

FROM SWARM DRONES TO PREDICTIVE INTELLIGENCE: THE EXPANDING ROLE OF AI IN MILITARY RESILIENCE UNDER VUCA-BANI CONDITIONS

Radu OGNEAN

“Nicolae Bălcescu” Land Forces Academy, Sibiu, Romania
radu.ognean@gmail.com

Abstract: *The integration of artificial intelligence (AI) in military systems is reshaping contemporary warfare in a fundamental way, particularly under conditions defined by volatility, uncertainty, complexity and ambiguity (VUCA), as well as brittleness, anxiety, nonlinearity and incomprehensibility (BANI). This paper examines the role of AI as a key enabler of military resilience across three interconnected domains: autonomous systems, data-driven intelligence and cyber defense. It first analyzes AI-enabled swarm drones with a focus on decentralized coordination and operational robustness manifested in contested environments. Afterwards, it explores predictive intelligence platforms, such as Project Maven and commercial data fusion systems, thus leveraging machine learning for real-time intelligence, surveillance and reconnaissance (ISR) processing. Additionally, the paper investigates the applications of AI in cybersecurity regarding intelligent intrusion detection systems (IDS) and automated security operations. Beyond the technical capabilities, the paper emphasizes the critical role of civil-military collaboration, with a highlight on the dependence of military AI systems on dual-use technologies and private sector innovation, also addressing key challenges such as model reliability, adversarial threats and ethical accountability.*

Keywords: Artificial Intelligence, ISR Systems, Civil-Military Cooperation, VUCA-BANI, AI-enabled warfare

1. Introduction

The integration of artificial intelligence in military systems is accelerating rapidly, representing a structural transformation in the conduct of modern warfare in operational environments that are increasingly defined by the VUCA-BANI systemic characteristics. These conditions are challenging traditional military paradigms that rely on hierarchical decision-making with linear planning models. The ability to process vast volumes of heterogeneous data and to adapt to rapidly evolving conditions becomes a critical determinant of operational effectiveness in such environments.

AI technologies have emerged as key enablers in addressing this type of challenges. Of great importance are the

advancements in technologies related to swarm-enabled unmanned systems, predictive intelligence platforms and machine learning-based intrusion detection systems (IDS) that illustrate the breadth of AI applications across multiple operational domains. However, the transformative impact of AI goes beyond purely technological dimensions. Modern military AI systems are deeply embedded within broader socio-technical environments alongside private sector innovation, thus the civil-military cooperation becomes an absolutely essential condition in the realm of AI-powered innovations.

The current literature provides important insights into the individual applications of artificial intelligence in military affairs, but these contributions are often fragmented

across domains like autonomous systems, intelligence, surveillance and reconnaissance, decision support, cyber defense, or civil-military innovation ecosystems. Research on swarm drones, Project Maven, AI-based intrusion detection, and human-AI teaming tend to treat such developments as separate technological or operational phenomena, and do not connect them systematically to a broader resilience framework. Moreover, the association of AI-enabled military transformation with the combined VUCA-BANI paradigm is not yet adequately integrated in the present research. This creates a need for an interdisciplinary synthesis that can link technical capabilities, operational uncertainty, organizational adaptation and civil-military cooperation.

This paper adopts a qualitative narrative synthesis approach that aims to integrate technical, strategic and policy-oriented literature on the role of AI in military resilience in VUCA-BANI Conditions. The sources have been selected along three major criteria: conceptual relevance for AI-enabled military transformation, application to one of the core domains of the paper - autonomous systems, predictive intelligence, decision-making, cybersecurity and civil-military cooperation - and credibility of publication venue or institutional origin. The review includes peer-reviewed academic articles, books, institutional reports and selected policy documents issued by organizations such as NATO, research centres and defense-related institutions.

2. Conceptual Framework: AI and Resilience in VUCA-BANI Environments

The operational context of contemporary military systems is increasingly conceptualized through the dual lenses of VUCA-BANI. The VUCA framework captures the dynamic, unpredictable nature of modern environments. Its components, namely volatility, uncertainty, complexity and ambiguity are best addressed by agility,

information, restructuring and experimentation [1]. The BANI model refines this perspective further by emphasizing systemic fragility, cognitive overload and the nonlinear propagation of disruptions. Its components, namely brittleness, anxiousness, nonlinearity and incomprehensibility can be countered by resilience, empathy, improvisation and intuition [2].

The transition from VUCA to BANI introduces additional challenges that further underscore the importance of AI. For example, brittleness, defined as the susceptibility of systems to sudden failure, emphasizes the need for robust and fault-tolerant AI architectures. Anxiety, which reflects the cognitive burden on human operators necessitates the development of AI-driven decision support systems that can filter and contextualize information. Nonlinearity is particularly evident in swarm-based autonomous systems where small perturbations can lead to disproportionate outcomes. Lastly, the incomprehensibility that may rise from both system complexity and opaque algorithms can be countered by explainable AI (XAI) which has become a central research focus, aiming to render model outputs interpretable for human decision-makers in high stakes contexts [3].

3. AI in Autonomous Military Systems: Swarm Drones

The integration of AI in autonomous military systems has led to the emergence of swarm-enabled unmanned aerial vehicles (UAVs), an aspect which represents a paradigm shift from platform-centric to network-centric operations. In contrast to centralized command-and-control (C2) architectures, swarm systems rely on decentralized coordination, where individual agents operate on principles derived from swarm intelligence inspired from collective behaviours observed in biological systems such as colonies of insects [4].

At the core of AI-enabled swarm systems are

multi-agent frameworks that facilitate coordination and decision-making among autonomous agents. Multi-Agent Reinforcement Learning (MARL) has emerged as a dominant paradigm that allows agents to learn optimal policies through interaction with both the environment and other agents. The two representative information structures in MARL that are relevant to swarm intelligence can be observed in figure 1:

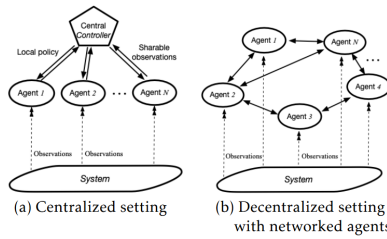


Figure 1: Information structures in MARL relevant to swarm intelligence [5]

In a centralized setting, a central controller aggregates information like joint actions for all agents. The information that is exchanged between the central controller and the agents can include local policies designed for each agent by the controller and also feedback information from the agent. In a decentralized setting, agents do not need a controller because they can communicate via an ad-hoc communication network where information is exchanged between neighbours [5].

In such systems as mentioned above, each drone can dynamically adjust its behaviour based on local observations, while contributing to a global objective such as area coverage, target tracking and coordinated attacks. From an operational point of view, swarm drones provide significant advantages in terms of resilience and effectiveness because of their distributed nature that ensures that the failure or loss of an individual node does not critically degrade overall mission performance, thereby enhancing robustness in adversarial environments. Drone swarms can perform rapid area surveillance and target acquisition, allowing for real-time adaptation to dynamic conditions, including

threat evasion and mission configuration. These capabilities are particularly relevant in anti-access/area denial (A2/AD) scenarios where traditional manned systems can face significant constraints because of the need of a human operator. The deployment of swarm systems also introduces a range of technical and operational challenges. One critical issue is the vulnerability of communication links to electronic warfare tactics. Research efforts in the private sector have focused on developing resilient communication architectures, including mesh networking and AI-based adaptive routing strategies [6]. In the context of VUCA-BANI environments, AI-enabled swarm drones exemplify a shift toward adaptive, decentralized and resilient military systems. Their ability to operate under conditions of uncertainty and maintain functionality despite partial system degradation, aligns closely with the requirements of modern conflict scenarios. Nevertheless, their effectiveness depends upon advances in robust AI algorithms and secure communication infrastructures that are sustained by research in both private and military sectors.

4. AI-Driven Predictive Intelligence and ISR Systems

Integration of AI in ISR systems transformed the manner in which military organization collect, process and exploit critical information in the operational landscape. Contemporary ISR architectures are becoming increasingly data-centric and are relying on the ingestion and fusion of different heterogenous data streams that originate from different sources like satellites, unmanned aerial systems (UAS), signals intelligence (SIGINT), human intelligence (HUMINT), imagery intelligence (IMINT) and open-source intelligence (OSINT). All these different sources are causing an exponential growth in data volume, which has rendered traditional analytical approaches insufficient. Thereby, adoption of AI-driven predictive intelligence

frameworks that are capable of extracting actionable insights in near real-time becomes more and more a necessity [7].

At the core of these AI-enabled ISR systems lies a processing pipeline that integrates the acquisition and preprocessing of data, feature extraction and inference. Machine learning techniques such as deep learning models, have demonstrated significant effectiveness in automating tasks such as object detection, image classification and activity recognition within full-motion videos and satellite imagery. Furthermore, convolutional neural networks (CNNs) are widely employed for visual data analysis and even signal intelligence such as automatic modulation recognition (AMR), where the modulation scheme of a received signal is detected by a CNN with no prior knowledge [8]. Another machine learning technique such as natural language processing (NLP), enables the extraction of relevant information from textual OSINT sources, including social media and news feeds [9].

A flagship example of how militaries are using AI to transform ISR implementation and the targeting process is the United States Department of Defense's Project Maven, promising speed and precision in processing battlefield data and the automatic identification of objects of interest. By automating the labor intensive image analysis process with feeds from drones, planes and satellites, Maven significantly reduces the cognitive burden on human analysts and accelerates the intelligence cycle from data collection to actionable output [10]. Started in 2017, the program quickly appeared in the public scene with a controversy, more exactly in the summer of 2018, Project Maven became faced with a public controversy when it was revealed that the US Department of Defense was using Google's machine learning platform TensorFlow, which is based on deep learning, to provide open-source APIs (Application Programming Interfaces) and to help military analysts detect objects of interest. A petition against Google's

involvement was signed by over four thousand Google employees [11]. More recently, commercial-military platforms such as those developed by Palantir Technologies have extended this paradigm by integrating large-scale data fusion capabilities with advanced analytics and decision support functionalities, enabling the correlation of disparate data sources, facilitating the generation of predictive models that support operational planning and targeting [12].

Predictive intelligence is already extending beyond simple descriptive analytics through the application of probability and time-based analysis in order to predict future events and behaviours, a feature that could be achieved by techniques such as recurrent neural networks (RNNs), including long short-term memory (LSTM) architectures that can be employed to model temporal dependencies in sequential data analysis in order to foresee potential actions, such as adversary movements or emerging threats. Anomaly detection is a very important technique used to detect any behaviour that deviates from regularity and might be linked with new types of threats or techniques. Such tools are extremely useful in environments with limited data availability.

In the context of VUCA-BANI environments, predictive intelligence serves as a critical enabler of resilience, allowing military organizations to anticipate actions and adapt to rapidly changing conditions, thus maintaining operational effectiveness in complex and contested domains. From a systemic perspective, AI-driven ISR capabilities exemplify the shift toward predictive and anticipatory military operations, but despite these advancements, this aspect introduces several technical and operational challenges. A good example is that data quality and bias remain significant concerns, as machine learning models are highly dependent on the representativeness of training datasets, thus inaccurate or biased data can lead to systemic errors in inference and potentially resulting in flawed

operational decisions. Interoperability also presents a challenge, particularly in coalition operations where data standards and system architectures may differ across participating entities, or even because of political and economic restraints. A good example of interoperability deficiencies are the current examples of the talks between the French finance minister's deputy and the Palantir group [13] or the regional and institutional resistance against a Palantir-powered platform in the UK [14].

5. AI-Augmented Decision-Making under Radical Uncertainty

Classical decision-making models which assume relatively stable conditions and bounded uncertainty are insufficient in VUCA-BANI contexts characterised by nonlinear dynamics and emergent threats. In this setting, AI can function as a critical enabler of adaptive decision-making by augmenting human cognition in the analysis of actionable courses of action (COA). A foundational conceptual model for understanding the military decision process is the OODA loop (Observe, Orient, Decide, Act). AI technology can enhance each phase of this loop, even though it cannot replace the human factor [15]. In the observation phase, AI systems can process vast streams of sensor data as ISR inputs, enabling near real-time situational awareness. During the orientation phase, ML models can integrate heterogeneous data sources and identify patterns, thus facilitating a more accurate interpretation of the operational environment. In the decision phase, AI-driven decision support systems can help the battle staff in generating and evaluating multiple COAs using simulation-based approaches. Finally in the action phase, AI-enabled systems can support decisions. However, the human factor cannot and must not be ignored in the OODA loop, thus coining the term "human-AI teaming", that can constitute a critical dimension of the decision-making. Rather than replacing human operators, AI systems should be

designed to function as cognitive amplifiers, enhancing human judgement while still preserving human oversight, a paradigm known as human-in-the-loop (HITL) [16].

One of the key technical approaches underpinning AI-augmented decision-making is reinforcement learning (RL). This technique allows an agent to learn its best behaviour from interacting with its changing environment. RL can be applied to adaptive planning, where predefined methods might not work. More advanced formulations, such as partially observable Markov decision processes (POMDP), consider uncertainties by enabling agents to make decisions based on partial information about and then update their beliefs whenever new information becomes available [17].

From a resilience standpoint, AI can strengthen decision-making through rapid adaptation, increased situational awareness and the consideration of several strategic alternatives under uncertainty. Nevertheless, its success is contingent upon integration with human operators, rigorous model validation and proper governance systems that are able to mitigate ethical and operational hazards.

6. AI in Cyber Defense: Intelligent Intrusion Detection Systems and Security Operations Center Automation

The increasing reliance on computer networks in military operations has elevated cyberspace to a critical domain of conflict [18]. Traditional cybersecurity mechanisms such as signature-based intrusion detection systems (IDS) are limited in their ability to detect zero-day exploits, polymorphic malware and advanced persistent threats (APT). As a result, the integration of AI into cyber defense architectures in order to enable adaptive detection and response mechanisms both in a military and civilian contexts is an idea that circulated for quite some time. Until quite recently, the idea of an AI-driven IDS was a challenging topic because of the difference of the application on ML in the cybersecurity field and other

areas where ML was used with a greater success [19]. However, recent studies show promising results in different machine learning and deep learning algorithms. These results can be observed in Figure 2:

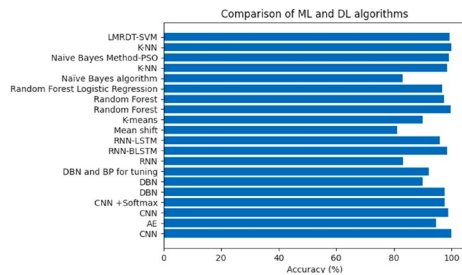


Figure 2: An analysis of the accuracy performance of ML vers DL algorithms [20]

The performance of the algorithms was tested against different types of network attacks, such as DoS (Denial of Service) U2R (User to Root), Probe, U2L (User to Local) attacks with accuracy ranging from 83% for Naïve Bayes Algorithm to 99.89% for K-NN. Even though the results seem promising, the authors of the study advise that the impact of time complexity and CPU utilization for individual packet inspections should be kept in mind when designing a system [20].

Apart from detection, AI can play a transformative role in the automation of Security Operations Centers, in which a massive number of alerts that are generated from heterogeneous security tools must be processed and acted upon. An approach for implementing AI solutions in SOC is through a Security Orchestration, Automation and Response (SOAR) platforms that utilize ML and NLP to prioritize alerts, automate workflows and gather relevant threat intelligence, with various examples of products already available in the industry. From the perspective of resilience, AI applications in cybersecurity contribute to the development of adaptive and self-healing infrastructures by enabling real-time threat detection and automatic mitigation. All these aspects help a military organization in maintaining operational continuity in the face of

persistent and sophisticated cyber threats.

7. Civil-Military Collaboration in AI-Driven Security Ecosystems

The emerging operationalization of AI in modern military systems is becoming ever more dependent upon complex civil-military ecosystems. As stated by the NATO Artificial Intelligence Strategy, modern AI systems are predominantly shaped by advances in the commercial sector and academic research [21]. At the data layer, AI-powered military capabilities depend heavily on various data sources of which many are civilian in origin as is the example of commercial satellite imagery providers and OSINT. All these streams of information enhance ISR capabilities. At the technological level, the development and deployment of AI systems are increasingly facilitated by private sector actors. Companies such as Palantir Technologies have played a significant role in providing data integration and decision-support platforms. These collaborative structures have been essential within the framework of AI applications, where the pace of innovation in the civilian sector often outstrips that of traditional military procurement cycles. But despite its advantages, civil-military collaboration in AI-driven ecosystems is associated with several obstacles such as the governance and regulatory frameworks. A significant example is the European Union's General Data Protection Regulation (GDPR) and the emerging AI Act that impose constraints on data usage and processing. From a strategic perspective, the convergence of civilian and military technological domains has profound significance when it comes to resilience within a VUCA-BANI world. These collaborations enhance adaptability by enabling access to a broader range of resources and expertise, thereby strengthening the capacity of military systems to respond to complex threats.

8. Conclusions

The integration of AI in military systems should be viewed not only as a technological evolution, but as a structural transformation of military resilience in VUCA-BANI conditions. Swarm drones are an example of how an abundance of heterogeneous data can be transformed into actionable operational knowledge. Similarly, intelligent IDS and SOC automation demonstrate how AI can assist in supporting cyber resilience.

However, the study is not without limitations. First, it relies on a qualitative synthesis of existing academic, institutional and policy-oriented sources, rather than on empirical testing or quantitative performance evaluation. Second, many AI-enabled military systems are still classified, experimental, or not fully documented in open sources, which constrains the ability to assess their actual operational effectiveness. Third, the paper covers broad domains of AI application, but does not provide detailed technical validation of specific models,

datasets or deployment architectures. Therefore, all these findings should be interpreted as an integrative conceptual analysis rather than as a definitive assessment of military AI performance.

Further research into the topic needs to be conducted from various perspectives. To begin with, more empirical studies are required to assess how effectively the systems powered by AI function within an operational environment, especially under circumstances involving adversaries and their ability to employ tactics such as electronic warfare, cyberattacks, and impaired communication channels. In addition to that, there is a need for further studies aimed at determining governance structures, accountability measures, and human oversight concerning military AI, especially during the decision-making processes. Finally, comparative research may be performed to determine the impact of varying innovation ecosystems on AI-enabled defense capabilities.

References

- [1] Bennet, N., Lemoine, G.J. What a difference a word makes: Understanding threats to performance in a VUCA world. *Business Horizons Journal*. 2014; vol. 1126:3.
- [2] Halil, F.L.M., Aziz, N.A.A., Hassan, A. Navigating Uncertainty: The Role of VUCA and BANI Frameworks in Educational Leaderships Strategies. *IJRIS*. 2025; vol. 9:5928.
- [3] Ali, S., Abuhmed, T., El-Sappagh S. et al, Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence. *Information Fusion*. 2023; 99:2.
- [4] Bonabeau, E., Dorigo, M., Theraulaz, G. *Swarm Intelligence: From Natural to Artificial Systems*. New York: Oxford University Press; 1999. p. 263.
- [5] Zhang, K., Zhuoran Y., Başar T. Multi-Agent Reinforcement Learning: A Selective Overview of Theories and Algorithms. In: *Handbook of Reinforcement Learning and Control*. New York: Springer; 2021. 335.
- [6] Gupta, L., Jain, R., Vaszkun, G. Survey of Important Issues in UAV Communication Network. *IEEE Communications Surveys & Tutorials*. 2015; vol.18:4-5, 10-16.
- [7] Allen, G. Artificial Intelligence and National Security – A study on behalf of Dr. Jason Mathemny, Director of the US Intelligence Advance Research Projects Activity (IARPA). Cambridge (SUA): Belfer Center for Science and International Affairs; 2017, pp. 27-28.
- [8] Zhang, F., Luo, C., Xu J., Luo, Y., Zheng, F. Deep learning based automatic modulation recognition: Models, datasets and challenges. *Digital Signal Processing*. 2022; vol.129.

- [9] Skopik, F., Akhras, B., Woisetschlager, E. On the Application of Natural Language Processing for Advanced OSINT Analysis in Cyber Defence [Internet]. Vienna: Austrian Institute of Technology; 2024. https://www.researchgate.net/publication/382680760_On_the_Application_of_Natural_Language_Processing_for_Advanced_OSINT_Analysis_in_Cyber_Defence. Accessed April, 20, 2026.
- [10] Manson, K., Scharre, P. Project Maven: Artificial Intelligence in Warfare [Internet]. The Center for a New American Security; 25.03.2026. <https://www.cnas.org/events/project-maven>. Accessed April, 21, 2026.
- [11] Hoijtink, M., Hardeveld A. Machine Learning and the Platformization of the Military: A study of Google's machine learning platform TensorFlow. International Political Sociology. 2022; vol. 16: 2.
- [12] Jeans, D. Exclusive: Pentagon to adopt Palantir AI as core US military system, memo says [Internet]. Reuters; 21.03.2026 [updated 08.04.2026]. <https://www.reuters.com/technology/pentagon-adopt-palantir-ai-as-core-us-military-system-memo-says-2026-03-20/>. Accessed April, 23, 2026.
- [13] Izambard, A. French finance ministry sounds out Palantir [Internet]. Intelligence Online; 14.04.2026 [updated 15.04.2026] <https://www.intelligenceonline.com/europe-russia/2026/04/14/french-finance-ministry-sounds-out-palantir,110702873-art>. Accessed April, 23, 2026.
- [14] Johnson, J. Britain has a weak hand in Palantir test case [Internet]. Reuters; 17.04.2026 [updated 17.04.2026]. <https://www.reuters.com/commentary/breakingviews/britain-has-weak-hand-palantir-test-case-2026-04-17/>. Accessed April, 23, 2026.
- [15] Johnson, J. Automating the OODA Loop in the Age of AI [Internet]. Center for Strategic and International Studies; 25.07.2022. <https://nuclearnetwork.csis.org/automating-the-ooda-loop-in-the-age-of-ai/>. Accessed April, 23, 2026.
- [16] Lazaros, K., Vrahatis, A.G., Kotsiantis, S. Human-in-the-Loop Artificial Intelligence: A systematic Review of Concepts, Methods and Applications. Entropy Journal. 2026; vol. 28:377.
- [17] Cassandra, A.R. Technical Report MCC-INSL-111-98 - A Survey of POMDP Applications, Microelectronics and Computer Technology Corporation. AAAI Fall Symposium. 1998. p 4-5.
- [18] Minárik, T. NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit [Internet], Tallinn (Estonia): CCDCOE. <https://ccdcoe.org/incyber-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/>. Accessed on April, 25, 2026.
- [19] Sommer, R., Paxson, V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection, 31st IEEE Symposium on Security and Privacy. 2010. pp. 305-310.
- [20] Sowmya T., Mary Anita E.A., A comprehensive review of AI based intrusion detection system. Measurement: Sensors. 2023. vol. 28: 5.
- [21] Summary of the NATO Artificial Intelligence Strategy [Internet]. NATO; 22.10.2021. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/10/22/summary-of-the-nato-artificial-intelligence-strategy>. Accessed April, 30, 2026.