Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume I, 167-171

Expectations and Opportunities for AI-enabled Systems Application in the Context of Military Communications and Cybersecurity

Angel Genchev
Bulgarian Defence Institute
"Prof. Tsvetan Lazarov"
Sofia, Bulgaria
a.genchev@di.mod.bg
ORCID: 0000-0002-0672-737X

Emil Ivanov
Ministry of Defence
Sofia, Bulgaria
emotsiv@gmail.com
ORCID: 0000-0003-1658-9588

***Abstract*—The rapid advancement of Artificial Intelligence (AI) is transforming military communications and cybersecurity by enabling higher levels of automation, adaptability, and data-driven decision-making. This paper examines the role of AI-enabled systems in military communication environments, with a focus on emerging operational trends, system requirements, and potential application areas. Particular attention is given to the effects of communication disruptions on mission effectiveness and to the growing need for resilient, secure, and interoperable communication infrastructures. The paper also outlines conceptual examples of AI-enabled military communication systems that can optimise network performance, prioritise critical data transmission, and strengthen cybersecurity through improved threat detection and response. The analysis shows that AI can significantly enhance situational awareness and real-time operational responsiveness, while also introducing new dependencies and implementation challenges. The study highlights the importance of adaptive system design and effective human-AI collaboration for the secure and reliable use of AI in military communications.**

***Keywords*—artificial intelligence, command and control (C2), cybersecurity, military communications.**

I. Introduction

Artificial intelligence (AI) has been developing at an incredible pace in recent years, impacting both civilian and military domains in ways that were difficult to predict in the past. The widespread availability of computing resources, vast libraries of open-source software, and large datasets has accelerated innovation and significantly reduced the difficulty of developing AI. As a result, AI technologies are no longer restricted to specialised actors but are increasingly accessible to a wide range of organisations, including potential adversaries [10], [11].

In the military domain, this shift is already visible. AI is being integrated into autonomous systems operating across air, land, sea, and cyber environments [12], enhancing capabilities such as multi-domain coordination, sensor exploitation, and decision support. At the same time, recent conflicts suggest that these technologies contribute to a more complex and contested operational environment, where threats are not only more persistent but also harder to identify and counter.

This paper focuses specifically on digital military communications, which rely on interconnected networks, protocols, and distributed systems to enable command and control (C2), where human–machine interaction plays an increasingly important role [13], [15]. As modern operations become more dependent on timely and secure information exchange, communication systems evolve into both a critical enabler and a potential point of vulnerability.

The objective of this study is to analyse the expectations, requirements, and opportunities for applying AI-enabled systems in military communications and cybersecurity, while also identifying key risks associated with their integration. In practical terms, the goal is to outline how these technologies can improve operational effectiveness without introducing unacceptable levels of dependency or risk.

II. Trends in the Military Operations

The integration of Artificial Intelligence into military operations is taking place in a rapidly evolving technological and regulatory environment. Although international discussions on the ethical and legal use of AI are ongoing, clear and enforceable frameworks are still limited. The absence of harmonised legal and ethical standards for military AI raises additional concerns regarding accountability, transparency, and the delegation of decision-making authority. In practice, this creates uncertainty, particularly in scenarios where adversaries may choose to employ AI capabilities without adhering to such constraints, including in the targeting of communication systems and cyber infrastructure.

One of the most noticeable developments in modern military operations is the increasing complexity of

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol1.75

communication systems. Unlike civilian networks, military communications are expected to function in contested and degraded environments, where infrastructure may be disrupted or deliberately attacked. Ensuring secure and reliable communication across geographically dispersed and often multinational forces remains a persistent challenge. This is further complicated by the need for interoperability between diverse technologies, ranging from terrestrial radio systems to satellite and data networks.

At the same time, military communication infrastructures are exposed to a continuously evolving cyber threat landscape [14]. Adversaries, including both state and non-state actors, employ a wide range of techniques such as advanced persistent threats (APTs), distributed denial-of-service (DDoS) attacks, and targeted intrusion campaigns. These threats do not only aim to compromise data but can also disrupt critical services and degrade overall operational capability.

The growing dependence on digital technologies further amplifies these risks. Decision-making processes increasingly rely on large volumes of data from multiple sources, which introduces additional vulnerabilities related to data integrity and availability. In practice, a successful cyber attack may have cascading effects that extend beyond the cyber domain, affecting mission execution and even personnel safety.

In this context, Artificial Intelligence is increasingly seen as a practical enabler for improving the resilience and adaptability of military communication systems. By supporting faster anomaly detection, adaptive network management, and more effective response to cyber threats, AI addresses several of the key challenges associated with modern military operations.

These factors highlight the critical role of modern technologies, particularly Artificial Intelligence, in addressing the complexity of military communications.

III. REQUIREMENTS OF MILITARY COMMUNICATIONS

Military communication systems must satisfy a set of stringent and often competing requirements, driven by the dynamic and high-risk nature of military operations. These requirements extend beyond conventional communication system design and are closely linked to mission effectiveness, operational security, and decision-making processes.

A. Security and resilience.

Communication systems must ensure the confidentiality, integrity, and availability of transmitted information. This includes the use of advanced encryption techniques capable of withstanding sophisticated cyber threats, as well as mechanisms for detecting, resisting, and recovering from attacks such as jamming, interception, and intrusion. Resilience is particularly critical in contested environments, where partial system degradation must not lead to total communication failure.

B. Adaptability and flexibility.

Military communication networks must be capable of rapid reconfiguration in response to changing operational conditions. This includes dynamic routing, spectrum adaptation, and the ability to integrate new nodes or platforms in real time. Flexibility is essential for maintaining operational continuity in highly dynamic and unpredictable environments.

C. Interoperability.

Modern military operations often involve joint and multinational forces, requiring seamless communication across heterogeneous systems and platforms. Communication infrastructures must support interoperability between different technologies, standards, and protocols, enabling effective coordination and information exchange across domains.

D. Low latency and reliability.

Timely delivery of information is critical, particularly at the tactical level, where delays can directly impact operational outcomes. Communication systems must therefore provide reliable and low-latency data transmission, even under adverse conditions such as network congestion or partial infrastructure disruption.

E. Situational awareness.

Communication systems should support the generation of a coherent and accurate operational picture by integrating data from multiple sources. This includes sensor data, intelligence inputs, and system status information, presented in a form that supports rapid and informed decision-making.

These requirements highlight the need for advanced, adaptive, and intelligent communication solutions, where AI can play a central role in balancing performance, security, and operational effectiveness. They also imply that any disruption in communication systems may have critical operational consequences.

IV. IMPACT OF COMMUNICATION DISRUPTIONS

Communication disruptions in military operations can have immediate and severe consequences, directly affecting command and control processes and overall mission effectiveness. In highly dynamic and time-critical environments, even partial loss of communication may lead to delays in decision-making, reduced situational awareness, and loss of coordination between units. Such disruptions increase the risk of operational errors, including misinterpretation of commands, failure to execute critical tasks, or unintended engagement of friendly forces. In addition, the inability to maintain reliable communication can compromise operational security and expose vulnerabilities that adversaries may exploit.

From a strategic perspective, communication failures can degrade the effectiveness of entire operational frameworks, limiting the ability to coordinate actions across different domains and levels of command. In extreme cases, prolonged disruption may result in mission failure, loss of critical assets, and increased risk to personnel.

Given the critical role of communication systems, ensuring their continuity, reliability, and protection against disruption is a fundamental requirement for modern military operations. This creates a strong need for intelligent and adaptive mechanisms capable of maintaining communication effectiveness under adverse conditions.

V. OPPORTUNITIES TO USE AI

In current military operational environments, where fast, secure, and reliable communication is critical, AI represents a key enabler for improving operational efficiency, resilience, and decision-making. AI-enabled systems can process large volumes of heterogeneous data in real time, which is particularly important in dynamic and uncertain conditions, supporting command and control (C2) processes.

One of the primary advantages of AI is its ability to enhance communication efficiency and adaptability. AI-driven network management can dynamically optimise routing, allocate bandwidth, and adapt to changing conditions such as interference, congestion, or partial infrastructure failure. This is particularly important in contested electromagnetic environments, where communication channels may be degraded or intermittently unavailable.

Another important advantage is the improvement of interoperability between different systems and units. By leveraging machine learning (ML) and natural language processing (NLP), AI can facilitate multilingual communication and support seamless interaction between multinational forces and heterogeneous platforms. From a cybersecurity perspective, AI provides advanced capabilities for detecting, analysing, and responding to threats. By continuously monitoring network traffic, system logs, and behavioural patterns, AI models can identify anomalies that may indicate malicious activity. Techniques such as behavioural analysis, deep learning, and anomaly detection enable early identification of cyber threats and support proactive defence mechanisms.

Adversarial AI techniques represent an emerging challenge, as malicious actors may manipulate input data or exploit vulnerabilities in AI models to degrade performance, evade detection, or influence decision-making processes.

In addition, AI supports automated threat assessment and response. AI-driven systems can classify incidents based on severity, origin, and potential impact, enabling faster and more efficient allocation of resources. Integration with incident response platforms allows the implementation of automated response actions, such as isolating compromised nodes, blocking malicious traffic, or initiating predefined mitigation procedures.

Another important application area is the optimisation and prioritisation of data transmission. In environments with limited bandwidth, AI can evaluate the relevance and urgency of transmitted information, ensuring that critical data is delivered with priority. This is particularly relevant for sensor networks, where large volumes of raw data must be filtered and processed before transmission.

AI also enables the integration of communication and electronic warfare capabilities. By analysing the electromagnetic environment in real time, AI systems can optimise the performance of friendly communication systems while simultaneously minimising the effectiveness of adversary systems.

The role of AI varies across the different levels of military operations:

– **Tactical level**. AI systems support real-time operations by assisting personnel, enabling semi-autonomous actions, and enhancing situational awareness. Applications include autonomous platforms, swarm coordination, and adaptive sensor networks.

– **Operational level**. AI enables multi-sensor data fusion, situational assessment, and evaluation of alternative courses of action. It supports planning processes by optimising resource allocation and analysing different operational scenarios.

– **Strategic level**. AI can support long-term planning and decision-making by modelling complex scenarios, analysing adversary behaviour, and assessing the potential impact of different strategies. It may also contribute to information operations and influence activities in the information domain.

Despite these advantages, effective implementation of AI requires strong human–AI collaboration. While AI systems provide speed and analytical capabilities, human operators remain essential for contextual understanding, ethical judgment, and strategic decision-making [13, [15]. Practical implementation of AI-enabled systems in military environments also presents significant challenges. These include computational constraints at the tactical level, limited availability of representative training data, high requirements for model adaptation, and the need to ensure reliable performance under resource-constrained and adversarial conditions.

VI. CONCEPTUAL EXAMPLES OF AI-ENABLED MILITARY COMMUNICATION SYSTEMS

The application of Artificial Intelligence in military communications can be illustrated through several conceptual system models addressing key operational challenges. These concepts are aligned with the dynamics of the decision-making process, commonly described by the OODA loop [4], and reflect the differing requirements across tactical, operational, and strategic levels. Current developments in industry and research further demonstrate the continuous evolution of such systems [2], [3]. The effectiveness of communication systems at these levels depends on key performance characteristics, including latency, throughput, reliability, and security. While higher levels of command prioritise reliability and security, they can tolerate higher latency. In contrast, tactical-level operations require near real-time communication with strict latency constraints. These differences define the appropriate technological approaches and optimisation strategies.

A. AI-based WAN optimisation model.

A conceptual AI-based WAN optimisation model with distributed agents is illustrated in Fig. 1.

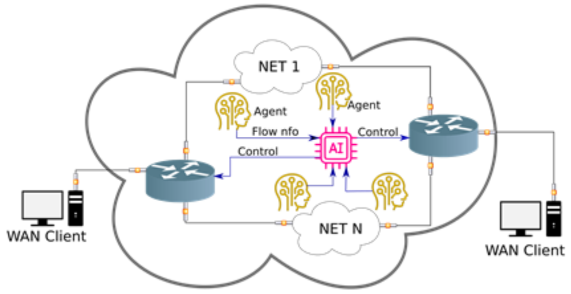

Fig. 1. AI-based WAN optimisation model

Network optimisation in tactical environments has traditionally relied on dynamic resource management and state estimation techniques [5], [6], followed by more advanced approaches such as software-defined networking and SD-WAN optimisation [7]. Building on these developments, a conceptual AI-based wide-area network (WAN) optimisation model can be constructed by integrating distributed monitoring agents and a central AI-based optimisation module. The agents collect real-time data on network conditions, including traffic load, delay, packet loss, and link availability. This information is transmitted via a management channel to an AI controller, which dynamically selects optimal routing paths and resource allocation strategies. Compared to traditional rule-based approaches, AI-driven optimisation enables predictive and adaptive behaviour, improving throughput and resilience under varying operational conditions.

B. AI-driven data filtering and prioritisation in sensor networks.

A conceptual network model, implementing an AI filter, is suggested in Fig. 2. It can be implemented as a component of a software-defined network similar to the separated planes network in [8].

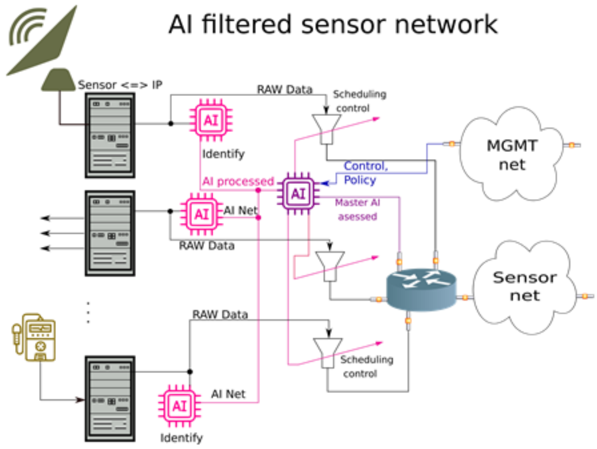

Fig. 2. Conceptual model of an AI-filtered sensor network

In bandwidth-constrained environments, efficient data transmission is a critical requirement. A conceptual model for AI-based filtering can be applied to sensor networks, where large volumes of raw data are continuously generated. In this model, AI modules embedded within sensor controllers analyse incoming data streams and determine their relevance based on learned patterns or predefined criteria. Only significant events, such as target detection, are prioritised for transmission. A higher-level AI controller aggregates these outputs and dynamically adjusts transmission priorities based on operational context and network conditions. This approach extends existing concepts of prioritised data handling and quality of service in distributed networks [8], enabling more intelligent and context-aware traffic management. It reduces unnecessary data transmission, optimises bandwidth utilisation, and ensures that critical information is delivered with minimal delay.

C. AI-enabled cybersecurity architecture.

A simplified diagram of the possible implementation of an AI-based solution to defend a network is presented in Fig. 3.

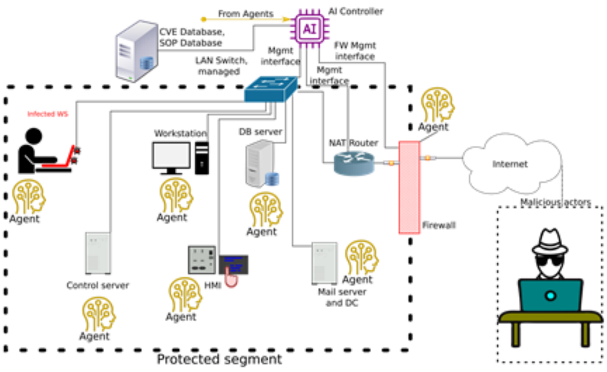

Fig. 3. AI-enabled conceptual model of a computer network

AI can also be integrated into communication systems to enhance cybersecurity through continuous monitoring, threat detection, and automated response. A conceptual architecture includes distributed monitoring agents deployed across network nodes and a central AI controller responsible for assessment and control functions. Similar approaches have been explored in recent research and development efforts, including the AInception project [9], which investigates AI-driven and algorithmic solutions for automated network protection and response. In such architectures, the assessment component analyses network activity to classify behaviour as normal or malicious, while the control component determines appropriate response actions. These actions may include isolating compromised nodes, blocking malicious traffic, or alerting human operators. Different deployment strategies are possible, ranging from full agent distribution across all network devices to selective deployment at critical points such as routers, switches, and firewalls, each involving trade-offs between data availability, system complexity, and implementation cost.

These conceptual models demonstrate how AI can be embedded within military communication infrastructures to improve performance, efficiency, and security. While they are based on current technological capabilities and research trends, their practical implementation requires further validation in real-world operational environments.

VII. CONCLUSIONS

This paper examined the role of Artificial Intelligence in the context of military communications and cybersecurity, focusing on current operational trends, system requirements, and the impact of communication disruptions. The analysis highlighted the increasing complexity and vulnerability of modern military communication infrastructures, driven by their dependence on digital technologies and exposure to evolving cyber threats.

The study identified key opportunities for the application of AI, including adaptive network management, intelligent data prioritisation, enhanced situational awareness, and advanced cyber threat detection and response. These capabilities demonstrate the potential of AI to significantly improve the resilience, efficiency, and responsiveness of military communication systems.

In support of this analysis, three conceptual models were proposed, addressing AI-based WAN optimisation, intelligent sensor data filtering, and AI-enabled cybersecurity protection. These models illustrate how AI can be integrated across different layers of communication infrastructures to address both performance and security challenges. At the same time, the integration of AI introduces new challenges, including increased system complexity, dependence on data quality, and the need for reliable human–AI interaction. Ensuring transparency, robustness, and controllability of AI systems remains a critical requirement for their effective deployment in military contexts.

Future research should focus on validating the proposed conceptual models through simulations, experimental environments, and operational scenarios, as well as assessing their performance under realistic communication and cybersecurity constraints.

Acknowledgements: The work in this paper has received funding from the European Union – European Defence Fund under GA no. 101103385 (AInception). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. The European Union cannot be held responsible for them.

REFERENCES

[1] S. Prasad, D. Behl, J. Raju, and T. Lewis, “Building AI-driven closed-loop automation systems,” IBM Developer, [Online]. Available: https://developer.ibm.com/articles/an-introduction-to-closed-loop-automation/ .

[2] Thales Group, “Tactical networks,” [Online]. Available: https://www.thalesgroup.com/en/markets/defence-and-security/mission-critical-communications/tactical-networks .

[3] General Dynamics Mission Systems, “Warfighter Information Network-Tactical (WIN-T),” [Online]. Available: https://gdmissionsystems.com/communications/warfighter-information-network-tactical .

[4] L. M. Blaha, “Interactive OODA Processes for Operational Joint Human-Machine Intelligence,” in STO-MP-IST-160, pp. 3–18.

[5] A. S. Peng, D. M. Moen, T. He, and D. J. Lilja, “Automatic Dynamic Resource Management Architecture in Tactical Network Environments.”

[6] R. Fronteddu et al., “State Estimation for Tactical Networks: Challenges and Approaches,” in MILCOM 2018, pp. 1042–1048, doi:10.1109/MILCOM.2018.8599823.

[7] VMware, “SD-WAN Dynamic Multipath Optimization,” [Online]. Available: https://kb.vmware.com/s/article/2733094 .

[8] C. Gedo et al., “GIG QoS Inter-Domain Interoperability Challenges,” in MILCOM 2007, https://doi.org/10.1109/MILCOM.2007.4455023.

[9] AInception Project, “Project overview,” [Online]. Available: https://www.ainception.eu/overview .

[10] S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, 4th ed., Pearson, 2021.

[11] NATO STO, “Artificial Intelligence and Autonomy in Defence,” Science & Technology Organization, 2020.

[12] P. Scharre, Army of None: Autonomous Weapons and the Future of War, W. W. Norton & Company, 2018.

[13] M. Lewis et al., “Human–Machine Teaming for Military Decision Making,” IEEE Computer, vol. 51, no. 12, pp. 38–45, 2018.

[14] ENISA, “Artificial Intelligence Cybersecurity Challenges,” European Union Agency for Cybersecurity, 2021.

[15] J. Kott and C. Arnold, “The Promises and Challenges of AI for Military Decision-Making,” Military Operations Research, 2019.