BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Artificial intelligence in multidomain operations: a SWOT analysis

Captain (N) (r) Sorin TOPOR, Ph.D.*
Adrian Victor VEVERA, PhD. Eng.**
Alexandru Georgescu, Ph.D.***
Ella Magdalena Ciupercă, Ph.D.****

*National Institute for Research and Development in Informatics ¨– ICI Bucharest/
Associate member of the Romanian Academy of Scientists
e-mail: sorin.topor@ici.ro
**National Institute for Research and Development in Informatics – ICI Bucharest
e-mail: victor.vevera@ici.ro
***National Institute for Research and Development in Informatics – ICI Bucharest
e-mail: alexandru.georgescu@ici.ro
****National Institute for Research and Development in Informatics – ICI Bucharest
e-mail: ella.ciuperca@ici.ro

Abstract

Multidomain operations are a strategic concept that integrates multiple domains of operation (land, sea, air, space and cyber) to achieve common objectives in a complex and dynamic environment. In the context of rapidly evolving technology, Artificial Intelligence (AI) has become an essential tool for optimizing and streamlining multi-domain operations, providing innovative solutions for sectors such as mobility and maneuver of forces and weapons, logistics, decision-making and other military technologies. In this paper, we will highlight the applications, benefits and challenges associated with the implementation of AI in multi-domain operations through a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis and propose some future development directions.

Keywords:
Artificial Intelligence; multidomain operations; SWOT analysis.

Article info
Received: 15 February 2025; Revised: 3 March 2025; Accepted:14 March 2025; Available online: 2 April 2025

Citation: Topor, S., A.V. Vevera, A. Georgescu și E.M. Ciupercă. 2025. "Artificial intelligence in multidomain operations: a SWOT analysis". *Bulletin of "Carol I" National Defence University*, 14(1): 108-121. https://doi.org/10.53477/2284-9378-25-07

The implementation of Artificial Intelligence (AI) in multi-domain operations is considered a turning point that will provide innovative solutions, based on the valorization of all previous experiences and knowledge of the military domain and incorporating not only new capabilities in data processing and decision-making systems, but also other emerging technologies such as augmented reality, quantum cryptography and new cybersecurity models.

However, the success of its implementation depends on the correct approach to weaknesses and threats, as well as capitalizing on strengths and opportunities. In our paper, through SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis we will demonstrate that an army that invests in AI, in a balanced perspective, combining technological innovation with ethical and strategic responsibility, will not only have an essential decision-making support tool but also has a real capability to connect to an increasingly intelligent future.

State of the art - the specificity of using AI in multidomain operations

Initially, multidomain operations were considered a set of operational functions. Today, they represent a central doctrinal element through which modern armies are shaped and soldiers are transformed into fighters capable of facing future military operations. Multidomain operations integrate the use of space and cyber capabilities in land, air and naval operations (FM3-0 2022). This historical stage represents a revolution in the conduct of military operations in that, for the first time, technologies specific to these capabilities were used by adversary forces to challenge decisions and execute offensive measures against their own combined forces.

The operational environment understanding model represents the absolute novelty of this new doctrine. Knowledge of the operational environment is the precursor to any effective activity. It is made up of five domains (land, maritime, air, outer space and cyberspace) and three dimensions (physical, informational and human). For its knowledge and understanding, disruptive technology, especially AI, represents a real support for the collection, analysis and processing of information, support in the development of decisions and in the dissemination of information to autonomous combat platforms or which integrate command-control (C2) systems of different capabilities and specific to each domain.

Cyberspace, one of the five domains of the operational environment, integrates digital networks and information technology infrastructures, resident information, telecommunications networks, computer systems, embedded processors and controllers, relevant frequency bands in the electromagnetic spectrum, etc., into global networks that allow fast connections, anywhere and anytime, as well as the geostrategic context in which they operate (Vevera and Ciupercă 2019). The systems that operate within these networks are of one's own forces, friendly or allied, of

enemies, of host nations or supporters of a cause, communication and mobile telephony systems, social and media networks, and other technical infrastructures such as weapons, autonomous platforms, computers, controllers, etc.

AI has the potential to be the most important technological development of the historical period we are going through, attracting the attention of many specialists in the field of security and defense sciences. In fact, the final report of the US AI Security Commission (Final Report 2025) mentions that this technology is so versatile that a historical parallel can be drawn with the transformative effect of electricity in all fields of human activity, an effect that the American inventor Thomas Edison described as "a field of fields... it holds the secrets which will reorganize the life of the world" (Schmidt 2021).

The current stage of development and implementation of AI is at a level where we can encounter new threats and vulnerabilities, as well as disruptive events, as a result of the large-scale implementation of the technology (Georgescu 2022). This trend shapes international relations and global cooperation frameworks in this area (Ciupercă et al. 2022), stimulating the ambitions of confirming the normative power position in the field of the EU and the USA on the one hand and of China and Russia on the other. These powers seek to implement AI in a sustainable and safe way to maximize the positive impact on their own military, economic and strategic capabilities, but at the same time to ensure that their own and other actors do not generate unacceptable risks to critical infrastructures and digital systems which the functioning of the globalized world depends on. The new operational environment forces military leaders to understand the information relations specific to war through three dimensions, namely: the physical, the informational and the human. In this view, any military activity involves the organization of echelons and the coordinated conduct of their activities in the three directions determined by terms of time, space, and purpose. Thus, the combat power of a dominant operational component is applied to the other components of the combined force, coordination being achieved through unique requirements regarding the organization and conduct of combat.

The major challenge lies in the reality that anyone can use these technologies, adapting them quickly to be used safely and to counteract the effectiveness of previous versions. In this context, understanding the adversary's relative advantage requires understanding the capabilities of all actors involved, the adversary's purpose and objectives, the particularities of the operational environment for the geographical area where the conflict is taking place and, more than that, the influences and interdependent relationships of each domain and dimension. The large number of activities specific to armed conflict, from logistical support to direct combat, leads us to focus on the analysis of a set of challenges and circumstances essential for maintaining the security of forces in the context of increasing the lethality of weapons and combat systems. Of particular interest are the operational-

tactical decisions in direct confrontations, decisions developed with the support of disruptive technologies (AI). These are embodied in battle orders, in the design of courses of action and the choice of the optimal course, in the selection of offensive reaction measures in response to threats from the operational environment and the enemy, and in measures to coordinate efforts and achieve effective cooperation, with potentially lethal consequences.

In some armies, norms and recommendations are developed regarding the use of autonomous systems in combat. For example, regulations regarding the use of precision-guided munitions (fire-and-forget missiles) are designed with systems for monitoring target identification by a human operator, without the possibility of his intervention (DoD Directive 3000.09 2012).

The regulation of the development and use of AI by the armed forces is a complex matter, governed not only at the national level but also at the European level, at the alliance level or at the corporate level. In addition to the emerging national framework, the most important framework is the European one, which seeks to encourage ethical and trustworthy AI through specific legislation (European Commission 2021a), action plan (European Commission 2021b) and voluntary standards generated by High-Level Expert Groups (European Commission 2019) that broadly define no-risk applications, minimal-risk applications, high-risk applications and unacceptable-risk applications, each with different levels of regulation and different emphasis on self-regulation.

The two most important frameworks for a perspective on AI regulation for the armed forces are those created by the US Department of Defense (DoD 2019) and NATO (Stanley-Lockman and Christe 2021), which have a strong compatibility of vision, both being focused on several force principles: accountability, legality, fairness, explicability and traceability, governability, reliability. Here, we should also add voluntary frameworks created by companies in the AI industry or industries implementing AI. These frameworks can be more cost-effective by being specialized on the specific challenges of the respective industry. An example of this is the automotive industry, through the BMW AI governance framework (BMW Group 2020). However, we could also see voluntary frameworks in the arms industry because these companies will want to prevent the risk of overregulation by the state by demonstrating their own responsibility.

The lessons learned from contemporary warfare fully demonstrate that current military technology offers multiple opportunities, with advances in all fields of science establishing fewer and fewer barriers to limiting threats and violence against global peace. Revisionist and revanchist tendencies of some actors will inevitably trigger tensions that will be based on the performance of military technologies and the race to achieve relative balance in military efficiency. AI technology will probably

be the most important for delegating authority to combat systems/platforms, as well as for establishing the level of human control. Choosing the wrong direction in cyber diplomacy, even if it is represented by a set of promises and declarations of intent, will not be able to be blurred, with attenuated effects, without careful prior thinking, without identifying the optimal course from a multitude of scenarios.

In this sense, the analysis of AI technology in the context of multi-domain operations, followed by the identification of possible solutions to solve future challenges and the use of opportunities for beneficial purposes for human safety can bring added value to research and development in the field of military sciences.

Method – SWOT analysis

Based on the existing literature analysis, specific to the field of military sciences, we used the SWOT (Strengths, Weaknesses, Opportunities and Threats) method to better reflect the characteristics of AI in multi-domain operations. The purpose of this analysis is to identify the advantages of developing military applications based on AI, to distill the opportunities for implementing scientific advances in future military operations, as well as the current challenges for the target areas of the ratio of requirements for strengthening human security vs. economic and technological development. We believe that the results of this analysis will provide some guidelines to guarantee a positive change in the development and use of AI technology in support of the decision-making component for organizing and planning multi-domain operations.

As a result of the analyzed literature, we identify the following strengths, weaknesses, opportunities and threats that AI can bring to each area and direction established for multi-domain operations, presented in table no. 1.

Strengths

S.1 – *Automate decisions regarding speed and efficiency*: AI can quickly analyze information from a variety of sources such as: satellites, drones, individual sensors or implemented in combat equipment, etc., can search online scientific publications and propose solutions in the development of strategies or for the efficient coordination of operations that are carried out simultaneously in multiple domains. Autonomous systems, such as drones or land and naval robots, can be supported or even coordinated by AI to perform complex missions without direct human intervention. Sufficiently advanced AI systems can even systematize in real time information from human agents who verbally report changes on the battlefield.

S.2 – *Advanced data analysis capabilities*: AI algorithms can reduce human errors, provide solutions that are more accurate by analyzing large volumes of data and information, execute complex operations and learn to adapt to new situations. They

TABLE NO. 1

Implementing AI in Multidomain Military Operations: A SWOT Analysis

	FAVORABLE FACTORS FOR AI IMPLEMENTATION IN MULTIDOMAIN OPERATIONS	UNFAVORABLE FACTORS TO AI IMPLEMENTATION IN MULTI-DOMAIN OPERATIONS
INTERNAL SOURCE (ARMY)	*Strengths* *S1: Automate decisions for speed and efficiency* *S2: Advanced data analytics capabilities* *S3: Optimized resource consumption and logistics* *S4: Increased interoperability* *S5: Reduced risks to the human component* *S6: Increased precision and lethality to the adversary*	*Weaknesses* *W1: Technology dependency* *W2: High implementation and maintenance costs* *W3: Complexity of integration into current organic structures* *W4: Capital intensity* *W5: Errors in the decision-making process (programming, data interpretation, etc.) with serious consequences* *W6: Cascading compromise of military information systems* *W7: Cyber vulnerabilities*
EXTERNAL SOURCE	*Opportunities* *O1: Development and implementation of technologies* *O2: Integration of knowledge from several scientific fields* *O3: Inter-institutional and international collaboration and cooperation* *O4: Spin-offs and spin-ins as a way to compensate for increased costs*	*Threats* *T1: Use of AI for aggressive purposes* *T2: Ethical and legal challenges* *T3: The problem of human resources in the competition for high-performance AI* *T4: Amplification of the technological gap between national components of the joint forces* *T5: Dependence on the civilian economic environment for specific resources*

can also be used to create predictive models and simulations of operational scenarios, providing essential support for anticipating results and optimizing strategies.

S.3 – *Optimization of resource consumption and logistics*: AI can automate repetitive and complex processes, reducing execution time and the value of the effects of human errors. By analyzing operational requirements and their predictability, it can optimize field distribution, minimizing delays and risks associated with supply. In addition, AI facilitates communication and coordination between operational components involved in a multi-domain operation in real time, protecting critical infrastructure and sensitive information. The application of predictive AI models together with blockchain technologies allows for the secure and efficient management of intelligent, informational and energy networks, allowing for high precision and efficient exploitation of human resources, weapons and combat systems. Especially in multi-domain operations, this aspect represents the rapid and efficient management of resources within the framework of logistical support.

S.4 – *Increased interoperability*: AI technologies can contribute to increased interoperability between different multinational armed forces and host nation or international organizations. AI algorithms can optimize communication between units, even in conditions of great diversity and technological complexity.

S.5 – *Reduced risks to the human component*: Autonomous or semi-autonomous systems can take over risky tasks, increasing the overall security of the mission and the safety of human life. In addition, it can provide personalized experiences, increasing the level of training and training of the military while substantially reducing the physical risks of equipment destruction and injury to the military.

S.6 – *Precision and increased lethality among adversaries*: AI can contribute to increased precision of attacks, identifying targets with precision. Increased lethality can occur through the analysis and prediction of enemy behavior, by increasing autonomy and combat effectiveness, and by developing autonomous weapon systems. Of course, a number of ethical issues arise here that require clarification.

Weaknesses

W.1 – *Technology Dependence*: One of the main risks is related to the excessive dependence on AI that can lead to the loss of essential human critical thinking skills and new types of vulnerabilities, in case of technological and system failures. If an AI-based system were to be affected by a cyber-attack, the entire operational ecosystem could be compromised. On the other hand, resistance to change from decision-makers or operators who fear replacement or loss of their position in the function can represent a threat within the team intended to solve a mission.

W.2 – *High implementation and maintenance costs*: The development and implementation of advanced AI solutions requires considerable resources, both financial and human specialists. These costs include research, algorithm development, specialized infrastructure, specific acquisitions and specialized personnel training programs. In addition, the continuous maintenance and updating of systems to keep them at the highest performance standards is another critical economic factor.

W.3 – *Complexity of integration into current organizational structures*: Integrating AI technology into existing military echelon technologies can be a major challenge. This involves staff training and cognitive changes for operators to quickly adapt to new technologies and abandon traditional technologies and processes.

W.4 – *Capital intensity*: The increased technological capital needs of the defense industry necessary for multi-domain operations can represent a major vulnerability by limiting investments in military equipment as well as in communication systems, cyber warfare, AI, drones, satellites, etc., but also in training personnel to operate effectively in specific military domains. Thus, high operational costs and the risk of economic overload will aggravate economic instability and the capacity to conduct multi-domain operations. Another aspect concerns the lack of long-term sustainability. With the investment sector no longer being managed correctly, the maintenance of equipment and infrastructures will exceed maintenance plans, the collapse of financial and technological support capacities being a clear possibility.

W.5 – *Decision-making errors (programming, data interpretation, etc.) with serious consequences*: Although AI can improve the decision-making process, programming or data interpretation errors can lead to serious consequences. In multi-domain operations, where wrong decisions can lead to high loss of human lives or the escalation of conflicts, excessive dependence on AI without critical human supervision can represent a serious threat. A key issue in this context is the

phenomenon known as the "black box" of artificial intelligence, which refers to the difficulty humans face in understanding and auditing AI decision-making processes. This lack of transparency reduces accountability and limits the ability to optimize algorithms by correcting errors. The consequences of this situation are twofold: AI systems may be unjustifiably accepted, leading to unforeseen and potentially devastating effects, or they may be rejected, hindering competitiveness and widening technological gaps relative to adversaries.

W.6 – *Cascading compromise of military information systems* to affect not only the targeted system but also other components in the network (weapon systems, communications, weapon networks, etc.), with chain effects that endanger the entire operational capacity. Thus, if a domain control system is compromised, for example, a land forces cyber system, the capabilities of the air and naval components will also be affected, disrupting the synchronization and coordination of operations carried out in several directions.

W.7 -–*Cyber vulnerabilities*: AI technology is closely linked to the digital infrastructure and can become the target of cyber-attacks. In addition, the exploitation of programming errors or the admission of information controlled by the adversary during the machine learning process can lead to wrong decisions or mission failure and loss of trust in the technology. Vulnerabilities to cyber-attacks can be amplified by the complexity of communication networks and the large number of connection points of electronic devices in the networks used. Also, the architecture of AI systems can be opaque to military technical support personnel, meaning that the remediation of problems caused by an adversary or errors could only be done by the provider, introducing an additional element of complexity in the planning and conduct of operations.

Opportunities

O.1 – *Development and implementation of technologies*: Disruptive technologies and especially AI can be used to create innovative solutions in areas such as disaster management, crisis management and other multi-domain operations, where rapid coordination between entities of the various components of the combined forces is essential. Innovations in the field of natural language machine learning or digitalized visual observation can be new capabilities that improve operational efficiency.

O.2 – *Integrating knowledge from multiple scientific fields*: The use of AI algorithms allows the integration of knowledge from multiple fields, improving the process of knowledge discovery and decision-making. This approach leverages the strengths of AI technology specific to military applications to provide much more comprehensive information.

O.3 – *Inter-institutional and international collaboration and cooperation*: The use of AI can stimulate collaboration between various government entities and international

organizations, combining expertise from various professional and scientific fields, facilitating the exchange of information and the coordination of resources to resolve transnational events such as terrorism or cyber conflicts. In addition, AI can contribute to identifying solutions to complex global problems such as adapting to climate change or strengthening cyber defense.

O.4 – *Spin-offs and spin-ins as a way to offset increased costs*: The interaction between the civilian and military sectors facilitates the transfer of technology and resources to develop multi-domain operations and to support innovation in both domains. For example, the Internet, GPS and drones are military systems that have been transferred to the civilian sector and have a huge impact on the global economy. Specifically, spin-ins, AI and ML (machine learning), battery and energy storage technologies, autonomous vehicle technology, etc., are being adapted and integrated into the military sector to improve the performance and efficiency of military operations.

Threats

T.1 – *Use of AI for aggressive purposes*: In addition to using AI for defensive purposes, an adversary can also exploit it to increase the aggressiveness of attacks. For example, autonomous drones and cyber-attacks can be used to develop lethal weapons and undermine the defense and security of both operational and national security components. The paradigm of hybrid threats is also undergoing transformations because AI-based systems can implement cyber, physical or electronic attacks on critical infrastructures, as well as disinformation, manipulation and propaganda campaigns, with much lower costs and risks for the actor implementing them.

T.2 – *Ethical and legal challenges*: Responsibility in the use of autonomous weapons as well as the use of AI in autonomous decision-making applications, raises numerous ethical and legal issues. For example, there is no global regulation for establishing responsibility in the event of an error in an autonomous system. We consider the scenario in which an American drone, operated by AI, decided to attack anyone who tries to prevent it from carrying out its orders, including its own operator (Nețoiu 2023). In addition, the use of autonomous weapons may amplify concerns about possible human rights violations.

T.3 – *The problem of human resources in the competition for high-performance AI*: In the context of multi-domain operations, where technology plays an essential role in the success of missions, human resources become a critical factor in both the development and implementation of intelligent solutions and in increasing the shortage of professionals. These will generate significant delays in the development and implementation of innovative solutions, high costs of recruitment, training and retention of personnel, and difficulties in developing an organizational culture for public and military entities. Thus, the costs and resources necessary to ensure continuous professional training of civilian and military personnel will be much higher and will put additional pressure on the already affected budgets of the

institutions. These issues affect all armed forces around the world, regardless of resource abundance, as the relative gap between the private and military sectors remains significant in all countries.

T.4 – *Widening technology gaps between national components of joint forces*: The rapid pace of AI technology development in line with national economic opportunities can lead to technology gaps, which, at the level of national armed forces, establish different levels of readiness to face emerging challenges and threats. Thus, some nations may be vulnerable if they do not invest sufficiently in technological research and development to keep up with the rapid pace of development of disruptive and emerging technologies. A sharp technology gap limits the ability to cooperate with allies, including political and strategic consequences (Stanley-Lockman and Christe 2021).

T.5 – *Dependence on the civilian economy*: AI implementation is subject to increasingly stringent regulations, which can limit flexibility and increase compliance costs, which can erode the interest in their development by a private partner. Developers of AI solutions with military potential may be targeted by an adversary for sabotage, data theft or infiltration into systems to distort the functioning of AI systems or provide access to other military systems. Last but not least, the global economic model that emphasizes the mobility of capital has resulted in numerous instances in which critical entities in the development of technologies with dual potential have been taken over partially or entirely by an entity from a rival/adversary state, possibly also in coordination with the armed forces or intelligence services of that state (such as China's digital and electronic technology companies). Also, the dependence of military entities on critical civilian communications or energy networks can affect the conduct of a multi-domain operation by importing vulnerabilities specific to civilian infrastructures to physical and cyber-attacks by the enemy. In addition, if civilian economies are not sufficiently robust or resources are limited, they can generate difficulties in providing materials and logistical services, aspects that can lead to conflicts of priorities between civilian and military infrastructures. In the case of AI, military actors in countries with limited resources can end up depending on civilian suppliers not only for the development of specific AI solutions but also for computing capacity, data sets or other services under the Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) or Platform-as-a-Service (PaaS) paradigm. Last but not least, a global or regional economic crisis can affect both the civilian and military sectors, generated, in particular, by economic sanctions and trade blockades that will limit access to external resources.

Discussions on the interaction of the analyzed elements

Capitalizing on strengths and opportunities can counterbalance weaknesses and threats and create advantages for the development of divergent and disruptive technologies, through AI. Information created based on AI can quickly reform

multi-domain operations strategies as well as contribute to identifying opportune operational requirements for the development of combat means and platforms. The identified opportunities can eliminate threats (except T2).

The ethical and legal aspects that are included in T2 cannot be eliminated through AI development opportunities, which are related to the human factor. Thus, concurrently with these developments, a reconversion of the military career and professional specialties is necessary; therefore, university training programs must be adapted to the particularities of hybrid warfare, with an emphasis on innovative ways to identify solutions to deal with the listed threats, independently, at the level of each decision-making echelon.

In addition, based on the strengths, plans can be developed to develop new opportunities in industry and military education, with military bases becoming centers for the development of the regional economy (Topor 2024). To do this, mindsets must be changed, and initiatives regarding equipment, acquisitions and education must be prioritized based on impact studies according to the ultimate objective, namely maintaining national security and defending the population, resources and critical infrastructures.

Anyone using an internet search engine will be able to observe a paradox, namely that simultaneously with the evolution of revolutionary technologies such as AI and quantum computing, more and more malicious cyber actors are attacking critical infrastructures such as: communication and energy networks, banks and financial services, other critical infrastructures and even the citizens of a country. The purpose of these actions is to degrade the economic capacity of a state, to degrade the defense capacity, to limit or sabotage the production of critical goods and services including for the armed forces, but also to demoralize the population, to prove the attacker's power for psychological coercive purposes and to undermine the trust in authorities of citizens but also of partners, allies and investors. Moreover, it is recognized that a contemporary conflict is staged and takes place predominantly in the digital domain.

Under this approach, we appreciate that strategies based on the SWOT combination can transform and strengthen the security of multi-domain operations based on AI, maximizing their growth and stability by:

- Government support for investments in the development of companies that produce electronic chips and conductors, as well as for those that develop critical AI infrastructure. They can be achieved through strategic approaches to trade and import/export policies that help Romanian companies develop and create data centers and digital platforms whose services could be exported worldwide;
- Government support for the effective governance of the development of ethical and trustworthy AI systems by ensuring reliability, transparency, accountability and other attributes of safe AI systems enshrined in the European and NATO frameworks. An important role is played by the state's

involvement in ensuring secure sources of relevant data for training AI models. Poisoning of datasets for AI models is one of the most insidious new cyber threats, and safe and trustworthy datasets have become a critical national resource to identify, protect and capitalize on (Sambucci and Paraschiv 2024);
- Development of competent leadership, especially in the procurement and technology implementation sectors. AI generates effective solutions, but without the critical thinking of human leadership, gains in efficiency, costs, and security will not be maximum. All national communities, including the military and intelligence, must streamline their procurement services, modernizing based on AI, cloud and revolutionary technologies, whose exploitation period is relatively very short, due to their constant renewal. Hence the need to outsource such services, which through blockchain technology can ensure a high level of information security;
- Development and multiplication of public-private collaborations in the field of cyber defense. The expansion of identified threats to other areas, not only that of military operations, will affect governmental and economic relations of the spin-ins type, with rapid effects on the combat power of all military components involved. In this regard, strengthening the existing effort to institutionalize operational collaboration will allow private sector agencies and companies to act more quickly to respond to incidents and to support national institutions in blocking cyberattacks. In addition, international institutional collaboration relationships in the field of cyber defense can be formed and strengthened. This way, good practices can be exchanged and popularized, collaborative procedures can be established to discover vulnerabilities in software, and safe and secure models can be built that are constantly adapted to new AI security challenges.

Even though AI is and will remain a subject and goal of interstate competition for a long time to come, it must be accepted that it also represents a huge potential in the field of economic and military development. This strategy can materialize in operational plans that transform inter-institutional cooperation into directions for the development of AI technologies in order to establish safe and sustainable adoption models. Thus, the transatlantic dialogue and cooperation between the US and the EU is to occupy one of the most important roles in the face of China's tendencies, and implicitly other countries, to gain hegemonic positions in the AI competition to determine future superpowers.

Conclusions

Artificial intelligence is an emerging digital technology with systemic impact, which can also have a transformative effect on multidomain operations. Within these operations, AI-based systems can perform data collection and analysis roles, support decision-making, facilitate communication and interoperability between actors

and systems, and occupy concrete functions in the order of battle, such as logistics and maintenance optimization roles, cyber attacker and defender roles, but also autonomous systems operation roles. In a military context, all these functions bring significant benefits. In the context of multi-domain operations, in the five domains identified by NATO (air, water, land, space and cyber), the role of AI will be vital to ensure the congruence, coordination, effectiveness and flexibility of the forces engaged in such operations. In this article, a SWOT analysis was conducted on the field of AI in the military context, which resulted in a series of recommendations for the Romanian authorities. The existing framework for cross-border cooperation in the military field on the regulation of the ethical and responsible use of AI was also analyzed based on the risks of corruption by adversaries or the malfunction of these complex and difficult-to-repair systems. We believe that further research can lead us to concrete standards for the implementation of AI in military systems, including weapons systems, that are compatible with the NATO and European frameworks, and that ensure not only the necessary capabilities for the armed forces in multi-domain operations, but also a leveling factor against a potential adversary with more numerous military resources.

References

BMW Group. 2020. *BMW Group Code of Ethics on AI.* https://www.bmwgroup.com/content/dam/grpw/websites/bmwgroup_com/downloads/ENG_PR_CodeOfEthicsForAI_Short.pdf.

Ciupercă, E.M., C.E. Cîrnu, A. Stanciu, and I. Cristescu. 2022. "Leveraging socio-cultural dimension in cyber security training." *EDULEARN22 Proceedings.* ISBN: 978-84-09-42484-9, ISSN: 2340-1117. pp. 5242-5248. doi:10.21125/edulearn.2022.1239.

DoD. 2019. "AI Principles: Recommendations on the Ethical Use of Artificial Intelligence." Defense Innovation Board, USA. https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF.

DoD Directive 3000.09. 2012. "Autonomy in Weapon Systems." U.S. Department of Defence. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.

European Commission. 2021a. "COM (2021) 206 final Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

European Commission. 2021b. "Coordinated Plan on Artificial Intelligence 2021 Review." ANNEXES to COM(2021) 205 – 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 - Fostering a European approach to Artificial Intelligence. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A205%3AFIN.

—. 2019. *Ethics guidelines for trustworthy AI. High-Level Expert Group on AI.* https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

Final Report. 2025. National Security Commission on Artificial Intelligence, p. 20. https://assets.foleon.com/eu-central-1/de-uploads-7e3kk3/48187/nscai_full_report_digital.04d6b124173c.pdf.

FM3-0. 2022. "Operations." Headquarters, Department of the Army. https://irp.fas.org/doddir/army/fm3-0.pdf.

Georgescu, A. 2022. "Cyber Diplomacy in the Governance of Emerging AI Technologies – A Transatlantic example." *International Journal of Cyber Diplomacy,* (ISSN 2668-8662) vol. 3: pp. 13-22. https://doi.org/10.54852/ijcd.v3y202202.

Nețoiu, R. 2023. "Noile drone controlate de inteligența artificială îi omoară chiar și pe operatorii lor. Scenariul Terminator de care se teme armata SUA." *Digi24.ro.* https://www.digi24.ro/stiri/externe/noile-drone-controlate-de-inteligenta-artificiala-ii-omoara-chiar-si-pe-operatorii-lor-scenariul-terminator-de-care-se-teme-armata-sua-2372223.

Sambucci, L., and E.A. Paraschiv. 2024. "The accelerated integration of artificial intelligence systems and its potential to expand the vulnerability of the critical infrastructure." *Romanian Journal of Information Technology and Automatic Control* (ISSN 1220-1758) 34 (3): 131-148. https://doi.org/10.33436/v34i3y202410.

Schmidt, E. (coord.). 2021. "Final Report - National Security Commission on Artificial Intelligence." NSCAI, Washington DC, US. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

Stanley-Lockman, Z., and E.H. Christe. 2021. "Summary of the NATO Artificial Intelligence Strategy." *NATO Review.* https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html.

Topor, S. 2024. "The Contribution of Military Research and Development (R&D) to the Developent of the Regional Economy." *Romanian Cyber Security Journal* (ISSN 2668-6430) 6 (2): 85-93. https://doi.org/10.54851/v6i2y202408.

Vevera, A.V., and E.M. Ciupercă. 2019. "The dimensions of CYBER WARFARE in the sino-russian space." *Romanian Cyber Security Journal* 1 (2): 31-36. https://rocys.ici.ro/documents/57/2019_fall_article_3.pdf.

Xinhua. 2024. "China accelerates AI development to build AI innovation center." *English.gov.cn., The State Council, The People's Republic of China.* https://english.www.gov.cn/news/202404/06/content_WS6610834dc6d0868f4e8e5c57.html.