTATION

Military neutrality, which was proclaimed in 2007 by the adoption of the Resolution of the National Assembly of the Republic of Serbia, expressed the determination that the state independently creates its defense policy (Government of the Republic of Serbia, 125/2007-3). A strategic concept based on the total defense model was accepted, as a comprehensive response of the defense system to registered challenges, risks and

security threats significant for the defense of the state (Government of the Republic of Serbia, 94/2019-4). The model should be realized relying on its own strengths and potentials, which further implies the necessity of active monitoring and adoption of the most modern technologies. Any prolongation of this activity significantly affects the operational capabilities of the defense system in all aspects. Delaying modern security concepts exponentially distances us from the possibility of defending the concept of military neutrality in the future.

The Government of the Republic of Serbia has recognized the importance of the development of AI and the legal regulatory definition of the framework for its use. The document in which the Government clearly defined the further development of AI is the Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025. In the previous decade, considerable funds were invested in digitalization and infrastructure development for the implementation of modern information technologies, and among other things, the preparation of conditions for the development and implementation of AI. Office for Information Technology and EGovernment is next to more of the ministries responsible for the implementation of the activities as mentioned earlier. The construction of the State Center in Kragujevac confirmed the Government's determination to invest in and develop the information technology sector. The key areas that are recognized as the bearer of AI development in the strategy are education and science, the economy and the public sector. The prerequisites considered as necessary relate to regulation, open data and infrastructure. However, in contrast to a large number of countries that adopted their strategies for the use of AI in the security system, the Republic of Serbia has not mentioned such a thing anywhere for now. It is best to look at the use of AI in the national security sector through examples and ways that have already been implemented by certain relevant countries and through an attempt to adapt it to the possibilities and needs of the Republic of Serbia (Government of the Republic of Serbia, 96/2019-5).

The use of AI in the national security system of the Republic of Serbia has enormous potential and as it has already found its application in various aspects of other countries. In particular, we point out the possible application of AI in the framework of national security, which would refer to challenges, risks and threats to security:

1. *Threat Alerting*: The AI will be used to analyze large amounts of information from various sources, including social media, the Internet, satellite imagery and communications, to identify potential threats to national security. It can also notify responsible organizations and individuals about security-related situations.
2. *Border control*: AI has capabilities to participate in monitoring and controlling borders and territorial areas using surveillance systems, unmanned aerial platforms and image processing systems, as well as detection of illegal activities, trafficking and migration.
3. *Cyber security*: Analysis of cyber-attacks, prevention and early detection of hacker attacks and responses to them in real-time, as well as identification of the source of cyber-attacks and prevention of future attacks.
4. *The fight against terrorism and organized crime*: Through the analysis of mass communications and the monitoring of activities in cyberspace of potential persons who are designated as members of terrorist and criminal groups.
5. *Public safety*: Multisensory platforms for monitoring and surveillance of public spaces based on algorithms that recognize faces and vehicle registration marks, monitor activities in certain perimeters and analyze the movements and emotions of people, can significantly prevent the emergence of security threats to people and infrastructure.
6. *Information analysis and decision-making*: Analyzing intelligence data and proposing strategies and decisions for responsible organizations in the decision-making system is one of the key purposes of AI.
7. *Training and simulation*: AI can be used for training security personnel and simulations in preparation for responding to crisis situations.
8. *Development of modern combat platforms*: The use of AI algorithms and concepts within combat systems can be implemented through both application platforms, as a hardware and as a software solution.

Challenges, risks and threats lead to the fact that AI can find its use in the national security system through various sectors of application. Potentially become the engine of development of a part of the system and equipment that is used above all in the dedicated industry and the modern concept of the use of institutions that are factors security, i.e. primarily the Serbian Armed Forces.

However, as in many other areas, the use of AI in the national security system raises privacy and ethical challenges. It is important to develop strict protocols and regulations for the use of this technology in order to limit misuse and protect the privacy of citizens. It is necessary to implement AI in systems both at the hardware level and at the software level that are used in the defense of national interests in case national security is threatened.

EXPERIENCES OF GREAT BRITAIN

Great Britain published Owen AI defense strategy on June 15, 2022. Analyzing the concept, methodology and intended end state, we can see through which stages the strategy has passed and how a serious country considers such an important resource. The strategy was created as a natural need to modernize the armed forces and improve the entire security and defense sector. Competitiveness on a global level, which is a constant in relation to the great powers. In the context of security challenges, risks and threats, defense must be a priority for research, development and experimentation, in order to maintain a strategic advantage by using innovative concepts and cutting-edge technologies, and this certainly includes AI. The advantage is considered not only in the sense of supremacy over others but also in the area of deterrence against threats resulting from the possession of AI by the enemy. One of the basic postulates of improving the national security strategy is the determination to strengthen it through science and technology (UK MoD).

Defining the term AI in the defense domain, this Strategy sees it as a family of general-purpose technologies, each of which can enable machines to perform tasks that typically require human or biological intelligence. When defining the term, it is necessary to take into account two terms that are indivisible factor AI, namely machine learning and data management. Machine learning is the instrument of AI, and data management is a necessary condition machine learning is based on. In this way, from complete control, through automated operation of the system, to a fully autonomous system that independently makes decisions.

The strategy is defined through four basic goals:

1. Transform the defense sector into an organization ready to accept AI: The goal will be realized through engaging and animating the professional public and the able-bodied part of the population, recruiting key talents; analyzing political challenges; continuing with the modernization of the digital agenda, and improving the knowledge and technologies that make it possible.
2. Adopt and leverage AI at a speed and scale that delivers advantage: The formulation of organizations that will enable the realization of the goal, in order to take advantage of the short-term and long-term opportunities of all subjects. First of all, through international cooperation and systematic experimentation.
3. Strengthen the defense and security AI ecosystem in the UK: Realization of the goal primarily through building trust and as well as clarifying requirements, and commercial barriers, encouraging joint engagement and supporting business growth.
4. Shape the global development of AI to promote security, stability and democratic values: Influence through various aspects to present the state as responsible for the global development of artificial intelligence, to promote security and stability, and finally to actively participate in the development of future security policy.

Realization of the set goals should provide the defense system with an advantage in decision-making, efficiency, new capabilities, and improvement of the entire system. Centralized management of this project was not accepted as a solution, but was made available to a wide range of state security factor. The Ministry of Defense is a factor that should define policy and strategy through goals, directing strategic programs and ensuring general coherence. Other functional units through the management of the assigned project segments should follow the instructions and elaborate on them. In the end, the command of the armed forces at the strategic level should ensure strategic and operational integration in the domain of armed struggle.

The ultimate goal of the Strategy is for Great Britain to become a "scientific and technological superpower" by 2030. The National Strategy AI should have a role to fully transform and improve the entire industry.

The integrated operational concept they are considering in the UK describes how quality information and rapid technological change are transforming the very nature of warfare. New technologies are generating large amounts of data, formulating new threats and vulnerabilities, and expanding the scale of potential attacks through advanced next-generation capabilities (such as drones, high-velocity weapons, and advanced cyber-attacks). All this will significantly affect the decision-making time in the sense that a person will not be able to analyze all the available data on his own, but will have to consult a machine. Future conflicts will be shifted to the domain of information operations that will be shaped by AI. A radical change in the concept of defense has been in transition for a long time and the strategic competition related to AI is intensifying, so the response to these challenges must be fast, ambitious and comprehensive (UK MoD).

A STEP TOWARDS AUTONOMOUS WEAPON SYSTEMS

Artificial intelligence has taken its developmental path from symbolic influence to connectionism[11]. As stated in (Sheikh, Prins and Schrijvers 2023) the development of AI during the 50s of the 20th century was symbolic in the theoretical and conceptual sense, however, during the 80s there was a significant development of expert systems, so today the prevailing trend of machine learning. The potential of developing unconventional technologies according to (Scharre 2019) with primary use in the national security system was recognized by the United States of America and in response to Sputnik[12]. President Dwight Eisenhower[13] ordered the formation of two agencies of national importance. The first was NASA[14] which had a mission to win the space race. However, the

[11] In recent years, revolutionary changes have taken place in the field of learning and memory, which express great enthusiasm but also controversy. They reflect the development of ideas based on the assumption of parallel processing of information distributed over many units, which is known as parallel distributed processing or connectionism.

[12] Sputnik 1 was the first artificial satellite launched into orbit on October 4, 1957, in honor of the anniversary of the October Revolution.

[13] Dwight David "Ike" Eisenhower (Denison, October 14, 1890 – Washington, DC, March 28, 1969) was an American military leader and politician, best known for the successful command of the Allied forces in Western Europe during World War II war, as well as by serving as 34th president of the USA.

[14] National Aeronautics and Space Administration (NASA).

other one is called DARPA[15] or "The Department of Mad Scientists" as Michael Belfiore called it[16] had the function of developing advanced defensive weapons. It was this department that developed the computer network called ARPANET, which is known today as the INTERNET. This publicly available resource will be one of the most important tools of AI both for collecting data and for directly manifesting activities.

Why is it important to distinguish between automated and autonomous control systems in developing a national security strategy? Previously, we made a conceptual distinction between these two terms. However, the use of such systems in security and defense systems, and especially in the military, can sometimes be misunderstood. Broad consideration of autonomy and misunderstanding of the essence leads to the interpretation that alone, automation of a process is identified with autonomy. The armed forces of the SFRY[17] also dealt with this problem, during the 70s of the last century, the theoretical positions of cybernetics were accepted as a science that deals with the management of various systems and processes. So, for the first time, some self-correcting processes were mentioned. The principle of feedback was the basis of the system in order to make the end result as accurate as possible. On the principles of that JNA[18] process in that period started planning the concept of the automation system in airspace control management. A series of proposals were developed, culminating in the final project that began work in 1984 under the name "Automated Systems Marconi" (Branković 2021). The system was able to independently manage the available defense systems based on the entered data and make a recommendation on the use of resources to neutralize the threat, but not to independently respond to the threat. In that period, one of the most complex systems not only in the country but also globally gave guidelines for further development and it is safe to say that he was a pioneer in the development of what is now called an autonomous system.

---

15 DARPA (Defense Advanced Research Projects Agency) is an agency of the US Department of Defense responsible for the development of new technologies for the military of the United States of America (USA).

16 Michael Belfiore is a writer and journalist. Some of his notable works include "Department of Mad Scientists: How DARPA is Remaking Our World," published by Smithsonian Books.

17 SFRY – Socialistic Federal Republic of Yugoslavia

18 JNA – Yugoslav People's Army.

USSR[19] in the same period as the aforementioned SFRY, in accordance with its deterrence strategy, developed a system for automatic warning of intercontinental ballistic missiles, i.e. the "Eye" project. The system had the task of using satellite technology to detect the threat in a timely manner, to look at possible aspects of defense and to alert the headquarters, which should respond adequately (Podvig 2002). This system is important because it just shows that a machine cannot consider all the influencing factors, reason like a human and make an expedient decision based on a limited number of resources. Namely, on September 26, 1983, the system was a false danger that was reflected in the detection of the takeoff of two rockets from the USA towards the territory of the USSR. If there was no man in the command system at that time, the machine would have responded to the threat in accordance with procedures and reacted with available countermeasures. However, a man was in the chain of decision-making. Today it can be analyzed and studied what level of autonomy can be granted to you in the decision-making process (Scharre 2019).

Technological innovation is unstoppable and the defense industry has concentrated its efforts on solving the individual requirements of the defense system (Taddeo and Blanchard 2022). The military industry has always been a generator, implementer and distributor of cutting-edge technologies. The US Air Force in 2009 adopted the "Unmanned aerial vehicle system development plan for the period 2009-2047", however, that plan did not explicitly state that the research would focus on the autonomy of unmanned aerial vehicles. A couple of years later, in 2014. USA introduced so-called "Third equalization strategy[20]" in order to revive military-technological supremacy on a global level. The central part of this strategy is dedicated to robotics, autonomy and the association of man and machine (Hillner 2019; Dombrowski 2015). Both of the aforementioned plans focus on aircraft as a central part of development, however, it is notable that in 2014 they recognized the necessity of autonomy and artificial intelligence as an indivisible part of new weapon systems. In addition to the well-known unmanned aerial vehicles of strategic importance "MQ-9 Reaper" and "RQ-4 Global Hawk", which justified and proved their importance and role in a large number of activities of the US armed forces around the world. Her primacy in terms of autonomy still belongs to the first fully autonomous aircraft

[19] USSR – Union of Soviet Socialist Republics

[20] The Third U.S. Offset Strategy.

"X-47B[21]". In 2013, this aircraft made a fully autonomous flight and landed on an aircraft carrier. The only command she gave the man was to land, everything else she did completely independently. Two years later, the same aircraft performed the first autonomous refueling of another aircraft completely independently. This set the limit points for the development of autonomous armed systems, i.e. that they can perform an activity from point A to B without human corrections without a special command (Nowak 2016). Similar projects are being developed by other superpowers such as the Russian Federation and the People's Republic of China. Constant competition on a global level makes the development of these systems even more dynamic and advanced.

The autonomous armed system that has already been proven in use by several armies of the world is "IAI Harpy[22]" is a fully automated hovering missile developed by the Israeli Aerospace Industry and has been in use for almost 25 years. Combining the capabilities of an unmanned aerial vehicle and a missile, the "Harpy" searches, identifies, acquires, engages and destroys enemy radar targets in a fully autonomous operation. It is interesting to note that if after selecting a target for any reason the target stops emitting radiation, "Harpy" stops the attack and starts searching for a new target.

The analysis of data from public sources on which this paper is based also supports the fact that there are certainly more modern and advanced autonomous armed systems that will certainly shape the future space of modern operations. The above-mentioned examples of specific projects and plans that plan the development of autonomous systems, as well as various other areas of application, speak in favor of the fact that the perspective is completely justified and certain.

---

21 The X-47B is a tailless, strike fighter-sized unmanned aircraft developed by Northrop Grumman as part of the U.S. Navy's Unmanned Combat Air System (UCAS) Carrier Demonstration program.

22 HARPY is an all-weather day/night "Fire and Forget" autonomous weapon, launched from a ground vehicle behind the battle zone. Programmed before launch to perform autonomous flight to a pre-defined "Loitering Area", in which they loiter and search for radiating targets.

CONCLUSION

Artificial intelligence is a postulate that is the reality of our present and an indivisible component of the future concept of living. From all that has been stated, it can be concluded that the reality in which we live cannot be imagined without the technological achievements that are found in our environment and which have become everyday use. Defense based on the concept of total defense requires us to actively follow modern trends, propose new projects and finally develop autonomous weapon systems. Through the pursuit of process automation and autonomy, we have contributed to the fact that currently we simply want the machine-device-robot to be independent in a certain sphere of work it performs. National security and the environment in which it is defined is always based, as a rule, on the most modern technological achievements and it forces us to develop new concepts and solutions in order to bring supremacy to the big powers at the global level, and to other small actors to preserve the ecosystem such as military neutrality. It is certain that the Republic of Serbia cannot independently develop technologies AI. The potential of the defense industry certainly has the basis for the initial stages of projects for the development of autonomous armed systems for tactical purposes, but it certainly can and should consider foreign solutions that have been offered and actively participate in international projects. Great Britain itself, as a power and a champion in many aspects, insists on international cooperation and the creation of common conceptual solutions that it will later independently adapt to its needs. It is also necessary for Serbia in the near future to define goals, and means and formulate tasks for all factors of security and defense in order to start implementing this probably less important technology of the 21st century. In addition to the above, it is necessary to actively promote the social acceptance of this modern technology, with adequate legitimate values and a legal basis. It is necessary for the state to think strategically about the realization of national interests and to use all available opportunities, actively monitor the development of its instruments of power and correlate the strategy in accordance with modern concepts and thinking. Concrete measures can be implemented through development plans, investments in scientific research and concrete projects.

REFERENCES

Branković, Živojin. 2021. „[PARTNER 2021] VOJIN odnedavno sa najmodernijom opremom: Kako je domaćim snagama razvijen Sistem automatizacije centra Vazdušnog osmatranja, javljanja i navođenja – SA cVOJIN.“ TangoSix. https://tangosix.rs/2021/24/11/partner-2021-vojin-od-nedavno-sa-najmodernijom-opremom-kako-je-domacim-snagama-razvijen-sistem-automatizacije-centra-vazdusnog-osmatranja-javljanja-i-navodjenja-sa-cvojin/.

Čolić, Miro. 2022. „Komparativna analiza koncepta situacione svjesnosti i OODA pretlje“. *Strategos,* vol. 6, br. 2: 145-175. doi: https://hrcak.srce.hr/287952.

Čubura, Nikola. 1977. *Kibernetika u rukovođenju razvojem oružanih snaga*. Beograd: Vojnoizdavački zavod.

Milosavljević, Milan. 2015. *Veštačka inteligencija*. Beograd: Univerzitet Singidunum.

Dombrowski, Peter. 2015. “America’s Third Offset Strategy: New Military Technologies and Implications for the Asia Pacific. *S. Rajaratnam School of International Studies*. https://www.files.ethz.ch/isn/191706/PR150608Americas-Third-Offset-Strategy.pdf.

Government of the Republic of Serbia, Defense strategy of the Republic of Serbia 94/2019-4, December 27, 2019, https://www.mod.gov.rs/multimedia/file/staticki_sadrzaj/dokumenta/strategije/2021/Prilog4-StrategijaOdbraneRS-ENG.pdf, last accessed 14 October 2023.

Government of the Republic of Serbia, Resolution of the National Assembly on the protection of sovereignty, territorial integrity and constitutional order of the Republic of Serbia 125/2007-3, December 26, 2007, https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/rezolucija/2007/125/1/reg, last accessed 14 October 2023.

Government of the Republic of Serbia, Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025 96/2019-5, December 31, 2019, https://www.srbija.gov.rs/extfile/sr/437310/strategy_artificial_intelligence-condensed261219_2.docx, last accessed 17 October 2023.

Hammond, Grant T. 2001. *The Mind of War, John Boyd and American Security.* Washington DC: Smithsonian Books.

Hillner, Eric P. 2019. "The Third Offset Strategy and the Army modernization priorities". *Center for Army Lessons Learned*. https://usacac.army.mil/sites/default/files/publications/17855.pdf.

Nowak, Edvard J. 2017. „The Aircraft Carrier's Relevancy in Future Conflicts." Master's Thesis. Marine Corps University Quantico: United States Marine Corps, Command and Staff College.

Osinga, Frans P.B. 2006. *Science, Strategy and War: The Strategic Theory of John Boyd.* Amsterdam: Routledge.

Podvig, Pavel. 2002. "History and the Current Status of the Russian Early-Warning System". *Science and Global Security*, 10(1): 21-60.

Russell, Stuart, and Peter Norvig. 2010. *Artificial Intelligence: A Modern Approach, Third Edition*. London: Pearson Education.

Scharre, Paul. 2019. *Army of None: Autonomous Weapons and the Future of War.*, New York: W. W. Norton & Company.

Sheikh, Haroon, Corien Prins and Erik Schrijvers. 2023. "AI as a System Technology." In Mission AI. Cham: Research for Policy. Springer. https://doi.org/10.1007/978-3-031-21448-6_4.

Solomonoff, Raymond J. 1956. "An Inductive Inference Machine". *IRE Convention Record, Section on Information Theory.* 56–62.

Taddeo, Mariarosaria and Alexander Blanchard. 2022. "A Comparative Analysis of the Definitions of Autonomous Weapons". *Sci Eng Ethics* 28, 37. https://doi.org/10.1007/s11948-022-00392-3.

Tay, Shu Ing, Lee Te Chuan, A. H. Nor Aziati and Ahmad Nur Aizat AhmadAhmad. 2018. "An Overview of Industry 4.0: Definition, Components, and Government Initiatives". *Journal of Advanced Research in Dynamical and Control Systems*, Vol. 10, 14-Special Issue, 10.

Turing, Alan M. 1950. "Computing machinery and intelligence". *Mind* Vol. 59, No. 236: 433-460. doi: http://www.jstor.org/stable/2251299.

United Kingdom Ministry of Defense [UK MoD], Defence artificial intelligence strategy, June 15, 2022, https://assets.publishing.service.gov.uk/media/62a7543ee90e070396c9f7d2/Defence_Artificial_Intelligence_Strategy.pdf, last accessed 18 October 2023.

Wiener, Norbert. 1965. *Cybernetics, Second Edition: or the Control and Communication in the Animal and the Machine*. Massachusetts: The MIT Press.

Александар Павић*

Универзитет одбране у Београду,
Школа националне одбране

Хатица Бериша**

Универзитет одбране у Београду, Војна академија

ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА И РАЗВОЈ СТРАТЕГИЈЕ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ – ИЗАЗОВИ И ПЕРСПЕКТИВЕ

Резиме

Правци развоја стратегије националне безбедности увек су по правилу усклађени са виталним националним интересима и модерним тековинама друштва, који су прожети савременим изазовима, ризицима и претњама и расположивим инструментима моћи. Свеобухватно увођење вештачке интелигенције у систем функционисања државе кроз различите области примене имаће значајан утицај на будући развој друштва. Методологија и динамика имплементације зависиће свакако од потреба и могућности државе. Циљ овог истраживања је да анализира могућности вештачке интелигенције у домену одбране, актуелизује тему и приближи стручној јавности. Основна теза овог рада говори да је разматрање могућности примене вештачке интелигенције у будућем развоју система националне безбедности потребно дефинисати у стратешким документима државе. Основна чињеница која иде у прилог тези је све већи утицај вештачке интелигенције на развој аутономних оружаних система, као и измењена физиономија савремених оружаних сукоба.

Начин живота какав данас познајемо инхерентно се ослања на високу технологију, што недвосмислено наглашава потребу за разматрањем важних аспеката употребе вештачке интелигенције. Ово је посебно важно са аспекта приближавања ове револуционарне технологије обичном човеку који од ње очекује оптимизацију и унапређење окружења у којем живи и ствара. Свака технологија која има потенцијал да конкурише људској моћи у процесу одлучивања

* aleksandar.pavic@mod.gov.rs; ORCID: https://orcid.org/0009-0005-6737-0094.
** hatidza.berisa@mod.gov.rs; ORCID: https://orcid.org/0000-0002-9432-5273.

мора се детаљно разматрати и друштвено прихватати у оквирима који не угрожавају универзална људска права. Широка прихватљивост вештачке интелигенције представља неопходан услов за њену примену у стратегији националне безбедности. Претходно наведена чињеница поставља се велики изазов за будуће креаторе политике, који морају балансирати између етичких и функционалних аспеката улоге вештачке интелигенције у нормативно-правном и безбедносном домену.

Разматрање употребе вештачке интелигенције у систему националне безбедности и одбране је од кључног значаја за државу. Напредак вештачке интелигенције значајно ће утицати утиче на развој технолошко-техничких могућности државе. Имплементацијом нових способности у систем одбране вештачка интелигенција ће бити значајно средство обрађања од малициозних активности потенцијалних непријатеља, али исто тако и средство активног деловања у циљу остварења националних интереса. Међутим, употреба вештачке интелигенције у систему националне безбедности представља изазов пре свега у сфери приватности и етике, што захтева развој строгих протокола и норматива за њену употребу. Анализа великог борја извора потврђује постојање напреднијих аутономних оружаних система, што јасно имплицира перспективу њихове примене у будућим оружаним сукобима. Рад даје приказ где су на примеру две стратегије развоја и употребе вештачке интелигенције јасно виде вектори даљег развоја. Имплементација у систему одбране је од суштинског значаја за обезбеђење супериорности у домену одбране националних интереса.

Вештачка интелигенција представља неизоставан аспект модерног живота што даје још један аргумент за њену употребу у систему националне безбедности и одбране. Реалност у којем државе свој систем националне безбедности заснивају на концепту тоталне одбране имплицира да је нужно следити савремене трендове и развијати аутономне оружане системе. Национална безбедност захтева коришћење најновијих технологија, што нас стимулише да развијамо нове концепте и решења, доприносећи тако глобалној безбедности, а уједно и заштити националних интереса. Иако Република Србија нема могућности да самостално развија вештачку интелигенцију, може активно учествовати у међународним пројектима и имплементира инострана решења. Важно је да се дефинишу циљеви, средства и задаци за све чиниоце безбедности

и одбране, како би се имплементирала ова витална технологија. Промовисање друштвеног прихватања вештачке интелигенције, уз поштовање етичких принципа и правних норми, једнако је важно државно питање. Држава треба стратегијски да размишља о остваривању националних интереса и да користи све расположиве ресурсе, пратећи развој својих инструмента моћи и адаптирајући стратегију у складу са савременим концептима.

Кључне речи: вештачка интелигенција, стратегија националне безбедности, аутономни оружани системи, фактор, рат, војне снаге, војни систем, ресурси.

* Овај рад је примљен 25. марта 2024. године, а прихваћен на састанку Редакције 20. јуна 2024. године.