THE USE OF ARTIFICIAL INTELLIGENCE IN MODERN ARMED CONFLICTS

Ivana Z. Zirojević[1]

Достављен: 16. 11. 2023. *Језик рада*: Енглески
Кориговано: 25. 01. 2023., 17. 02. и 12. 03. 2024. *Тип рада*: Прегледни рад
Прихваћен: 11. 04. 2024. *DOI број*: 10.5937/vojdelo2401073Z

Artificial intelligence, as the latest technology of the modern age, represents a set of algorithms, i.e. software tools that, when applied to certain hardware, enable various devices to become "smart", meaning, to be capable to perform many tasks autonomously without constant oversight by man. In modern armed conflicts, artificial intelligence (AI) is used both in various forms of software tools, which help situational analysis and faster decision-making, and in the form applied to hardware when they enable faster identification of targets and more precise targeting. This paper presents forms of artificial intelligence that are most commonly used in today's conflicts. Also, particular emphasis is placed on the use of cyber weapons, which represent ever more significant element of modern conflicts. However, the risks that occur when using AI are also stressed. Although its use reduces certain traditionally recognized risks, new risks emerge resulting from the use of these powerful tools for the purposes of conflicts. The conclusion is that this new technology enables us, as a society, more „humane" conflicts, with fewer victims and less damage, and yet, the use of that technology still depends on people and their reasons for conflicts.

Key words: *artificial intelligence, armed conflicts, cyber warfare, security, new technologies.*

[1] University in Belgrade, Faculty of Security Studies, Belgrade, The Republic of Serbia, email: izirojevic@gmail.com, https://orcid.org/0009-0004-2610-7444.

Introduction

The latest technology that shows the potential to change both the world and armed conflicts is artificial intelligence. The capability of artificial intelligence programs to quickly process enormous quantity of data, and react to them in accordance with assigned task, as well as the machine learning capability, or automated upgrading of existing algorithms based on tasks performed and observed shortcomings and errors, open great possibilities for their application in modern armed conflicts as well. There are different definitions and interpretations of the notion of artificial intelligence, depending on the point of view. In its Report on defining artificial intelligence, the European Commission presented the widely accepted and often quoted definition of the technology of artificial intelligence: “Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or similar).” (European Commission, 2018).

It is important to understand that AI is not just one unique technology, but it should be observed as an infrastructure, as a means that enables more efficient, cost-effective, solid and autonomous exploitation of other technologies and assets (Euronews, 2023). The value of such technological tools has been recognised in the field of security.

A conflict of states aimed at achieving certain interests or political goals still makes the basis for many interstate disagreements. However, most recently, much more common are the new, asymmetrical, hybrid wars, characterised by a different profile of participants, disproportionate forces, expansion of the front across several spheres of life. Today’s wars are characterised by a great complexity and abundance of non-military operations, and as Panarin states “the strategy is not created by a sword, but through using other means” (Panarin, 2019, pg. 53). Such conflict is an ideal field for the application of different artificial intelligence tools. However, potential downsides of the accelerated development of AI weapons are emerging - the algorithms are becoming ever more powerful, the demand grows and, despite high prices, there are non-state factors who more often come into possession of this mighty weapon. That fact is particularly important having in mind that the majority of modern armed conflicts have the character of non-state conflicts, which is supported by information that non-international and guerilla wars and terrorism have been playing a growing part in the overall number of wars over the last thirty years and so (Jeftić, Mišev, Obradović and Stanojević, 2018, pg. 27).

The Role of Artificial Intelligence at Different Levels

It is clear that the use of new technologies brings new possibilities, but we should not disregard the risks associated with it. The role of artificial intelligence, as the new and powerful software tool in modern armed conflicts as a threat to security, can be regarded from multiple points of view. However, one should primarily differentiate its role within the system of defence, within an armed conflict, and the security of the very artificial intelligence systems. At that, one should have in mind that the use of artificial intelligence systems in the system of defence reduces certain traditional security risks (the risk of the loss of personnel - military and civilian, collateral damage), but new risks emerge, such as the vulnerability of armed systems due to greater exposure to software attacks that are connected to the use of AI technologies.In modern armed conflicts artificial intelligence is useful both at strategic, and operational, and at tactical level, through different software or hardware components. Table 1 presents some of currently most common uses of AI tools in modern armed forces.

Table 1.
The use of AI tools at different levels of the system of defence

Level	Strategic	• Facilitates strategic planning • Assists decision-making • Predictive analysis (threat identification)
	Operational	• Logistics • Training
	Tactical	• Data collection • Assists decision-making (quick analysis) • Autonomous weapon systems

Source: Author.

At strategic level, artificial intelligence can facilitate strategic planning and decision-making owing to the tools for the analysis of a great quantity of data from different historical and contemporary sources (for example, the tools for natural language processing, which can sum up trends from a large number of media, social networks and other sources), which enables a better insight into potential threats, allocation of resources and geopolitical trends. Apart from that, a predictive analysis that is based on AI-algorithms can enable earlier threat identification and, consequently, a better preparation for the reaction (for example, development and testing different scenarios of strategic decisions outcomes), and it can assist in better formulation of long-term strategies. Given that these tools are able to quickly and diversely analyse the great quantity of data, thus arriving at conclusions that might be overlooked by man, these tools assist in better self-regulation, self-control and self-activation of different combat systems. For instance, by means of AI, a quick and efficient non-structured data analysis can be produced in the form of photographs, audio or video recordings, as well as the structured analysis of natural language. In that manner, input data can be swiftly and efficiency translated into information that are useful for decision-making on the ground. This type of AI tools is already being used in the current conflict in Ukraine, where the satellite image analysis is done in this way. Furthermore, the tools for machine learning contribute to continuous enhancement of decision-making process.

In the US Armed Forces, one of the most advanced armed forces in terms of the use of AI tools, several such systems are in use, such as: Joint Battle Command-Platform (JBC-P), which integrates satellite photographs, input data from sensors and intelligence, and then analyses and visually presents them using AI algorithms, thus contributing to much easier and faster decision-making process; then there is Artillery Tactical Data System (AFATDS), command and control system that uses AI to process information from different sources, which are used for real-time artillery fire support, as well as the well-known “Maven Project” whose goal is to develop AI algorithms for automated analysis and interpretation of visual data, and to assist responsible authorities with situational analysis and target identification; or Command Post of the Future (CPOF), a system developed in US Defense Advanced Research Projects Agency (DARPA), which is capable of integrating data from various sources using AI technologies, and, on the basis of that, presents a comparative and real state on the ground to responsible authorities, for the purpose of facilitating the process of planning and combat mission execution.

Other states as well work on integrating AI systems into their military capacities, such as France (Combat Digital Cloud – a digital platform that enables fast exchange of information and analysis in real time, thus shortening decision-making time to several seconds), or Israel, whose system of the new generation TORCH-X facilitates quick decision-making, targeting and firing in different environments (Eshel, 2023). At operational level, AI tools are most often used for logistic purposes, and as support to military operations, or for the purpose of a more optimal allocation of resources, personnel or equipment, in accordance with requirements (weather conditions, situation on the ground, enemy positions). Frequent use at this level refers to predictable maintenance and logistics, such as the prediction of the need for equipment maintenance before the failure occurs. For example, GE Predix system enables reading and AI analysis of data from sensors in military equipment, which reduces unplanned delays and improves operational readiness. Also, AI programs for the training of military personnel, such as VBS3 (Virtual Battlespace 3) help providing better and faster training of personnel in more realistic environment.

At tactical level, AI tools can also assist in collecting (for example using UAVs), analysing and understanding the situation in the field (quick analysis of photographs, voice and other input data), hence, they can assist in deciding the following tactical steps. For instance, Advanced Tactical Airborne Reconnaissance System (ATAC) is used for the detection and identification of targets by means of algorithm analysis of pictures gathered through air reconnaissance, and as support in decision-making for pilot personnel. Apart from that, at tactical level, AI algorithms can be found in autonomous weapon systems that, with minimal engagement of military personnel, are able to successfully execute combat tasks. Currently, the most often used are unmanned aerial vehicles, popularly known as drones, which represent fully autonomous or remotely controlled aircraft (of different level of autonomy), which are used in many countries for surveillance, reconnaissance or targeted attacks. Well-known models of unmanned aerial vehicles are: General Atomics MQ-9 Reaper (US aircraft for surveillance, reconnaissance and firing), DJI Phantom Series (aircraft produced by Chinese company DJI (Dà-Jiāng Innovations), whose Phantom series is well-known for its aerography and videography, Heron (unmanned aerial vehicle produced by Israeli company Israel Aerospace Industries, which is used for intelligence purposes, for surveillance and reconnaissance in many countries), CH-4 (Chinese unmanned aerial vehicle, the product of the company China Aerospace Science and Technology Corporation –CASC, intended for reconnaissance and combat missions, known for its reliability and cost-effectiveness), as well as Bayraktar TB2 (Turkish unmanned aerial vehicle, known primarily for its combat missions especially in Syria and Lebanon and recently in Ukraine). Apart from aircraft, increasingly used are unmanned ground vehicles, more precisely, a form of autonomous ground platforms, designed for different purposes - placing mines, demining, reconnaissance or combat. There are even forms of unmanned tanks. This type of autonomous weapons gains in popularity since their use protects human personnel in different operations. Those are small “drones on the ground”, robots equipped with AI programs, which, with different level of autonomy, are able to move and perform tasks. There are also unmanned water platforms which include autonomous surface vehicles (ASV) and autonomous underwater vehicles (AUV) that are used for surveillance, mine recognition and underwater research. Much like the other platforms, they are more or less independent in their work.

Hence, artificial intelligence software, contribute to the enhancement of the levels of contemporary armed conflicts through tools that provide assistance to strategy during decision-making and in lifting the fog of war (incomplete situational awareness and incomplete information in a conflict), while hardware components, modern weapons with embedded AI elements, help waging the war faster, more precisely and from a greater distance. In theory, artificial intelligence should help in reducing the number of victims in war, because better identification of targets and more precise firing reduce collateral damage (Convention on Certain Conventional Weapons, 2018:2), and the use of unmanned platforms reduces the presence, and consequently, the exposure of the military personnel on the ground. However, technological advantages that the use of these advanced tools brings cannot eliminate accidental or intentional human mistakes which evidently happen in modern conflicts. Moreover, cyber warfare is also present in today’s conflicts, which no longer exclusively pertains to cyber space, but, with the integration of software elements and electronic communications in modern weapons, appears in certain form in other combat areas.

One must not overlook security implications of artificial intelligence. Its tools have their flaws as well, such as standard software errors, imperfections of algorithms, poor quality of input data or unpredictability of actions of a model that they are learning. Thus, they can, due to potential unwanted and unpredicted consequences, jeopardise the very project they are engaged on with their autonomous decisions, and consequently, unintentionally pave the way to a new kind of risks, cyber attacks, through the vulnerability of engaged AI technology. Having in mind that the wheel of technological changes rarely goes backwards, and that it is certain that AI tools are going to be more widely applied for security purposes, and used in the conflicts of the future, it is useful to analyse the basic elements of the application of this new technology in modern armed conflicts, and advantages and challenges that it brings to the battlefield.

Types of Artificial Intelligence in Modern Armed Conflicts

Artificial intelligence is already present in modern armed conflicts both through the use of exclusively software tools, and “smart” hardware, classic or modern arms equipped with AI tools. However, given the all-encompassing character of artificial intelligence technology, its application in military activities can be observed from different perspectives, such as, for example, the purpose of its use, the situations in which they will be most often used or AI tools that are to be most often applied. In 20th century, the precursors of today’s artificial intelligence tools were used most often for data collection, reconnaissance, and for logistic calculation. Today, their application has spread to the field of training of troops, precise firing of defined targets, and to cyber space (Schreiner, 2023).

The forerunner of the use of artificial intelligence for military purpose, or the first use of electronic devices for remote data collection and acting in accordance with them, is considered to be the use of a US military electronic system named “Igloo White”. The US military started using this system in the Vietnam War late in 1967, and it consisted of three main components (Shields, 1971): 1) battery sensor for detection of seismic, acoustic or electric signals emitted by enemy vehicles or personnel, 2) aerial platforms for gathering sensor signals, which were forwarded to ground surveillance system or they were analysed at the very platform by trained personnel, and 3) surveillance system for the analysis of received data and issuing orders for immediate reaction regarding the data received. More than twenty thousand different electronic sensors were dropped from aeroplanes over the jungle of Laos, which was traversed by a railway line “Ho Chi Minh” for the provision of supplies to the north Vietnam. The devices were able to capture sounds, measure the seismic activity, and even measure the level of ammonia in the air. On the basis of data obtained in such way, decisions were made on military actions on the ground (National Museum of the United States Air Force, 2023).

Another example that can be considered to be the early use of AI for military purposes is Pentagon’s project of a “smart” truck, from the late eighties of 20th century, which was supposed to autonomously collect soldiers behind enemy lines (Tomić, 2013: 182) or the use of AI software dubbed “Dynamic Analysis and Replanning Tool” (DART) which was used in 1991 to arrange transport of supplies and personnel and to solve other logistic problems, which enabled the US military to make great savings (Artificial Intelligence Timeline, 2019). At the beginning of 21st century, the use of the first unmanned aerial vehicles was recorded that were equipped with artificial intelligence in the modern sense, in different armed conflicts. In Afghanistan and Iraq, the United States of America used armed drones, which, through the use of artificial intelligence algorithms, were capable of conducting autonomous flights, following targets and using weapons (Cole, 2012).

In modern conflicts, it happens that certain areas of application of AI tools overlap, meaning that chronological or technological limit of the application of some of these tools has not been clearly defined. Table 2 presents several most common fields of application of AI tools in different phases of a conflict.

In the period of conducting preparatory activities in case of potential conflicts, AI is used, primarily, for reconnaissance and intelligence gathering, for logistic purposes (to calculate optimal supply-chain, and it assists in speeding up the process of organisation and delivery), and for more efficient process of recruitment and training (of both regular military servicemen and new AI tools and weapons). For example, programmes for the training of personnel, such as the training programme for US Navy, that monitors the learning progress of an individual and adapts the speed of the training (NSWCDD, 2021), contribute to more efficient and cost-effective training of all armed forces branches.

Table 2:
Application of AI tools according to the time of the use

Time of the use	Before conflicts	• Reconnaissance • Data collection • Logistics • Recruitment • Training
	During conflicts	• Assistance in decision-making • Autonomous weapons algorithms
	After conflicts	• Role in information and propaganda • Monitoring • Assessment of security situation

Source: Аутор.

During conflicts, AI is also used for already mentioned purposes, but far more important application of AI tools is the assistance in decision-making and algorithms that control new weapons of different level of autonomy. After conflicts, depending on the outcome, AI tools that can considerably aid the victorious side are those that, through information and propaganda activity, assist so that the defeated accepts the results of the conflict, as well as those tools that enable a higher level of observance and monitoring, and the assessment of security situation (Andresky&Henderson, 2018, стр. iii).

In addition, researchers of Deloitte company have identified several capabilities of AI technology that can be used by military, as a (still) leading actor in contemporary armed conflicts (Table 3).

Table 3:
Possible military areas of application of AI tools (Deloitte, 2023)

	Detection	Planning	Field operations	Support
Armed Forces	The use of AI systems for intelligence gathering and analysis. The use of smart sensors to monitor and detect objects and personnel.	The use of available data and machine learning for the improvement of the process of planning resources and expenditures related to missions or training.	The provision of data in real time and rapid response to improve the mission outcome. Protection of personnel, assets and information.	Speeds up the process of procurement and management of supply contracts. Proposes better solutions for the use of available budget. Support to personnel service in candidate selection process, automated services and salary calculation.

Table 3 (Deloitte, 2023) lists artificial intelligence software tools that can be used for military purposes, stressing their economic, organisational and information aspect of use. These tools help quicker and more reliable acquisition of data necessary for decision-making at strategic, operational and tactical levels, and their analysis and use results in significant savings in the military budget.

In short, according to Vincent Boulanin from Stockholm International Peace Research Institute (SIPRI), at the moment, there are no areas of military activities where artificial intelligence tools cannot be used (Euronews, 2023), but they are most often used within autonomous weapons and for AI assisted decision-making. Another important use of AI tools is in the field of cyber warfare, which goes beyond cyber space because of ever greater networking and reliance on software tools even in conventional arsenal.

Perhaps, due to the constant development of new AI tolls, so far, no detailed division has been developed, or the classification made of AI technologies used in modern armed conflicts, which would include both hardware and software components of this technology. Still, they can be generally presented as software AI tools, or as hardware tools, or weapons with elements of artificial intelligence most often used in today's conflicts. Though the majority of AI tools can be applied at all levels of a conflict, presently, at the tactical level of conflicts, autonomous weapons are most commonly used, while at operational level, AI is used for decision-making. Cyber weapons are used at all levels, but in modern conflicts, perhaps the most dangerous use is at the strategic level, since it can lead to a series of omissions at other levels of modern armed conflicts.

Autonomous weapons

Autonomous weapon systems represent weapon systems with integrated technical capabilities that enables them, after initial activation by man, to act autonomously by means of different platforms on the ground, water, under water, in the aerospace or space, such as drones, torpedoes or different kinds of vehicles.

International discussions have not yielded a generally accepted definition of autonomous weapon systems (Congressional Research Service, 2023, pg. 1). Experts even do not agree on the technical definition of an autonomous weapon (CCW/GGE:1), 2023). Namely, a question is raised as to how to define the autonomy of a weapon - is it enough that an armed system can fully act autonomously or, is it necessary for man to approve the action, and in what cases, and, whether a weapon is autonomous if only one of its components or functions is autonomous. In one analysis (Taddeo&Blanchard, 2022:37) as much as twelve definitions of this kind of weapon systems have been identified, which certain states and international organisations differentiate by attaching different levels of significance to legal, ethical or military issues.

In one of the technologically most advanced armed forces in the world, the US Armed Forces, opinions are divided, hence, as Allen states (Allen, 2022) in the Directive 3009.09 of the US Department of Defence, it is not sufficiently clearly defined what autonomous and what semi-autonomous systems are, and he notes that almost every time that US military talks about "AI projects" they refer to the possibility of machine learning which definitely is not the only distinction of artificial intelligence systems. In the said Directive, lethal autonomous weapon systems are defined as "fully autonomous", or "armed systems that, once activated, can select and engage targets without further intervention of a human operator" (Congressional Research Service, 2023, pg. 1), unlike semi-autonomous armed systems, where man (Bächle and Bareis, 2022:4) selects the target and approves the firing from the weapon system. Weapon system operators, regardless of the level of automation, are demanded to maintain an appropriate level of human judgement regarding the use of force, whereby that level is not clearly defined in the Directive, because of the diversity of very armed systems, the type or context of an armed conflict (Congressional Research Service, 2023, pg. 1). Apart from that, the thing that makes the approach of the US military to the autonomy of development and use of the said armed systems different from some other armed forces or non-state groups is the defined process of testing and evaluating, and precisely defined chain of approving new weapons of that kind and of any alterations that take place in the process of development or use, for instance during machine learning. Such approach certainly is commendable in the sense of the responsibility both to one's own military and to civilians, and it is in agreement with international humanitarian law, but it can bring asymmetric advantage to the other side, which, in case of a conflict and use of autonomous weapons would not dwell on possible consequences of non-compliance with similar standards.

In other states as well, there is similar vagueness that may be caused by not making difference between definitions of the capabilities of the technology (whether a weapons system can do something autonomously or not) and by defining the manner of use of the technology (whether we should and in what way, and under which conditions, allow a system to do something autonomously). In case of the Russian Federation, official position, stated in communication with a group of government experts of the UN Convention on certain conventional weapons (Document of the Russian Federation (2021), it is stated that this state advocates for maintaining human control over lethal autonomous weapon systems regardless of the level of technological development of these systems, but it does not define them in greater detail, and considers that the term "reasonable human control" does not have a factual meaning for further development and use of such weapon systems. On the other hand, certain Russian manufacturers of such weapons routinely refer to their automated and robot military systems as systems equipped with artificial intelligence, although they do not possess whatsoever the capability of machine learning (Alen, 2022), but are controlled by man.

This ambiguity is not surprising, having in mind the continuous and fast development of these new technologies, and the secrecy in which that development takes place. Currently, most often mentioned examples of autonomous weapons equipped with AI technology are unmanned aerial vehicles and other unmanned platforms such as ground or underwater platforms, self-guided missiles and loitering munitions (Filipović, 2023:215).

The advantages of autonomous weapons are not only reflected in the ability to act autonomously once man activates them. Owing to the capability to quickly process great quantities of data, and to act swiftly and more precisely, the tools based on artificial intelligence considerably contribute to the acceleration of the tempo of a war, and enable easier remote attacks and reduce the loss of personnel. One of important advantages of the use of artificial intelligence in conflicts is the increased precision, owing to the models of deep machine learning, which are permanently upgraded thus enabling more precise (real-time) determination and adaptation of the trajectory of fired projectiles, while minimising the complexity of environmental conditions (Li, Zhu & Zhao, 2021:1205), which is why a location need not be fired at, but only the concrete target, even if it is just one man. This, in theory, significantly reduces the devastation of infrastructure, as well as human casualties, both military and civilian. Yet, modern conflicts in Ukraine and Israel show that the existence of technology that enables more humane approach in armed conflicts (Zurek, Kwik & Engers, 2023: 1) still does not ensure its application in real-life conflicts for potentially many reasons (political argumentation, not-knowing or not-possessing modern technology, non-existence of international control).

Moreover, modern AI weapons are still not sufficiently technologically reliable to let them act autonomously; it takes new and more advanced algorithms, especially for more precise targeting and for collaboration, or paired engagement of several pieces of weapons equipped with AI tools (for example drone swarms). That is shown by current developments in Palestine and the Israeli use of weapons guided by artificial intelligence, whose results are still far from acceptable according to the norms of international humanitarian law. At that, one should bear in mind that the artificial intelligence system used by Israeli military, dubbed Habsora (eng. Gospel) is relatively new, since they have been using it for only several years now. Perhaps, because of the urgency for Israel to react to the attack by Hamas, the system was not adequately tested and trained which leads to unreliability, mass destruction and great number of human casualties (Davies, McKernan & Sabbagh, 2023). Also, this system is intended to provide assistance to human operators in decision-making and to speed up target identification, while the very activation of the weapon is done by man, which brings into question the selection of targets such as schools, hospitals or humanitarian organisations' offices.

In any case, the weapon by itself, regardless of the level or degree of development of technology used, cannot ensure advantage in a conflict unless used in a right way and in accordance with a defined strategy and doctrine (Caliskan&Legeois, 2017).

Artificial Intelligence Assisted Decision-Making

While developing a strategy and during its operational transformation into tactics, and during an armed conflict itself, a fast and decisive assessment of time and space represent very important factors. Communication in war is also a great challenge, notwithstanding modern communications, which often enable a higher level of manipulation than classical means of communication, so that the problem of contradictory, false and uncertain reports increases the problem of war projecting. The accuracy and flow rate of information make the basis for good strategic, operational and tactical decisions. Having in mind the influence of data accuracy and the speed of decision-making on the outcome of a conflict, it can be said that artificial intelligence also modifies the combat in some way, as its superiority in processing and delivering information significantly contributes to making faster and better decisions and to adapting given strategy to the situation on the ground.

For those reasons, information domination is becoming more and more important in strategic sense, and it is defined as the superiority in generation, manipulation and use of information. Information domination is becoming an unavoidable element in "decision-making superiority", i.e. in faster and more efficient decision-making process in crisis (Nørgaard & Linden-Vørnle, 2021).

Because of its superiority in said activities, artificial intelligence algorithms are ever more often used as an aiding tool of leaders when making predictions and decisions regarding military activities. Their ability to swiftly process and analyse enormous data basis in different ways, enables making conclusions that may be omitted by man thus helping in better development of strategy and tactics in the field. Tools for machine learning also contribute to continuous enhancement of decision-making process. Apart from that, AI tools can predict more precisely behaviour models of the parties in a conflict, and recommend actions, and enable better understanding of the environment (for example by means of fast analysis of input data such as photographs, audio or video recordings). In that manner, input data can be swiftly and efficiency translated into information that are useful for decision-making on the ground.

However, we must pay attention to the challenges of relying solely on these tools, since they themselves are susceptible to errors and imperfections (hidden hacker attacks, placement of false data, or so-called data poisoning, algorithm mistakes). Specific challenge is presented by software training of decision-making tools, because of a paradox that occurs - if the tools are imperfect, they cannot be realistically used in a conflict, and if they are not used, their learning is impeded in peacetime. In those cases, algorithms are trained using historical data on battles, or data of other countries which makes the training process and the use of AI tools longer and more costly.

Cyber Weapons

Though traditionally not considered as a weapon, powerful algorithms based on artificial intelligence, capable of autonomously searching for and exploiting the vulnerabilities of computer networks and in software, are becoming ever more important attack weapon in modern conflicts. This chiefly refers to software that can access enemy software that control today’s modern weapons, thus incapacitating them. Incapacitating can be done even before the combat (through the placement of computer viruses or placement of false or malicious data), and it can be also done during a conflict, after an AI based weapon has been launched, one can work on the “devaluation” of enemy software.

Perhaps, the area in which, at this moment, artificial intelligence tools are used the most is cyber warfare. Because of the ever-greater transition of cyber tools from cyber space into the real world, the tools related to cyber security, meaning, purely software tools, emerge today in armed conflicts as well. Due to the increased network-centricity, or increased orientation and dependence of military communications on moder communication networks and assets, cyber space, today in the status of the fifth battle space (Putnik, 2022, pg. 55) plays an ever more prominent role. By using cyber assets in the circumstances of armed conflicts, one can significantly influence the strategic decisions of the opposing side (through placement of false or malicious data, unauthorised access to software, change of algorithms), and operational or tactical actions (software aircraft hijacking, jamming enemy communications), while, on the other hand, these tools can be used for the protection of one’s own resources.

The advantage of cyber and AI tools is the fact that they are in the virtual world, easy to hide, difficult to recognise and react to (Kissinger, Schmidt & Huttenlocher, 2022, pg. 151), which makes them an ideal weapon for the assault and defence. The power of cyber weapons often lies in not being recognised (known) by the enemy, who does not even know if the attack happened in the first place (whether someone had unauthorised access to electronical systems) and who is behind it. This leads to asymmetry between the attacker and defender of cyber security, where attackers are in more favourable position. That is why the algorithms for the recognition of attacks or attempts at unauthorised access, and for responding to cyber threats that can significantly jeopardise military actions are becoming irreplaceable segment of modern armed conflicts. These software tools are capable of recognising the schemes of cyber attacks concurrently creating appropriate tools for the defence of the system (Eliacik, 2022).

Apart from that, ever greater reliance of the society and military on communication networks, which make the basis of today's technologies and communication, speeds up the humanity and leads it to the network-centricity, but it increases the vulnerability and sensitivity of states and infrastructural systems to cyber attacks. The higher level of digitalisation of a society, the greater the vulnerability. Because of the increased network-centricity of entire society, cyber conflicts are expanding the front to all spheres of life, so that a successful cyber attack can be catastrophic for many participants. Although, there are mostly no direct human casualties, such attacks could result in accidental, unintentional victims. It can be said that modern conflicts are becoming network-centric as well, since, as Stojanović states, new technologies virtualise new battle space, increase fire power, the speed and precision of action as well as the insight into the real situation, and facilitate real time command (Stojanović, 2020).

Whether we will in the future come to fully autonomous, yet functional artificial intelligence, it depends both on the development of technology, and ethical and legal decisions that should be made in the present. In other words, it is necessary, among other, to raise and solve the issues of autonomy and accountability (Nørgaard, 2021), and apply the solutions in order to end up with artificial intelligence that would be an equal participant in a conflict.

Conclusion

The capability of artificial intelligence programs to quickly process enormous quantity of data, and react to them in accordance with assigned task, as well as the machine learning capability, offer great possibilities for their application in modern, hybrid, and asymmetric armed conflicts. However, for a wider military use it is necessary to further enhance the reliability and precision of AI systems, increase resilience to cyber attacks, reduce the possibility of accidental errors, ensure a reliable operation in diverse environments and advance the process of integration of human decisions with the actions of artificial intelligence combat systems.

Literature

[1] Allen, G. (2022). DOD Is Updating Its Decade-Old Autonomous Weapons Policy, but Confusion Remains Widespread. *Center for Strategic & International Studies, 06. 06. 2022*. https://www.csis.org/analysis/dod-updating-its-decade-old-autonomous-weapons-policy-confusion-remains-widespread. Посећено 5. 6. 2023.

[2] Andresky, N. & Henderson, J. (2018). *Operationalizing Robotic and Autonomous Systems in Support of Multi-Domain Operations* [White Paper]. Army Capabilities Integration Center – Future Warfare Division. https://info.publicintelligence.net/USArmy-RoboticAutonomousMultiDomainOps.pdf. Посећено 01. 07. 2023.

[3] Bächle, T. C. & Bareis, J. (2022). “Autonomous weapons” as a geopolitical signifer in a national power play: analysing AI imaginaries in Chinese and US military policies. *European Journal of Futures Research* 10:20. https://doi.org/10.1186/s40309-022-00202-w.

[4] Caliskan, M. & Liegeois, M. (2017). Technology and War Strategy. Beyond the horizon, 13. 06. 2017. https://behorizon.org/technology-and-war-strategy/. Посећено 28. 7. 2023.

[5] Convention on Certain Conventional Weapons (2018). Humanitarian benefits of emerging technologies in the area of lethal autonomous weapon systems. CCW/GGE.1/2018/WP.4. https://ogc.osd.mil/Portals/99/Law%20of%20War/Practice%20 Documents/US%20Working%20Paper%20-%20Humanitarian%20benefits%20of%20 emerging%20 technologies%20in%20the%20area%20of%20LAWS%20-%20CCW_ GGE.1_2018_WP.4_E.pdf?ver=O0lg6BIxsFt57nrOuz3xHA%3D%3D.

[6] Convention on Certain Conventional Weapons *(2019). Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects. CCW/MSP/2019/9, 13.12.2019. documents-dds-ny.un.org/ doc/UNDOC/GEN/G19/343/64/PDF/G1934364.pdf?* Посећено *08. 06. 2023.*

[7] Convention on Certain Conventional Weapons (2023). Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons System. CCW/GGE.1/2023/CRP.1. https://docs-library.unoda.org/Convention_on_Certain_ Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_ Autonomous_ Weapons_Systems_(2023)/CCW_GGE1_2023_CRP.1_0.pdf

[8] *Congressional Research Service (2023).* Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems. Updated May 15, 2023. Посећено 19.09.2023. https://crsreports.congress.gov/product/pdf/IF/IF11150

[9] Davies, H., McKernan, B. & Sabbagh, D. (2023). ‘The Gospel’: how Israel uses AI to select bombing targets in Gaza. The Guardian, 01.12.2023. https://www.theguardian.com /world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets

[10] Deloitte (2023). The Age of With - The AI advantage in defence and security. Посећено 01.02.2023. https://www2.deloitte.com/ca/en/pages/deloitte-analytics/articles/age-with-ai-advantage-defence-security.html.

[11] Document of the Russian Federation (2021). «Considerations for the report of the Group of Governmental Experts of the High Contracting Parties to the Convention on Certain Conventional Weapons on emerging technologies in the area of Lethal Autonomous Weapons Systems on the outcomes of the work undertaken in 2017-2021». https://documents.unoda.org/wp-content/uploads/2021/06/Russian-Federation_ENG1.pdf. Посећено 19.09.2023.

[12] Eliacik, E. (2022). Guns and Codes: The era of AI-wars begins, Dataconomy Media GmbH*, 17.08.2022.https://dataconomy.com/2022/08/17/how-is-artificial-intelligence-used-in-the-military/.* Посећено *26.06.2023.*

[13] Euronews (2023). È pericolosa l'intelligenza artificiale in guerra? Quanto?. 18.02.2023. https://it.euronews.com/2023/02/18/e-pericolosa-lintelligenza-artificiale-in-guerra-quanto. Посећено 28.7.2023.

[14] *European Commission* (2018). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Artificial Intelligence for Europe, Brussels, 25.4.2018 COM (2018), 237 final (2018). Brussels. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237.

[15] Eshel, T. (2023). Advancing Battle Management Systems. European Security & Defence. 21. 03. 2023. https://euro-sd.com/2023/03/articles/30027/advancing-battle-management-systems/ . Посећено 19. 09. 2023.

[16] Filipović, A. (2023). Lethal autonomous weapon systems (laws) – towards global regulation or indiscriminate employment?. *ПОЛИТИЧКА РЕВИЈА бр. 01/2023, год.* (XXXI) XXIII vol. 75. DOI 10.5937/polrev75-43187.

[17] Jeftić, Z., Mišev, G., Obradović, Ž., i Stanojević, P. (2018). Savremeni konflikti i njihove tendencije. Vojno delo 7/2018, str. 23-40. DOI: 10.5937/vojdelo1807023J

[18] Kissinger, H. A., Schmidt E. & Huttenlocher D. (2022). The Age of AI and Our Human Future. London: John Murray.

[19] Li, W., Zhu, Y. & Zhao, D. (2021). Missile guidance with assisted deep reinforcement learning for head-on interception of maneuvering target. *Complex & Intelligent Systems (2022)* 8:1205–1216. https://doi.org/10.1007/s40747-021-00577-6

[20] Nørgaard, K. & Linden-Vørnle, M. (2021). Cyborgs, Neuroweapons, and Network Comman. Scandinavian Journal of Military Studies, Volume: 4 Issue: 1, 94–107. https://sjms.nu/articles/10.31374/sjms.86#B1, DOI: 10.31374/sjms.86. Посећено 28.7.2023.

[21] National Museum of the United States Air Force (2023). Igloo White. https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/195948/igloo-white/. Посећено 24.05.2023.

[22] Naval Surface Warfare Center Dahlgren Division (2021). My Navy Learning provides personalized, adaptive learning for Sailors. NSWCDD DNA Public Affairs, 20.08.2021. https://www.navsea.navy.mil/Media/News/Article-View/Article/2740281/my-navy-learning-provides-personalized-adaptive-learning-for-sailors/. Посећено 25.05.2023.

[23] Панарин, И. Н. (2019). *Хибридни рат: Теорија и пракса* (Драгана Стефановић, прев.) (Гибриднаја воина: теорија и практика, Москва: Горјачаја линија - Телеком, 2018). Београд: Клуб генерала и адмирала Србије, Удружење Милутин Миланковић.

[24] Путник Н., (2022). *Сајбер рат и сајбер мир* (1. издање). Београд: Академска мисао: Факултет безбедности.

[25] Стојановић, С. (2020). Ратови 21. века и класична стратегијска мисао. Изазови савременог света: стратешко деловање држава или резултанта глобалних и локалних процеса и повода?, Стратешке студије, Vol. 1 (2020), Article 2 (p. 30–44), https://doi.org/10.18485/fb_iss.2020.1.ch2. Посећено 28.7.2023.

[26] Schreiner, M. (2023). AI in war: How artificial intelligence is changing the battlefield. The Decoder, January 9th, 2023. https://the-decoder.com/ai-in-war-how-artificial-intelligence-is-changing-the-battlefield/. Посећено 30.05.2023.

[27] Shields, H. S. (1971). *Project CHECO Southeast Asia Report*. Igloo White, January 1970-September 1971, DEFENSE TECHNICAL INFORMATION CENTER. https://apps.dtic.mil/sti/citations/ADA485194 . Посећено 25.05.2023.

[28] Taddeo, M., Blanchard, A. A Comparative Analysis of the Definitions of Autonomous Weapons Systems. *Sci Eng Ethics* **28**, 37 (2022). https://doi.org/10.1007/s11948-022-00392-3

[29] Томић, Б. М. (2013). Развој мисли у кретању до мултидисциплинарности: преломни тренутак за вештачку интелигенцију. *ВОЈНО ДЕЛО, јесен/2013.* УДК: 113/119:167 ; 004.8 ; 159.955.

[30] Zurek, T., Kwik, J. & Engers, T. van (2023). Model of a military autonomous device following International Humanitarian Law. *Ethics and Information Technology (2023)* 25:15. https://doi.org/10.1007/s10676-023-09682-1

Summary

Throughout history, armed conflicts have often been the biggest users, but also the main drivers of the development of new technologies of the time. Currently, the most state-of-the-art technology is artificial intelligence, that is, software programs capable of independent learning and improvement. Since the beginning of the development of artificial intelligence in the middle of the twentieth century, this technology has been used in various forms mainly as software tools for gathering and analysing information.

In modern armed conflicts, artificial intelligence is used both in various forms of software tools, which help situational analysis and faster decision-making, and in the form applied to hardware, i.e. to various weapons and unmanned platforms, when they enable faster identification of targets and more precise targeting, thereby significantly influencing the course and outcomes of contemporary armed conflicts. The use of cyber weapons is significant as well, although it does not fit the classic definition of weapons, as it is an increasingly important element of modern conflicts, due to the influence of cyber warfare in traditional combat areas.

Artificial intelligence tools are used in all phases of a conflict. Before the actual conflict, they can be used for information gathering and reconnaissance, for logistical calculations that contribute to the savings in the military budget, as well as to easier, faster and more adequate recruitment and training of military personnel. During the unfolding of the conflict, decision-making tools are already in use, as well as algorithms for managing autonomous weapon systems, while after the conflict, various artificial intelligence tools help in further monitoring and assessing the security situation, and their informational and propaganda role should not be neglected either in the occupied territories.

The use of various artificial intelligence tools in the military today takes place at all levels: strategic, operational and tactical. At the strategic level, its importance lies in software that can perform predictive analysis and assist the authorities in decision-making, thus facilitating strategic planning. At the operational level, AI software is most commonly used today to assist in logistics and training of military personnel. At the tactical level, AI tools are most widely used in the collection and rapid analysis of data in the field, enabling rapid tactical decision-making and facilitating identification of targets, as well as in the software that manage autonomous weapon systems.

However, the use of this new technology creates new risks (algorithmic and software errors, hacker attacks), but also reduces certain traditionally recognized risks of conflict (fewer civilian and military casualties, less destruction of infrastructure). For these reasons, the great challenge of the human society is to find a balance between the possibilities provided by artificial intelligence and its adequate use and control. This new technology enables us more „humane“ conflicts, with fewer victims and less damage, but in the end, the use of that technology still depends on people who use it and on their reasoning.