



AGNIESZKA ROGOZINSKA

War Studies University,

Academy of Piotrkow, Poland

ORCID iD: 0000-0002-3462-7851

ARTIFICIAL INTELLIGENCE IN MULTI-DOMAIN OPERATIONS: APPLICATIONS, LIMITATIONS AND GOVERNANCE CHALLENGES – A CRITICAL REVIEW

ABSTRACT

The purpose of this article is to critically examine the use of artificial intelligence (AI) in supporting the planning, coordination and execution of multi-domain operations. It considers the applicability of systemic and functional approaches and qualitative methods to the analysis of AI-enabled military capabilities. A critical review of literature, doctrinal and conceptual documents, institutional materials and selected case studies was conducted. The reviewed evidence indicates that AI can support operational planning, information processing, decision support and selected forms of coordination across land, air, sea, space and cyberspace. At the same time, the evidence varies in maturity: some applications are conceptual or experimental, whereas others represent more established operational capabilities. The review also identifies technological, organizational, cybersecurity, interoperability, legal and doctrinal constraints that condition the practical utility of AI in multi-domain operations.

KEYWORDS: artificial intelligence, multi-domain operations, interoperability, security, autonomous systems

STRESZCZENIE

Celem niniejszego artykułu jest krytyczna analiza wykorzystania sztucznej inteligencji (AI) we wspieraniu planowania, koordynacji i realizacji operacji wielodomenowych. Analizie poddano zastosowanie podejścia systemowego i funkcjonalnego oraz jakościowych metod badawczych. Przeprowadzono krytyczny przegląd literatury, dokumentów doktrynalnych i koncepcyjnych, materiałów instytucjonalnych oraz wybranych studiów przypadku. Zebrany materiał wskazuje, że AI może wspierać planowanie operacyjne, przetwarzanie informacji, wspomaganie decyzji oraz wybrane formy koordynacji działań na lądzie, w powietrzu, na morzu, w kosmosie i cyberprzestrzeni. Jednocześnie stopień dojrzałości analizowanych rozwiązań jest zróżnicowany: część zastosowań ma charakter koncepcyjny lub eksperymentalny, podczas gdy inne reprezentują bardziej ugruntowane zdolności operacyjne. Przegląd wskazuje również na ograniczenia technologiczne, organizacyjne, cyberbezpieczeństwa, interoperacyjności, prawne i doktrynalne warunkujące praktyczną użyteczność AI w operacjach wielodomenowych.

SŁOWA KLUCZOWE: sztuczna inteligencja, operacje wielodomenowe, interoperacyjność, bezpieczeństwo, systemy autonomiczne

INTRODUCTION

Despite the growing reliance on AI in command systems, its actual impact on decision-making effectiveness in multi-domain operations remains contested, particularly under conditions of high operational complexity and uncertainty. Rapid advancements in information technology, including AI and the changing demands of modern military conflicts require military operations to be transformed into multi-domain operations. This transformation involves the integration of land, air, sea, space and cyber domains to achieve operational and strategic superiority.

The success of such operations largely depends on the command's ability to process vast amounts of data in real time and make rapid decisions. AI is essential in this context as a tool supporting command systems, rather than as an independent element of operational structures. Traditional hierarchical command models are increasingly inadequate in addressing information overload, leading to inefficiencies in decision-making and, in extreme cases, the degradation of command effectiveness.

AI systems can analyze data from multiple sources, identifying patterns and predicting enemy actions through algorithms designed to enhance operational effectiveness. This capability improves efficiency and reduces overall command response times. As a result, AI-based communication and decision-making are becoming increasingly powerful and automated. In this context, AI is becoming an integral feature across operational domains through parallel operational planning, risk analysis and coordination among land, air, maritime and cyber assets of the battlefield. At the same time, AI implementation is riddled with many obstacles. The most challenging include doctrinal limitations, interoperability of warfighter systems, legal concerns of autonomous combat systems and data security. Absence of uniform standards and regulation affects the ability to fully integrate AI and limits the operational effectiveness and applicability of AI. In order to be employed in dynamic and complex conflicts to meet the needs of an era of complex warfare, systems employing AI need to ensure continuous updating of operational procedures, training personnel and testing new models in real-world operational conditions.

AI in multi-domain operations is also vital because a large volume of information from sensors, drones, satellites, cyber systems and other sources must be processed in real time. The challenges associated with implementing AI in multi-domain environments are substantial. An integrated doctrinal, legal and technical framework developed by the military, including system interoperability and procedures for integrating autonomous combat systems into traditional command systems is a necessity. AI also requires a responsive strategy for optimal execution and fast response to a dynamically changing battlefield environment. Preliminary research indicates that the cognitive gap between technical development and institutions' readiness to adopt it limits the utility of AI in multi-domain operations.

This article assumes that multi-domain operations can be considered one of the main contemporary methods of conducting military operations. It is based on combining various operational domains and building advantage through the effective use of information and efficient decision-making. The literature emphasizes that the outcome of future conflicts will be determined not only by combat assets but also by the ability to influence the enemy's mindset and cognitive superiority.

As a result of the defined problem situation and identified cognitive gap, the main research problem was formulated as follows: Does AI support planning, coordination and selected activities of multi-domain operations? Three sub-problems were specified: 1. How do AI solutions support the planning process of multi-domain operations within command structures? 2. What role does AI play in the coordination and synchronization of activities conducted simultaneously across different operational domains? 3. What technological, organizational, legal, doctrinal and interoperability barriers condition the implementation and practical utility of AI in multi-domain operations?

This research examines the use of AI as a tool for enhancing both information processing and decision-making capabilities within command and control systems. The aim of this article is to examine the role of AI in multi-domain operations as a means of supporting decision-making and information processes, as well as to explore the relationship between AI and the effectiveness of information processing and decision-making.

The research hypothesis states that AI can improve information processing and decision support in multi-domain operations, but the practical utility of these capabilities depends on data quality, system interoperability, cybersecurity, appropriate human judgment, the legal and doctrinal conditions governing their use.

RESEARCH METHODS

The research process was based on the assumption that contemporary multi-domain operations require significant transformations in planning, coordination and execution because of increasing operational complexity and the growth of data generated by intelligence and command systems. AI was treated primarily as a decision-support and information-processing capability embedded in existing command-and-control structures rather than as an independent substitute for command authority.

A systems approach was adopted to analyze interactions between command-system components, information flows and AI-based decision-support tools. This was complemented by a functional approach, enabling assessment of AI across the stages of operational planning, coordination, synchronization and execution. Qualitative reasoning was used to compare capabilities, limitations and governance conditions across operational domains.

The study employed qualitative research methods, including a critical literature review, analysis of doctrinal and conceptual documents, institutional and policy materials and selected case studies of AI-related military applications. Sources were selected purposively according to their relevance to AI-enabled planning, command, control, information processing, autonomous, unmanned systems, interoperability, cybersecurity and legal or governance questions. Priority was given to peer-reviewed academic publications, official governmental and international-organization documents, recognized research institutions and documented military or industrial cases. Examples were included where they illustrated a specific capability, experiment, operational use, or governance problem rather than merely a general reference to AI. The review covered materials published primarily between 2010 and 2025, supplemented by earlier foundational material where necessary. The synthesis was thematic: findings

were grouped into planning, coordination and synchronization, implementation barriers and were then compared across operational domains. The study is not intended as a formal systematic review; therefore, no exhaustive database protocol or meta-analysis was applied. Conclusions were drawn using abstraction, generalization, inductive, deductive reasoning to maintain consistency between the research problem, methods, evidence and findings.

AI SOLUTIONS AS A SUPPORTING ELEMENT FOR MULTI-DOMAIN OPERATIONS PLANNING IN COMMAND STRUCTURES

AI systems are gaining increasing importance in the planning and execution of multi-domain operations, thanks to their ability to rapidly process information, analyze massive data sets and make real-time decisions. Due to their complexity and the need to integrate activities across land, sea, air, space, cyber and information environments, multi-domain operations require new management and coordination tools (Szczygielska et al., 2024, p. 17-18). In the operational planning process, AI is used to integrate data from a variety of sensors—from unmanned aerial systems and observation satellites to open and cyber sources (Kopeć et al., 2021, p. 26). Deep learning techniques enable filtering information noise, identifying significant patterns of enemy behavior and predicting their potential actions. An example of AI-supported military decision-making is the Israeli Fire Factory system. Publicly available sources indicate that the system uses data concerning previously approved targets to calculate ammunition requirements, prioritize, assign targets to aircraft, unmanned systems and propose strike schedules. The system should therefore be understood as a decision-support and planning tool rather than as an autonomous system independently conducting the entire targeting process (Newman, 2023). AI systems enable advanced predictive analyses that support the creation of operational scenarios and the assessment of the effects of various action options. Forecasting models based on real, simulated data enable optimal deployment of forces, resource allocation in time and space. An example is the experimentation conducted as part of the Project Convergence program by the U.S. Army Futures Command, where AI analyzes data from

multiple sensors and proposes the most effective military action options, taking into account current troop locations, enemy resources and anticipated responses (U.S. Department of Defense, 2025).

Optimization algorithms analyze thousands of possible action combinations in fractions of a second, recommending to commanders the most effective options in line with operational objectives. An example of such a solution is the Loyal Wingman (MQ-28 Ghost Bat), developed by Boeing in collaboration with the Royal Australian Air Force. This autonomous combat drone, designed to support manned aircraft, conduct reconnaissance, disrupt enemy systems and deliver weapons, also relies on AI systems. In these systems, AI not only analyzes the operational situation but also identifies targets, assesses their priority and selects the most appropriate means of engagement. In highly dynamic environments where human reaction times are excessive, AI can also take partial control of task execution (Boeing, 2026).

In military logistics, AI offers the ability to dynamically manage supply chains and predict resource requirements. Analysis of weather, topographic, operational data enables optimal planning of supply routes, the location of logistics points and the identification of risks related to supply disruptions (Krzewniak et al., 2024, p. 118-119).

In cyberspace, AI can support defensive functions such as anomaly detection, identification of suspicious network activity and automated or semi-automated responses to detected threats. Commercial cybersecurity platforms such as Darktrace illustrate the application of machine-learning techniques to network monitoring and threat detection. These examples should not, however, be interpreted as evidence that the same systems provide offensive cyber capabilities (Darktrace, 2021). An example of experimental AI application in the intelligence domain is Project SABLE SPEAR, a multi-year effort examining the application of artificial intelligence to intelligence analysis and the processing of open-source information. The project illustrates the potential of AI to support the discovery and analysis of information, while also highlighting organizational, technical, human and policy requirements for its effective implementation (Dudley, 2021, p. 7-14).

In air and space, AI supports air traffic management, satellite trajectory analysis, mission planning for unmanned aircraft and selected forms of orbital monitoring.

Systems and programmes discussed in public sources illustrate the use of automated data processing for object detection, tracking and mission support. The Athena example should be understood here as the Athena Simulation used within the Strategic Multilayer Assessment study rather than as an autonomous AI sensor-fusion system. A more appropriate example is the Athena Simulation used in a U.S. Air Force Strategic Multilayer Assessment study to examine information and influence in operational-level planning and assessment (Strategic Multilayer Assessment, 2021). Accordingly, Athena is treated here as a simulation and analytical framework rather than as an AI sensor-fusion system. Current U.S. defense programmes also illustrate the broader development of AI-enabled sensing and data processing, but their capabilities should be distinguished from fully autonomous decision-making systems.

AI can support dynamic decision-making by processing information across the battlespace and assisting commanders in developing and assessing courses of action. The U.S. Department of Defense identifies automation, artificial intelligence, predictive analytics and machine learning as elements supporting JADC2's ability to sense, make sense of and act on information across the battlespace (U.S. Department of Defense, 2022). The concept of digital twins is also increasingly being used, allowing the simulation of the effects of operational decisions before they are implemented (Javaid et al., 2023, p. 71-92).

In summary, the reviewed evidence indicates that AI algorithms can support predictive analysis, operational planning and the processing of large amounts of information. The literature also identifies potential benefits for decision support, logistics, cybersecurity, air and space information management. These findings should be interpreted cautiously because the evidence combines conceptual proposals, experiments, demonstrations and documented applications with different levels of operational maturity.

Table 1. *AI Applications in Multi-Domain Operations: Functions, Evidence Maturity, Operational Relevance and Limitations*

Operational domain/ function	AI-enabled application	Illustrative examples/ programmes	Evidence maturity	Potential operational contribution	Principal limitations/ risks
Planning and C2	Data fusion, predictive analysis, decision support.	Project Convergence; JADC2.	Experimental / demonstrative.	Faster processing of distributed information and generation of action options.	Data quality, model uncertainty, explainability, human reliance.
Land - ISR and C2	Analysis of reconnaissance data, geospatial information and tactical information.	MAARS; AI-supported C2 applications.	Documented platform capabilities; AI integration context-dependent.	Enhanced situational awareness and support to manoeuvre planning.	Sensor errors, data manipulation, operator dependence, limited autonomy.
Air	Mission planning, object detection, UAV coordination and autonomous mission support.	Project Maven; Skyborg; XQ-58A.	Experimental / demonstrative.	Faster analysis and support to dynamic mission management and human-machine teaming.	False positives, signal interference, autonomy-management challenges.
Cyber	Anomaly detection, threat identification and automated response.	Darktrace; AI-supported cyber-defence applications.	Documented capability.	Potentially faster detection and response to cyber threats.	Adversarial manipulation, data poisoning, attacks on AI infrastructure.
Space/ISR	Automated processing, classification and analysis of satellite-derived information.	Satellite imagery analysis; AI-supported ISR applications.	Experimental / documented analytical applications.	Faster processing of large volumes of imagery and support for situational awareness.	Misclassification, incomplete or biased training data, adversarial manipulation.
Multi-domain coordination	Cross-domain data fusion and near-real-time coordination.	CJADC2; Project Convergence.	Experimental / demonstrative.	Potentially improved information coherence and synchronization across domains.	Interoperability, communications resilience, dependence on data architecture.
Autonomy/ weapons governance	Target recognition, autonomous functions and human-machine teaming.	Harpy; Kargu-2; autonomous weapons literature.	Operationally fielded / debated; degree of autonomy varies.	Reduced response time in selected functions and new human-machine teaming options.	IHL compliance, accountability, predictability and human control.

Source: U.S. Department of Defense (2017, 2022, 2025), NATO (2021), QinetiQ (2026), AFRL (2023), Wieliczko (2024), Scharre (2018), Ertan et al. (2020), ICRC (2014), UNODA (2024), Willbold et al. (2024).

THE IMPORTANCE OF AI IN COORDINATING AND SYNCHRONIZING MULTI-DOMAIN OPERATIONS

The contemporary operational environment is characterized by unprecedented complexity and the interpenetration of operations across multiple strategic domains. The concept of multi-domain operations captures the essence of the modern battlefield, which encompasses not only traditional land, air, sea environments but also space and the cyber domain. Integrating these domains requires not only advanced command systems but also the ability to collect, process and utilize vast amounts of data in real time. AI components and algorithms are becoming a key tool for effectively coordinating operational activities across these domains. In the context of multi-domain operations, AI not only facilitates target recognition and identification but also integrates information from different domains, enabling commanders to achieve full situational awareness and conduct coordinated actions in real time. An example is the Project Maven system developed by the US Department of Defense, which uses machine learning algorithms to analyze drone video footage, enabling automatic object detection and threat classification in real time (U.S. Department of Defense, 2017).

In the land domain, AI can support command-and-control processes through analysis of reconnaissance imagery, geospatial data, tactical reports, helping to assess threats and develop movement or response options. Autonomous and unmanned ground systems can also provide reconnaissance, surveillance and target-acquisition functions. MAARS, for example, is an unmanned ground vehicle designed for reconnaissance, surveillance and target acquisition; its public documentation emphasizes operator control and safety features rather than autonomous AI-based engagement. It should therefore not be presented as evidence of an AI-enabled autonomous combat system. AI applications are better understood here as part of the wider command, intelligence and data-processing architecture in which such platforms may operate (QinetiQ, 2026).

The airspace is an exceptionally fast-paced operational environment, making AI support particularly valuable. AI algorithms are used to plan air missions, analyze airspace and manage fleets of unmanned aerial vehicles. An example of this is the Skyborg program, implemented by the US Air Force,

which develops autonomous combat drones, such as the XQ-58A Valkyrie, that work alongside fifth-generation fighters (AFRL, 2023). These systems analyze meteorological data, radar signals and information from early warning systems, enabling dynamic adjustments to flight paths and predicting the presence of threats.

BARRIERS AND CONDITIONS FOR AI IMPLEMENTATION IN MULTI-DOMAIN OPERATIONS

The third sub-problem concerns the conditions under which AI can be implemented and used with practical utility in multi-domain operations. The reviewed material indicates that technological capability alone is insufficient. Implementation depends on the quality and provenance of data, resilience to adversarial manipulation, secure communications and computing infrastructure, interoperability among systems, personnel competence, appropriate human-machine interaction, compatible doctrinal, legal, procurement and organizational arrangements.

AI is an increasingly important technological capability in the transformation of modern armed forces, particularly in multi-domain operations. However, the available evidence does not justify treating AI as inherently decisive. Its contribution depends on the specific task, data environment, system architecture, level of human oversight and organizational context. Implementing AI-based solutions in complex operational environments therefore involves technological limitations, security threats and systemic and organizational barriers, with implications for operational effectiveness, safety, ethics and compliance with international law.

One of the fundamental technological limitations is the quality of the data used by AI algorithms. Most machine learning-based solutions require large sets of training data, which in military settings are often incomplete, inconsistent, disrupted, or deliberately falsified by enemy actions. An example is the use of satellite reconnaissance systems, in which AI algorithms misclassify terrain objects – for example, camouflaged military installations can be recognized as elements of civilian infrastructure, leading to erroneous operational decisions (Willbold et al., 2024, p. 5-6). Another example is the situation in which radar

analysis systems in the air domain, using AI algorithms, misclassify reflections of signals distorted by atmospheric conditions as enemy airborne objects, leading to false alarms and excessive operator workload (Awan et al., 2023).

During the Russian-Ukrainian war, a surge in GPS spoofing attacks targeting drones was observed, which is consistent with the broader trend of using electronic warfare on the modern battlefield (Jhanjhi et al., 2025, p. 1-17). Such activities can directly impact AI algorithms, especially when they rely on multi-source sensory data. A lack of universal solutions capable of adapting to a dynamic, unpredictable operational environment limits their usefulness in real-world combat situations. Adversarial attacks pose an additional threat, involving subtle manipulation of input data (e.g., images or messages), which can lead to misclassification – for example, a civilian vehicle could be recognized as a military target. This phenomenon is particularly significant in autonomous systems, such as combat drones or anti-aircraft systems, where reaction time is limited and machine decisions must be made instantaneously. Implementing AI in a multi-domain environment also poses significant cybersecurity threats. The infrastructure supporting AI – communications systems, data centers and cloud computing-becomes a natural target for adversary attacks. In 2020, research by the NATO Cooperative Cyber Defense Centre of Excellence indicated that autonomous air traffic control systems can be used as attack vectors against military infrastructure if they are not adequately isolated and protected (Ertan et al., 2020, p. 128-129). Disrupting the information chain or infecting the algorithm with malicious code can result in operational paralysis of the entire group.

Additionally, the adversary may use disinformation, impersonate data sources, or create false radio signals and satellite images. AI-enabled synthetic media, including deepfakes, creates an additional risk for military information environments because manipulated audio-visual content can undermine the reliability of information used for situational assessment and decision-making (Mirsky et al., 2021, p. 1-38). At the organizational level, interoperability is a problem. AI systems developed by different countries (e.g., the USA, France, Germany), armed forces (air force, navy, land forces) and industrial suppliers (e.g., Thales, Raytheon, Leonardo) may be based on different architectures, protocols data exchange principles.

Standardization and interoperability efforts within NATO are supported by initiatives such as Federated Mission Networking, which provides a framework for information sharing and interoperability among NATO, national and partner forces. NATO's broader digital-transformation efforts also address secure, resilient and interoperable digital capabilities, including data and AI-enabled capabilities. However, the interoperability of AI-enabled systems remains dependent on common standards, data architectures, secure communications, testing and certification (NATO, 2023). There is a lack of common interfaces, certification policies and a uniform approach to operational data management.

The legal and governance dimension requires a distinction between the absence of a dedicated comprehensive treaty specifically regulating lethal autonomous weapons systems and the applicability of existing international law. Existing international humanitarian law applies to the development and use of weapons, including autonomous functions and imposes requirements such as distinction, proportionality, precautions in attack and applicable weapons-review obligations. The unresolved issue is therefore not a complete legal vacuum, but how existing rules should be interpreted and operationalized for increasingly autonomous systems and whether additional specific measures are necessary. Questions of responsibility and accountability remain significant, particularly where system behavior is difficult to predict or explain. Cultural and institutional barriers also emerge in military structures, including concerns about appropriate trust in automated recommendations and the need for personnel capable of understanding system capabilities and limitations (Scharre, 2018, p. 251-252).

Full AI implementation therefore requires not only infrastructure modernization but also doctrinal, educational, legal and organizational adaptation. The development of autonomous weapons remains controversial. The international debate on lethal autonomous weapons systems has continued within the Convention on Certain Conventional Weapons. The Group of Governmental Experts on emerging technologies in the area of lethal autonomous weapons systems continued its work in 2024 and 2025 and further sessions were scheduled for 2026. The continuation of this process demonstrates that international discussions concerning the regulation of autonomous weapons remain ongoing rather than concluded (UNODA, 2026). The process demonstrates continuing disagreement about the appropriate

form and scope of future regulation rather than a termination of negotiations. The International Committee of the Red Cross has advocated stronger international measures concerning autonomous weapons, while states continue to discuss the applicability of existing IHL and possible additional rules. Examples such as Harpy and Kargu-2 are relevant to the debate on autonomy and human control, but public sources do not by themselves justify treating every such system or deployment as equivalent to a fully autonomous LAWS capability. The governance challenge therefore concerns both compliance with existing law and the possible development of additional international norms.

One important direction of development is explainable and otherwise transparent AI, which may help commanders and operators understand and critically assess algorithmic recommendations (Arrieta, 2020, p. 82-115). Such approaches can contribute to transparency and calibrated trust, but explainability alone does not guarantee reliable or lawful operational use. Interoperability standards, secure data architectures, testing, evaluation, training and certification are likewise important conditions for responsible deployment.

In summary, the reviewed material indicates that AI may provide meaningful support for selected multi-domain functions, but its practical value is conditional. Key limitations include the quality and provenance of training data, vulnerability to manipulation, limited adaptability in dynamic combat environments, cyber risks, interoperability problems and uncertainty concerning human-machine responsibility. The evidence also differs in maturity: conceptual models, experiments, demonstrations and operationally deployed capabilities should not be treated as equivalent. Accordingly, responsible implementation requires technological testing and assurance together with doctrinal, organizational, legal and educational measures.

LIMITATIONS OF THE STUDY

The study has several limitations. First, detailed operational data concerning military AI systems are often classified or otherwise unavailable, which limits independent verification of performance, reliability and actual deployment. Second, the analysis relies substantially on publicly available academic, governmental, institutional, industry sources, whose level of detail and

evidentiary status varies. Third, the review combines conceptual proposals, experiments, demonstrations and documented operational applications; these categories cannot be treated as equivalent evidence of effectiveness. Finally, rapidly changing technologies and doctrines mean that specific system descriptions and governance arrangements may become outdated. The findings should therefore be interpreted as a critical synthesis of publicly accessible evidence rather than as an assessment based on comprehensive operational datasets.

CONCLUSIONS

Based on the critical review conducted, AI can be regarded as a significant decision-support and information-processing capability for selected functions of multi-domain operations. The reviewed evidence indicates potential improvements in information processing, information coherence, response time, but the strength of evidence varies across applications and levels of operational maturity.

Regarding the first sub-problem, the review indicates that AI can integrate data from distributed sources, support situational modelling, analyze imagery, signals and generate predictive assessments or action options. These capabilities may streamline operational planning under conditions of information overload. The available evidence, however, does not support a general conclusion that AI necessarily increases the accuracy or effectiveness of command decisions in all operational contexts.

Regarding the second sub-problem, AI can support coordination and synchronization across operational domains by processing heterogeneous information and assisting selected activities involving ground forces, unmanned aircraft, space-related monitoring and cyber operations. The contribution is potentially valuable where information must be processed rapidly, but it remains dependent on communications, data quality, interoperability and human supervision.

Regarding the third sub-problem, the review identified conditions and barriers that constrain implementation and practical utility. These include data quality and availability, adversarial manipulation, limited transparency and explainability, interoperability problems, cybersecurity risks, shortages

of relevant expertise and the need for coherent legal, doctrinal, procurement and organizational arrangements. These factors may limit the transfer of experimental or demonstrated capabilities into reliable operational use.

The findings provide qualified support for the research hypothesis. They indicate that AI can improve information processing and support decision-making in selected multi-domain functions, while its practical utility depends on data quality, interoperability, cybersecurity, human judgment, legal and doctrinal conditions. The review therefore does not establish unconditional effectiveness of AI in multi-domain operations. Future research should focus on: first, transparent, resilient and testable AI models for uncertain environments; second, interoperability and assurance standards for allied operations; third, legal, ethical governance of autonomy, including responsibility and human control in systems with critical functions.

REFERENCES

- Air Force Research Laboratory. (2023). *AFRL artificial intelligence agents successfully pilot XQ-58A Valkyrie uncrewed jet aircraft*, from <https://www.afrl.af.mil/News/Article-Display/Article/3480404/afrl-artificial-intelligence-agents-successfully-pilot-xq-58a-valkyrie-uncrewed/>
- Arrieta, A. B., et al. (2020). *Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI*. Information Fusion, 58, 82-115.
- Awan, M. Z., Jadoon, K. K., Masood, A. (2023). *Scalable and effective artificial intelligence for multivariate radar environment*. Engineering Applications of Artificial Intelligence, 125, 106680.
- Boeing. (2026). *MQ-28 Ghost Bat*, from <https://www.boeing.com/defense/autonomous-and-unmanned-systems/mq-28-ghost-bat>
- Darktrace Immune System Self-Learning Detection & Response, 8 September 2021, from <https://www.infosecurity-magazine.com/white-papers/prm/darktrace-selflearning-detection/>
- Dudley, C. A. (2021). *Lessons from SABLE SPEAR: The Application of an Artificial Intelligence Methodology in the Business of Intelligence*, 65, 1, 7-14. Studies in Intelligence.
- Ertan, A., Floyd, K., Pernik, P., Stevens, T. (eds.). (2020). *Cyber threats and NATO 2030: Horizon scanning and analysis*. NATO Cooperative Cyber Defence Centre of Excellence.
- International Committee of the Red Cross (ICRC) (2014). *Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects*.
- Javaid, M., Haleem, A., Suman, R. (2023). *Digital Twin applications toward Industry 4.0: A Review*, 3, 71-92. Cognitive Robotics.
- Jhanjhi, N. U. A., Khan, F. S., Ibrahim, M., Rasyid, H. A. B. A. (2025). *The Rise of GPS Spoofing Attacks on Drones in the Russia-Ukraine War*, 1-17. TechRxiv.
- Kopeć R., Wasiuta O., Wójtowicz T. (2021). *Wojna dronów. Militarne wykorzystanie bezzałogowych statków powietrznych*. Wydawnictwo Naukowe UP.
- Krzewniak, D., Moch, N., Sikorski, J., & Wawer, R. (2024). *Nowe technologie jako instrument realizacji polityki bezpieczeństwa informacyjnego: Prolegomena*. Uniwersytet w Siedlcach.
- Mirsky, Y., Wenke, L. (2021). *The Creation and Detection of Deepfakes: A Survey*, 1, 1, 1-38. ACM Computing Surveys.
- NATO (2021). *NATO Artificial Intelligence Strategy*. NATO.
- NATO Allied Command Transformation. (2023). *Federated Mission Networking [Fact sheet]*. NATO.
- Newman, M. (2023). *Israel quietly embeds AI systems to select targets in deadly military operations*. Bloomberg.

- QinetiQ. (2026). *MAARS weaponized robot*. QinetiQ, from <https://www.qinetiq.com/en-au/what-we-do/research-and-development/autonomous-systems/robotics/robotic-products/maars>
- Scharre, P. (2018). *Army of None: Autonomous Weapons and the Future of War*, W.W. Norton & Company.
- Strategic Multilayer Assessment. (2021). *Project Athena Final Study Report*. U.S. Department of Defense.
- Szczygielska, A., Wrzosek M. (2024). *Operacje wielodomenowe w XXI wieku: ewolucja amerykańskich operacji połączonych*. w: S. Markiewicz, W. Materak (red.), *Organizacja systemu rozpoznania zagrożeń państwa: zagrożenia militarne w wielodomenowych operacjach w przyszłych konfliktach zbrojnych*, 17-56. Akademia Sztuki Wojennej.
- U.S. Department of Defense (2025). *Project Convergence*, from <https://www.defense.gov/Spotlights/Project-Convergence/>.
- U.S. Department of Defense. (2017). *Project Maven Industry Day Pursues Artificial Intelligence for DoD Challenges*. Washington, DC.
- U.S. Department of Defense. (2022). *Summary of the Joint All-Domain Command & Control (JADC2)*. Strategy. Department of Defense United States of America.
- UNODA. (2024). *Group of Governmental Experts on emerging technologies in the area of lethal autonomous weapons systems: Background Paper on Existing International Humanitarian Law applicable to LAWS*. CCW/GGE.1/2024/CRP.3.
- UNODA. (2026). *Convention on Certain Conventional Weapons: Group of Governmental Experts on Lethal Autonomous Weapons Systems*. United Nations Office for Disarmament Affairs.
- Wieliczko, L. A. (2024). *Modernizacja lotnictwa wojskowego Australii*, 4, 50-61. Nowa Technika Wojskowa.
- Willbold, J., Sciberras, F., Strohmeier, M., & Lenders, V. (2024). *Satellite cybersecurity reconnaissance: Strategies and their real-world evaluation*. 2024 IEEE Aerospace Conference, 1-9.