

THE USE OF CYBERNETIC SYSTEMS BASED ON ARTIFICIAL INTELLIGENCE AS SUPPORT FOR THE DECISION-MAKING PROCESS IN THE MILITARY FIELD

Eugen Valeriu POPA

Vice President of STRATEGIKON, Bucharest, Romania

eugen.popa@strategikon.ro

ABSTRACT

In the future, at the strategic, operational, and tactical levels of warfare, replacing human will and human decision with autonomous Artificial Intelligence (AI) weapon systems becomes every day a high possible scenario. These systems are already in use and have the ability to successfully deal with threats faster than humans. Countering AI weapon systems will represent a great challenge in a future war. Both military and commercial robots will in the future incorporate “artificial intelligence” (AI) that could make them capable of performing tasks and missions on their own. In the military context, this gives rise to a debate as to whether such robots should be allowed to carry out missions, especially if there is a possibility that any human life may be in the line of fire. Thus, it can be stated that unconventional knowledge will be required for successfully defeat of such a weapon system.

KEYWORDS: Artificial Intelligence Big Data, Autonomous Weapon Systems, cyber security, Quantum Computing, drones

1. Introduction

Artificial intelligence (AI) broadly refers to any human-like behavior displayed by a machine or system. In the most basic form of AI, computers are programmed to “mimic” human behavior, using extensive data from previous examples of similar behavior. This can range from recognizing the differences between a drone and a bird to performing complex activities in a wide operational space, the determining processes of which can take place transcendently or simultaneously both in the classical area of military operations and in the civilian area, offering the possibility of rapid analysis of some scenarios that can take into account both the capability of operative units in the

area of operations, but also, for example, the influence of public opinion in the strategic decisions of the political factor and the way in which these decisions influence the behavior of military commanders.

The various expressions of modern military phenomena, from clandestine operations to the most complex forms of war, have demonstrated that the use of all means in direct combat operations is increasingly modifying the classical principles of a direct confrontation between the military capabilities of the belligerents, so that most of the determining processes that characterize a military operation, have become processes that exceed not only the military domain but also the traditional

geographic, economic, or political spaces of the belligerents. In the last decades, the global exponential development of both online information systems, but also the ever-increasing access of the population, the economic environment or political organizations, to expert analysis and synthesis systems, has made the determining processes of a military operations, even limited to a geographical area, have a complexity and speed of evolution impossible to perceive by the human factor through classical means of analysis, synthesis, evaluation and prediction.

Originally appearing as an opportunity and later becoming a necessity, the use of cyber systems based on concepts of “Big Data” and AI in the military environment not only provides military command structures with a real-time simulation for the consequences of approaching a certain strategy, but also has the ability to take tactical decisions at a local level, a concrete example being the drone systems that have the ability to jointly coordinate their actions without the intervention of a human operator in order to achieve an objective, being capable of developing optimal research strategies, camouflage or strategic or tactical maneuvers (Kallenborn, 2021). During operations in Gaza in mid-May 2021, the Israel Defense Forces (IDF) used a swarm of drones coordinated by an independent cyber system based on AI to locate, identify and attack Hamas militants (New Scientist, 2021).

The use of expert systems based on AI, by the military environment, will not be limited only to the battle spaces where they have an immediate decisive role, such as the cyber space, with the immediate objective of acquiring informational superiority, or to the automation of some decisions tactics involving the combination of several types of forces (naval, land, air, etc.), but these expert systems will be used more and more by “outsourced” decisions, especially from the logistics area, in processes that are involved mainly in organizing and preparing the fight.

The main opportunity element of using AI in the development of an optimal logistics system adapted to military operations with specific objectives also results from the fact that in recent decades, military analysts have observed that “during a military confrontation, direct combat operations occupied only 15-20 % of the effort, the rest being allocated to the activities of organizing and preparing the fight” (Stăncilă & Grecu, 2002). If the military confrontation reaches the level of a continuous confrontation, “as the last expression of the competitive phase, the irreconcilable phase” (Onișor, 1999), the war being waged on all levels and by all means (military, informational, economic, political, social, etc.), having at your disposal an expert logistics system based on an AI core connected to Big Data information systems, and built on “Quantum Computing” systems can provide indicators of tactical superiority of your own forces that cannot be matched by an enemy that uses classical systems.

From the strategic perspective, “the principles of war are not the same as those of combat operations, since war is a much more complex phenomenon, and combat operation is only a procedure, a way of action, of conducting the war, even a stage of it” (Onișor, 1999), the expert systems based on AI have the ability to bring at the level of political decision makers, at least the understanding, if not the ability to decide on some military strategies, by simulating, with a high degree of accuracy, the effects of such decisions on the course of the war. Thus, for example, the use of military force in a direct confrontation could be optimized from the perspective of the principle of capacity, together with elements of deterrence and elements related to the principle of prevention, such as the use of political, economic and military pressure or the embargo, boycott and blockade, or preventive strikes, and this optimization will be available in real time.

2. Typology of the AI Systems

As a classification, AI systems can be viewed from two perspectives:

2.1. Classification Based on Functionality:

- *Reactive Machine* – This AI has no memory power and no ability to learn from past actions. As example, the “Deep Blue” system from IBM can be used.
- *Limited theory* – With the addition of memory, this artificial intelligence uses information from the past to make better decisions (Sameer Bedar, 2022). Common apps like GPS location apps (Waze) fall into this category.
- *Theory of mind* – This A.I. is still under development in the academic environment, being created with the aim of having a very deep understanding of the human mind, (Sameer Bedar, 2022) its limits being the replication of a pre-existing human cognitive model. Even with this limitation, these systems are able to make decisions and elaborate various correlative models, certain limits of variation, similar to the human cognitive model that they replicate. Particularly interesting is the development of this type of machine for replicating collective cognitive models like simulating the decision vectors inside of a social group (Dubynin & Shishkin, 2017).
- *Self-aware AI* – This artificial intelligence, which could understand and evoke human emotions, as well as develop its own emotional states, is still only hypothetical, currently the metrics and taxonomy of such systems are still the subject of theoretical studies in academic research groups (Hong Lu et al, 2021).

2.2. Classification According to the Purpose of the System:

- *Artificial Narrow Intelligence (ANI)* – A system that performs narrowly defined scheduled tasks. This AI has a combination of reactive and limited memory capability. Most AI applications today fall into this category.
- *Artificial General Intelligence (AGI)* – This AI is able to train, learn, understand and perform tasks very similar to a human operator.
- *Super Artificial Intelligence (ASI)* – This AI performs tasks better than humans due to its superior data processing, memory and decision-making abilities. There are no real-world examples today.

Although most known AI systems are powered by algorithms based on systems of finite equations, using techniques such as machine learning and deep learning, to demonstrate “intelligent” behavior (Alcayde-García et al, 2022) implemented using classical cybernetic systems (hardware and operating systems) with sequential processing, where for finding a unique solution of a system of equations a finite number of iterations (Starzyk & Prasad, 2010) must be performed, compared with the use of “Quantum Computer” technology, where the solution of finite equations is instantly available despite of complexity of such an equations, can dramatically change the size and speed of development of AI cores (Zhong & Yuan, 2013).

A cybernetic system “learns” (Khedkar, 2022) when its AI core is able to successfully predict and react to unfolding scenarios based on previous results in similar scenarios (variation of a set of input parameters based on previously unknown functions). Machine learning refers to the process by which computers develop pattern recognition, or the ability to continuously learn and make predictions based on the correlation of various data

sets, and can make adjustments without being specifically programmed to do so. A form of artificial intelligence, machine learning effectively automates the process of building analytical models and allows machines to adapt to new scenarios independently.

There are three methods of machine learning (Khedkar, 2022):

- *Supervised* – learning works with labeled data and requires less training.
- *Unsupervised* – learning is used to classify unlabeled data by identifying patterns and relationships.
- *Semi-supervised* – learning uses a small set of labeled data to guide the classification of a larger set of unlabeled data.

3. Analysis of AI Systems and Their Applicability

Deep learning is a subset of machine learning that has demonstrated significantly superior performance compared with traditional machine learning approaches (Avant-Garde-Technology). Deep learning uses a combination of multi-layered artificial neural networks and data-intensive training and modeling, inspired by the latest understanding of human brain behavior (Avant-Garde-Technology). This approach has become so effective that it has even begun to surpass human abilities in many areas, such as image and speech recognition or natural language processing (Avant-Garde-Technology). Deep learning models process large amounts of data and are typically unsupervised or semi-supervised (Avant-Garde-Technology).

Extensive research in academia and industry results in shorter training time for systems and increasingly better results (Khedkar, 2022; Maxwell, 2020). Many systems designed for these tasks are in use today and produce very good results, but most AI systems in operation for the military and civilian domains are trained to

perform a single task and only under very specific circumstances, because unlike humans, these systems do not adapt well to new environments and tasks (Khedkar, 2022; Maxwell, 2020).

On the other hand, the models operating with AI systems are improving daily, showing their value in many applications. The performance of these systems can make them very useful for tasks such as identifying a T-90 (Khedkar, 2022; Maxwell, 2020) command battle tank in a satellite image, identifying high-value targets in a crowd using facial recognition, translating (Khedkar, 2022; Maxwell, 2020) text for analysis/synthesis from open source intelligence and text generation for use in information operations or PsiOps. The application domains in which AI has been most successful are those where there are large amounts of labeled data (Khedkar, 2022; Maxwell, 2020), such as ImageNet, Google-like search engines, and text generation. AI is also considered to be highly capable in areas such as recommendation systems, anomaly detection, prediction systems and competitive gaming.

An AI-based cyber system in these areas could help the military detect fraud in its contracting services, predict when weapons systems will fail due to maintenance problems, or develop winning logistics strategies in conflict simulations (Khedkar, 2022; Maxwell, 2020). Such a system is currently under development by the US Department of Defense, being supplied by the consortium between Palantir Technologies and Army Research Lab.

AI algorithms are able to collect and process data from a multitude of different sources to help make decisions, especially in crisis situations. In many circumstances, AI systems can quickly and efficiently analyze a situation and make the best decision in a critical situation. AI-based systems also have the ability to neutralize biases that may arise with the human input, with the disclaimer that AI may not yet have a fully

developed understanding of human ethical concerns. All of these applications and more can be force multipliers in day-to-day operations in the next conflict (Khedkar, 2022; Maxwell, 2020).

The projects under development that have AI-based systems in their component have highlighted a series of challenges in the definition, implementation and operation of such systems in real situations. The biggest problem is that developers need access to data and as most of this data is classified, the definition, implementation and especially training of such systems become a very sensitive topic. Many AI systems are trained using data that has been labeled by an expert system (Khedkar, 2022) (for example, labeling scenes that include an air defense battery) where the human component is at the core, and such large data sets are often labeled by military specialists in cooperation with private companies using manual methods. Getting this data and sharing is a challenge, especially for an organization that prefers to classify data and restrict access to it (Khedkar, 2022).

An example of a military dataset might be one with images produced by IMINT (Image Intelligence) systems and labeled by experts to describe the weapon systems found in the image, if any (Khedkar, 2022). Without sharing this with preprocessors and developers, an AI that uses this set effectively cannot be created (Khedkar, 2022). Due to the complexity of the logical infrastructure and the limitation of the hardware on which they run, AI systems are also vulnerable to becoming very large (and thus very slow) and consequently susceptible to “dimensionality problems” (Khedkar, 2022). The use of “Quantum Computing” hardware infrastructures eliminates the latency of large systems, but at the moment the number of specialists capable of developing such systems is limited to the level of a few dozen universities that develop “Quantum

Computing” type processor infrastructures. Put another way, training AI to recognize images of every possible weapon system would involve thousands of categories. Such systems will require an enormous amount of computing power and a lot of time dedicated to those resources (Khedkar, 2022). And, because for a comfortable efficient training of a model, it requires an infinite amount of these images to be completely accurate, this is something we cannot achieve (Khedkar, 2022). Furthermore, as we train these AI systems, we often try to force them follow “human” rules, such as grammatical rules. However, humans often ignore these rules, thus making developing successful AI systems for things like sentiment analysis (Khedkar, 2022) combined with speech recognition to be a really difficult task.

Another problem with AI systems is that under certain conditions, they can be easily fooled if the adversary has information about the underlying models with which the core was initially trained. This conceptual vulnerability was recently demonstrated by a team of engineers from the cyber security laboratory of the IT giant TENCENT in China who, through the controlled manipulation of data provided by the sensors of a TESLA driverless vehicle, managed to completely confuse the AI system that was driving that vehicle (Knight, 2019). Also, related to the initial data set used to train some AI systems, during the implementation of the test projects, limitations of the apparently super-human models were determined.

An AI’s image processing capability is not very robust when giving images that are different from its training set—for example, images in poor lighting conditions, that are at an obtuse angle, or that are partially obscured (Khedkar, 2022). Unless these types of images were in the training set, the model may struggle or even fail to accurately identify the content (Khedkar, 2022). Prediction systems, such as IBM’s Watson weather forecasting tool,

face problems of dimensionality and availability of input data due to the complexity of the systems they are trying to integrate into a finite model. Another simple weakness of an AI based system is its inability to perform interpolated multitasking roles. A human is able to identify an enemy vehicle, decide which weapon system to use against it, predict its trajectory, and then engage the target, almost in no time by parallel processing of parts of each task. This fairly simple set of tasks is currently impossible for an AI system to accomplish (Khedkar, 2022).

At best, a combination of AI's could be built where individual tasks are given to separate models. This kind of solution, even if it is feasible, would involve a huge cost in training it, would require a huge amount of computing power, not to mention training and testing the system. Many AI systems are not even able to transfer their learning to the same domain (Khedkar, 2022). For example, a system trained to identify a T-90 tank would most likely be unable to identify a Chinese Type 99 tank, (Khedkar, 2022) despite the fact that both are tanks and both tasks are image recognition. Also, AI systems implemented on sequential computing systems have great difficulties in interpreting the variations of the input set and the context that determines these variations or temporary missing of some subsets from the input parameters. These AI processor recognition systems do not understand what the image is, but simply learn the textures and gradients of the image pixels. In the case of scenes with the same gradients, the AI easily identifies parts of the image incorrectly. This lack of understanding can lead to misclassifications that humans would not make, such as identifying a boat on a lake as a BMP-3 vehicle (TAIFV, 2022).

Even without these weaknesses of AI-based systems, the main area where military research must pay special attention is that of the cyber defense of these systems.

We must assume that potential adversaries will try to trick or penetrate any accessible AI systems that military infrastructures use. The enemy will try to trick AI engines and image recognition sensors, cyber attacks will try to avoid intrusion detection systems, and logistics systems will be fed with altered data to block logistics supply flows with false demands. Conceptually, these attacks can be divided into three categories (Chase et al, 2021):

- *“Evasion” type* – during pilot project implementations these types of attacks have been shown to be easy to perform and often do not require computational skills. Attacks of this type often try to trick an AI engine in the hope of avoiding detection hiding a cyber attack, for example, or convincing a sensor that a tank is a school bus (Khedkar, 2022). The main survival skill in the field of combat operations may be the ability to hide from the sensors that feed enemy AI systems. As a result, military research may need to develop a new type of AI camouflage to defeat these systems, as it has been observed that for example a simple masking techniques, (Khedkar, 2022) such as placing bands of various colors in a certain pattern on a vehicle, can trick the AI systems.

- *Inference type* – whereby attackers cause a target machine learning model to divulge information about its training data to the attacker, with the adversary's main goal being to try to reconstruct the recordings used to train the AI core. Evasion attacks are often followed by inference attacks that obtain information about the AI system, which can then be used later to enable evasion attacks (Zi Hao Zhao et al, 2021).

- *Poisoning type* – aims the AI systems during training process in order to alter the ability of the these systems to make correct decisions, through enemy access to the data sets used to train the AI core. As a result, for example, mislabeled

images of vehicles can be introduced to fool targeting systems or manipulate maintenance data designed to classify imminent system failure as normal operation. Given the vulnerabilities of logistical supply flows, this would not be unimaginable, and furthermore, such an alteration would be difficult to detect if the AI system went live.

– *Extraction type* – exploit the access to the AI interface to learn enough about the operation of the AI in order to create a parallel model of the system (Khedkar, 2022). If the AI cores are not protected from unauthorized users, then those users could predict the decisions made by our systems and use those predictions to their advantage (Khedkar, 2022). We could imagine an adversary that will predict how an AI – controlled unmanned system will respond to certain visual and electromagnetic stimuli and thus influence its trajectory and behavior.

From the perspective of international legal regulations, which refer to the ethics of using AI systems and the rules of engaging these systems in combat operations, at this moment there are only incipient concerns. Many systems already use AI to some degree, but the next big step expected by many military strategists is the development and adoption of fully autonomous weapons systems, known as “Lethal Autonomous Weapons Systems” (LAWS) (Devison, 2017).

4. Discussions and Conclusions

Several non-governmental organizations, civil society, government representatives and industry members involved in the development of core AI-based systems have highlighted the importance of LAWS regulation. Some argue that a complete ban is the way to go, given the risks. Others argue that there should be at least a requirement for significant human control in the deployment of these weapons. At the moment, the subject is under discussion

within the United Nations. States parties to the Convention on Conventional Weapons (CCW) engaged in negotiations annually, from 2014 to 2016, when they decided to establish a Group of Governmental Experts.

While there is no doubt that AI core-based systems will be part of the future of military capabilities around the world, the landscape is changing rapidly in terms of evolving destructive capabilities. Artificial intelligence is advancing, but given the current struggle to give computers true knowledge and behaviors based on expert systems, as well as the limitations of the sensors that feed these systems with data, it will take some time for AI to be able to approximate human intelligence in high uncertainty actions characteristic to most real military operations.

Given the current inability of artificial intelligence to deliver real results with a high degree of predictability, a mandatory requirement in such high-stakes settings, it is understandable that many people want to ban autonomous weapons, but the complexity of the field means that any limitation should be carefully analyzed. Fundamentally, for example, the term autonomous weapon describes the actual weapon, that is a missile on a drone, or the AI that operates that drone?

From another perspective, the impact of the commercial market relative to the rapid expansion of autonomous systems development (Rodriguez, 2012) concerns cannot be overstated, and an even greater short-term problem is how to fully understand the global implications of the visible shift in the power base of AI expertise from military to commercial enterprises (Parly, 2019). AI-based computer systems are developing primarily because AI specialists are becoming more intelligent, so this relatively small pool of human experts is becoming a critical commodity. Up to this moment universities respond very slowly to this demand, and governments and industry have also lagged

behind in providing incentive mechanisms for students in AI systems field of expertise. Finally, increased commercial activity in using AI core for IT systems in automotive, logistics, etc., both in terms of attracting top talent and expanding the

capabilities of autonomous systems in everyday commercial products could be a double-edged sword that will undoubtedly affect military systems around the world in ways hard to imagine.

REFERENCES

Avant-Garde-Technology. Available at: <https://www.avant-garde-technologies.com/ai-ml-ds-bi>.

Alcayde-García, F., et al. (2022). *Power Transmission Lines: Worldwide Research Trends*, available at: <https://doi.org/10.3390/en15165777>.

Bedar S., (2022). *What is explainable artificial intelligence?*. Available at: <https://yoo.rs/what-is-explainable-artificial-intelligence>.

Devison, N. (2017). *A Legal Perspective: Autonomous Weapon Systems under International Humanitarian Law*. Available at: https://www.icrc.org/en/download/file/65762/autonomous_weapon_systems_under_international_humanitarian_law.pdf, accessed on 08 October 2022.

Dubynin, I.A., & Shishkin, S.L. (2017). Feeling of Agency versus Judgment of Agency in Passive Movements with Various Delays from the Stimulus. *Psychology in Russia, Vol. 10, Issue 3*, 40-56.

Lu, H., Hu, W., & Pan, C. (2021). *Artificial Intelligence and Its Self-Consciousness*, available at: <https://doi.org/10.1145/3456389.3456402>.

Kallenborn, Z. (2021). Israel's Drone Swarm over Gaza Should Worry Everyone. *Defense One*. Available at: <https://www.defenseone.com/ideas/2021/07/israels-drone-swarm-over-gaza-should-worry-everyone/183156/>, accessed on 08.10.2022.

Maxwell, P. (2020). Artificial Intelligence is the Future of Warfare (Just Not in the Way You Think). Available at: <https://mwi.usma.edu/artificial-intelligence-future-warfare-just-not-way-think>.

New Scientist. (2021). *Israel Used World's First AI-Guided Combat Drone Swarm in Gaza Attacks*. Available at: <https://www.newscientist.com/article/2282656-israel-used-worlds-first-ai-guided-combat-drone-swarm-in-gaza-attacks/amp/>, accessed on 08 October 2022.

Onișor, C. (1999). *Teoria Strategiei Militare*, Bucharest: AÎSM Press, 182, 183.

Parly, F. (2019). *Artificial Intelligence in Support of Defence*. Available at: <https://www.defense.gouv.fr/sites/default/files/aid/Report%20of%20the%20AI%20Task%20Force%20September%202019.pdf>.

Knight, W. (2019). Military artificial intelligence can be easily and dangerously fooled. *MIT Technology Review*. Available at: <https://www.technologyreview.com/2019/10/21/132277/military-artificial-intelligence-can-be-easily-and-dangerously-fooled/>.

Khedkar, A.A. (2022). *What is Artificial Intelligence (AI) and how is it changing the world?* Available at: <https://ashokakhedkar.com/blog/what-is-artificial-intelligence-ai-and-how-is-it-changing-the-world>.

Starzyk, J., & Prasad, D.K. (2011). A Computational Model of Machine Consciousness. *International Journal of Machine Consciousness, Vol. 1, Issue 2*, 24-30.

Stăncilă, L., & Grecu, I. (2002). *Lupta armată modernă*, Bucharest: AÎSM Press, 9.

Zhao, B.Z.H., et al, (2021). *On the (In) Feasibility of Attribute Inference Attacks on Machine Learning Models*. Available at: <https://doi.org/10.48550/arXiv.2103.07101>.