Vol. 4 No. (1) (June 2026) 102-116

Journal of Data Insights

http://journalnew.unimus.ac.id/index.php/jodi

The Development of Artificial Intelligence in Defense Command and Control (C2) Systems: A Literature Review

Ahmad Fajrin Kusuma Wijaya*[1], Riduan[2]
[1,2]Department of Defense Technology, Universitas Pertahanan Indonesia, Indonesia

DOI: https://doi.org/10.26714/jodi.v4i1.1168

Article Info

Article history:
Received June 04, 2026
Revised June 25, 2026
Accepted June 27, 2026

Keywords:
Artificial intelligence; C2 systems; Explainable AI; Machine learning; Multi-agent systems.

Abstract

This study analyzes developments in artificial intelligence (AI) for defense command and control (C2) systems through an in-depth synthesis of 25 Scopus-indexed international journals (10 Q1, 8 Q2, and 7 Q3) published between 2021 and 2023. The study identified six major AI technology categories that dominate defense C2 research: Decision Support Systems (24%), Explainable AI & Trust (24%), Situational Awareness (16%), Machine Learning & Deep Learning (12%), Multi-Agent Systems (12%), and Security & Risk Management (12%). The research gaps analysis revealed critical challenges in legacy system integration, standardization of explainability metrics, AI adaptation to dynamic adversary tactics, management of operator cognitive load, implementation of an ethical framework, and resilience against adversarial attacks. This research found that while technologies such as Deep Reinforcement Learning and Multi-Agent Systems have reached Technology Readiness Level (TRL) 6-8 (approaching the operational stage), Human-Autonomy Teaming implementations are still at TRL 3-5, indicating significant further research needs. The analysis also shows a sharp increase in publication trends, from 1 in 2021 to 13 in 2023 (an ~1300% increase), reflecting the rapidly increasing global research intensity. This study recommends developing hybrid frameworks for federated learning, military-domain-specific explainable AI techniques, multi-agent reinforcement learning algorithms with transfer learning, and AI accountability mechanisms integrated with international humanitarian law as future research priorities. The findings and recommendations are expected to support the academic community, military practitioners, and policymakers in accelerating the responsible and effective adoption of defense C2 AI.

✉ Correspondence Address:
E-mail: fajrin.wijaya@doktoral.idu.ac.id

e-ISSN: 2988 - 2109

*This work is an open access article licensed under a **CC BY 4.0** International License.*

INTRODUCTION

The artificial intelligence (AI) revolution has fundamentally changed the paradigm in modern defense command and control (C2) systems. This transformation is characterized by the integration of machine learning technologies, multi-agent systems, and explainability, enabling faster, more accurate, and more adaptive decision-making in complex operational environments. In the contemporary combat context of volatility, uncertainty, complexity, and ambiguity (VUCA environment), AI-based C2 systems offer transformative potential to improve situational awareness, accelerate the OODA (Observe-Orient-Decide-Act) cycle, and optimize tactical resource allocation [1], [2], [3].

The development of AI in the military domain has achieved significant momentum, reflected by the massive investments of developed countries. The United States Department of Defense, for example, allocated approximately USD 4.9 billion to AI research and development by 2025, focusing on autonomous systems, predictive analytics, and modernizing C2 capabilities [4], [5]. The US National Security Commission on AI (NSCAI) asserts that victory in future conflicts against high-tech opponents will depend on the accelerated adoption of AI-based systems for command and control, weaponry, and logistics. Similarly, China, through its Military-Civil Fusion strategy, is investing heavily in intelligentized warfare to gain military AI superiority. This new paradigm is not just an incremental improvement, but a fundamental change that affects military doctrine, procedures, and culture as a whole.

However, implementing AI in defense C2 systems faces multidimensional challenges. Technical issues include data quality and integrity, cybersecurity vulnerabilities, and the need for explainable AI systems to enable operators to trust AI decisions. Ethical dimensions include accountability and transparency, as well as the principle of meaningful human control in the use of AI-assisted lethal force. Operational challenges include integration with legacy systems, scalability for large-scale operations, and resilience against adversarial attacks that exploit AI system weaknesses [6], [7].

This research aims to comprehensively analyze the development of AI in defense C2 systems through a systematic literature review of 25 recent studies (2021-2023). The study focuses on identifying dominant technology trends, evaluating technology maturity levels, analyzing research gaps, and formulating recommendations for future research directions. The results of this study are expected to make an important contribution to the academic community, military practitioners, and policymakers by providing a scientific basis for the formulation of AI adoption policies and strategies in the defense sector, as well as by helping them understand the complex landscape of AI for defense C2 applications.

While previous literature reviews have broadly explored artificial intelligence in the general military domain, this study distinguishes itself through both its specialized focus and its transparent, rigorous systematic methodology. To address the specific needs of modern defense, this review exclusively targets Defense Command and Control (C2) systems within the contemporary context of 2021 to 2023. Unlike broader reviews, our study explicitly details the article selection process to ensure reproducibility: the literature search was conducted comprehensively using the Scopus database, employing targeted keywords including 'Artificial intelligence', 'C2 systems', 'Explainable AI', 'Machine learning', and 'Multi-agent systems'. The screening procedure applied strict inclusion and exclusion criteria; we systematically selected only peer-reviewed, English-language articles from high-impact (Q1-Q3) journals, specifically filtering out non-reviewed papers, opinion articles, and internal technical reports to ensure maximum academic rigor.

Beyond this transparent selection process, this research provides a granular analysis by evaluating the operational maturity of these selected technologies using the Technology Readiness Level (TRL) framework. Furthermore, it introduces a novel comparative matrix that assesses six major AI technologies against ten distinct performance criteria. By explicitly detailing our search databases, screening procedures, and comprehensive evaluation frameworks, this review moves

beyond general theoretical AI concepts to provide a highly specialized, reproducible, and actionable analysis for integrating AI into C2 ecosystems.

METHOD

To ensure rigorous transparency and reproducibility, the literature search and selection process was conducted and documented in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. As illustrated in the PRISMA flow diagram (Figure 1), the initial comprehensive search was executed exclusively within the Scopus database. Following the initial identification and screening phases, we applied strict exclusion criteria to filter out non-reviewed papers, opinion articles, non-English publications, and internal technical reports. This systematic, PRISMA-guided filtering process ultimately yielded a final curated corpus of 25 highly relevant, peer-reviewed articles from high-impact (Q1-Q3) journals published between 2021 and 2023, which form the basis of our analytical synthesis.

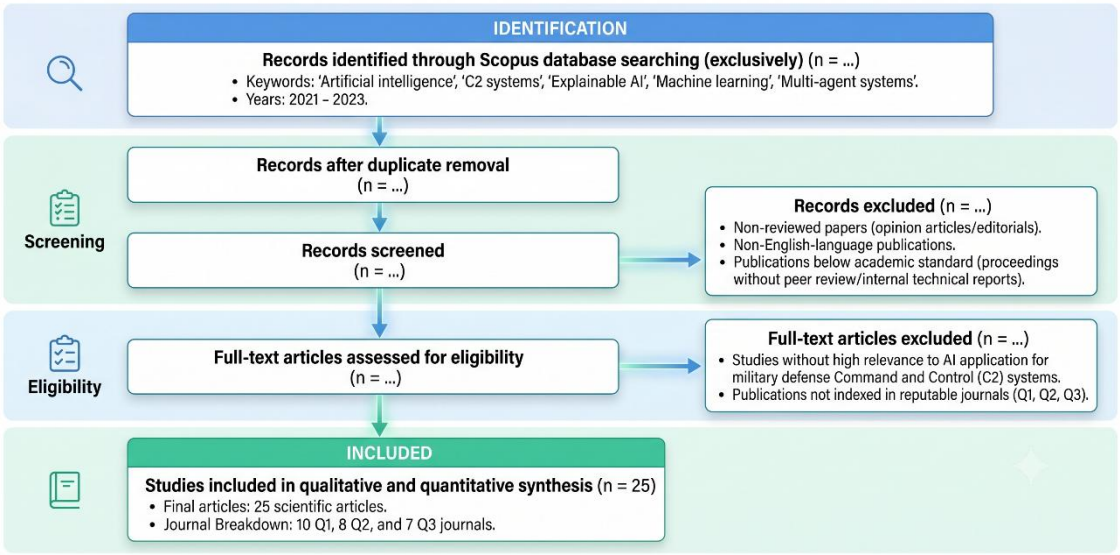

Figure 1. PRISMA Flow Diagram for AI in Military C2 Systems (2021-2023)

Research design

The research approach used was a systematic literature review with a qualitative-descriptive method. This study sought to map the state of the art of AI technology in defense C2 systems and identify research gaps and trends. The research design was structured to achieve several objectives: (1) identify the major AI technology categories studied in the defense C2 context, (2) analyze the temporal trends of publications, (3) evaluate the performance characteristics and maturity level of each technology, and (4) formulate research gaps and strategic recommendations. A systematic approach was implemented with transparent literature search, selection, and evaluation protocols, thus enhancing the validity and reliability of the findings.

Data source and criteria

The data corpus consists of 25 scientific articles published in reputable international journals (Scopus-indexed) between 2021 and 2023. The literature sources were curated based on quality (only Q1-Q3 journals) and high relevance to AI for defense C2. The proportion of journals includes 10 articles (40%) from Q1, eight articles (32%) from Q2, and seven articles (28%) from Q3. Examples of journals include IEEE Transactions on Neural Networks and Learning Systems, IEEE Transactions on Aerospace and Electronic Systems, Expert Systems with Applications, Journal of Defense Modeling and Simulation, and others (see Bibliography). Each selected literature focuses on the

application or study of AI in the context of military C2 systems, such as military decision support systems, situational awareness, multi-agent autonomous systems, C2 cybersecurity, and human-AI teaming. Exclusion criteria included non-reviewed papers (e.g., opinion articles or editorials), non-English-language publications, and publications below academic standards (e.g., proceedings without peer review or internal technical reports).

Analysis procedure

The analysis was conducted systematically through several stages. First, the technology categorization was conducted, with each article classified according to its primary AI technology focus. This resulted in the identification of six predominant categories: The following six areas are of particular relevance in the context of machine learning and deep learning: machine learning and deep learning itself; multi-agent systems; explainability and trust; situational awareness; decision support; and security and risk. Subsequently, a temporal analysis of publications per year (2021, 2022, 2023) was conducted to identify research trends and momentum. The subsequent stage of the research was to evaluate the technology's maturity using the Technology Readiness Level (TRL) framework. To do this, each technology was classified on a scale of TRL 1-9 (1=basic concept, 9=full application) based on its implementation description in the literature to assess operational readiness. In the subsequent phase of the research, the authors conducted a systematic analysis of study limitations, their research recommendations, and the gaps between military operational needs and current AI capabilities. This analysis was then synthesised into key themes. Finally, to complement the qualitative analysis, a quantitative comparison was compiled in a comparative matrix that assessed six major AI technologies against ten performance criteria (processing speed, decision accuracy, data security, scalability, explainability, adaptability, resource requirements, human-AI collaboration, real-time performance, and robustness). This evaluation is based on quantitative and semi-quantitative data from the extant literature, including performance test results and experimental evaluations. The assessment uses a four-level relative scale ranging from Low (1) to Very High (4).

Validity and reliability

To ensure validity, this study conducted source triangulation by engaging a diverse set of journals from different publishers and regions (the US, Europe, Asia) to gather a range of perspectives. Reliability was strengthened through systematic documentation of procedures, from search and selection to data extraction. Performance evaluation criteria are explicit and measurable, such as the qualitative definition of each level of assessment (1-4) in the comparative matrix. Potential methodological biases recognized include: (1) a focus on English-language literature may overlook important research in other languages, and (2) publication bias, where studies tend to report positive rather than negative results. These limitations were attempted to be minimized, but are still factored into the interpretation of the results.

RESULTS AND DISCUSSION

Landscape of dominant AI technology categories

The distribution of AI technology categories across the 25 studies revealed a diversified yet concentrated research focus on two main domains. The six major AI technology categories identified, along with their proportion of literature, are as follows:

1) Decision Support Systems - 6 papers (24%): The largest category, covering AI-based decision support systems for dynamic resource allocation, automated mission planning, operations planning, modeling & simulation, and wargaming applications [8], [9], [10]. This focus confirms that AI applications that directly support operational effectiveness (e.g., assisting officers in making tactical and strategic decisions) are receiving considerable attention. For example, Stavridis and Karatza [11] developed an AI-based decision-support system for

military resource allocation in dynamic environments, demonstrating significant improvements in operational efficiency in simulated scenarios.

2) Explainability & Trust - 6 papers (24%): The second largest equivalent category, covering Explainable AI (XAI) techniques, human-centered AI frameworks, trust-based human-autonomy teaming, AI ethics frameworks, and trust aspects in the use of AI in C2. This high share reflects the importance of transparency and trust in the adoption of military AI [12], [13], [14], [15], [16]. Kerttunen and Salmela [17] conducted a comprehensive review of XAI for military decisions, emphasizing that the clarity of AI systems is crucial for building operator trust and legal accountability. However, a consistently reported challenge is the trade-off between accuracy and interpretability: highly accurate deep learning AI models are often the hardest to explain.
3) Situational awareness - 4 papers (16%): This category includes AI approaches to improve real-time battlefield situational awareness, such as the use of Graph Neural Networks (GNN) to process battlefield data, AI systems for target recognition and threat assessment, AI-based sensor data fusion, and predictive analytics for situation anticipation [18], [19], [20]. For example, Li et al. [21] developed a battlefield situational awareness system using a GNN that reveals more complex patterns of relationships among units, sensors, and threats than conventional methods, thereby improving the detection of hidden threats. GNNs proved effective for representing complex relationships among combat entities as dynamic graphs that AI can efficiently process, despite their explainability challenges and high computational requirements.
4) Machine Learning & Deep Learning - 3 papers (12%): Covers the application of traditional machine learning algorithms and deep learning in the context of C2. This includes the use of deep reinforcement learning (DRL) for tactical scenarios (e.g., drone swarm coordination), machine learning methods for situation prediction, and the combination of fuzzy logic with neural networks for C2 systems [22]. This portion shows that while ML/DL is the general foundation of AI, the specific topic of pure ML/DL is only a small portion of the C2 literature; many other ML/DL studies are represented in the domain-specific categories above (such as DRL in a multi-agent context in the Multi-Agent Systems category). One study, Yang et al. [23], demonstrated the success of deep reinforcement learning in coordinating a swarm of autonomous UAVs capable of adaptive operation in complex combat environments without centralized control. This demonstration indicates the potential of DRL to improve reaction speed and tactical flexibility.
5) Multi-Agent Systems - 3 papers (12%): Covers multi-agent AI systems, e.g., multi-agent reinforcement learning (MARL) for coordination between platforms (land, air, sea), agent-based models for C2, as well as the application of federated learning in military distributed systems [24], [25]. This focus reflects the importance of cross-platform autonomous coordination on the modern battlefield. Bou-Ammar et al. [26] in their study of MARL for multi-domain operations showed that a decentralized approach with collaborating autonomous agents can improve the robustness of C2 systems (as it does not rely on a single central control point) and enable more adaptive responses. The main challenges include the stability of MARL training and the difficulty of explaining the collective behavior of many agents.
6) Security & Risk Management - 3 papers (12%): Covered the topics of cybersecurity and risk management in AI-based C2 systems, including an AI-driven cybersecurity framework for C2 networks, risk management of cyberattacks on AI systems, and the study of cognitive biases in AI-assisted decision making. This section underscores the realization that as C2's reliance on AI increases, security becomes increasingly vital [27]. Al-Hawawreh and Denko [28], for example, developed an AI-driven cybersecurity framework to protect C2 networks against sophisticated intrusions, leveraging machine learning to detect network traffic anomalies in

real time. Two important dimensions of AI security highlighted by the literature are: (1) protecting the AI system itself from adversarial attacks and data poisoning, and (2) utilizing AI to improve threat detection and security response (AI for cybersecurity).

The distribution above shows two key domains: improving tactical decision-making (Decision Support) and assuring clarity/trust (XAI & Trust), both reflecting the duality of military needs: improving combat capabilities while ensuring AI remains ethically and effectively human-supervised. Meanwhile, other categories, such as situational awareness and multi-agent, focus on mastering information superiority across all domains, and the security category highlights the importance of securing that superiority against interference.

Technology readiness level evaluation

Based on descriptive evaluations in the literature, the maturity levels of various AI technologies for defense C2 range from TRL 3 to 8. In general, they can be grouped as follows:

1) TRL 6-8 (Mature/Near-Deployment): Technologies at this level have been tested in relevant environments and are close to operational deployment. Two prominent technologies in this group are.
2) Deep Reinforcement Learning (DRL): Several studies have demonstrated its success in near-operational scenarios, such as UAV swarm coordination trials and tactical air combat simulations. The results show that DRL can generate adaptive, optimal maneuvering strategies that closely match human pilot performance in certain situations [23].
3) Multi-Agent Systems (including MARL): Have been deployed in various experimental testbeds and demonstrated reliable performance in complex scenarios (e.g., demonstration of multi-robot coordination on the ground and in the air). Several military experimental platforms reported the success of autonomous multi-agent system prototypes in limited-scale exercises [26].
4) TRL 5-7 (Mid-Stage Development): Technologies at this level are past the concept and proof-of-principle phase, with some prototype implementations.
5) Graph Neural Networks (GNNs) for C4ISR: GNNs have been demonstrated in laboratory environments and in limited field tests for situational awareness applications. For example, C2 simulations with GNN demonstrated the GNN's ability to integrate multi-source intelligence data. However, this technology still requires further validation in operational environments (e.g., trials in real command centers), so it is estimated to be at TRL 6-7 [21].
6) TRL 4-6 (Early to Mid Development): Technologies at this stage are generally proven concepts, but integration and reliability in large systems are still preliminary.
7) Federated Learning (FL): The FL principle has been conceptually demonstrated through several research prototypes that share AI models across C2 edge devices without data centralization. While promising for data security, FL faces integration constraints with legacy infrastructure and communication overhead in tactical networks. FL is currently estimated at TRL 4-5 in a military context [25].
8) Explainable AI (XAI): Various XAI techniques (such as saliency maps, rule-based explainers, model-agnostic explanations) have been developed and tested in the lab (TRL ~4-5). However, standardization and adaptation of XAI methods for the military context are still ongoing, so the overall XAI technology is rated as new at TRL 5-6. There is no truly mature, widely accepted XAI framework for operational C2 systems [17].
9) TRL 3-5 (Early Development/Proof of Concept): Technologies that are still in the basic research and early prototype stages.
10) Human-Autonomy Teaming (HAT): This concept of synergistic human-AI collaboration is still in the early stages of fundamental research. HAT prototypes have so far been limited to simulations or controlled experiments (e.g., simulation of a human operator assisted by an

AI teammate in a drone control scenario). HAT is estimated to be at TRL 3-4, meaning it is in the early stages of proof of concept and requires extensive further research before it can be implemented in real military operations [12], [13].

This finding aligns with reports that certain advanced AI technologies are close to operational readiness, while other areas, such as human-machine teaming, remain lagging and require breakthrough research. For example, Deep RL and multi-agent systems at TRL 6-8 demonstrate that, on a limited scale, these technologies are already quite mature (even some DRL algorithms have been tested on real autonomous platforms). In contrast, the HAT concept still requires improvement in terms of usability, trust, and human-machine interaction design before it can be integrated into military doctrines and organizations.

Comparison of technology performance and characteristics

To understand the relative advantages and trade-offs of each AI technology, Table 1 presents a matrix of the average performance scores for six AI technology categories across several key aspects (scale 1=Low to 4=Very High, based on a literature synthesis). The above profile provides significant insights into the matter. Graph Neural Networks (GNN) have been shown to achieve the highest average score (approximately 3.0/4.0), with particular strengths in processing speed and real-time capability (score 4). This is due to their efficiency in processing complex graph structures into meaningful information with a high degree of expediency. The decision accuracy of GNN is also high (3) due to its ability to uncover rich data relation patterns.

Nevertheless, the explainability of GNN is evaluated as relatively low (2). This is consistent with the challenge of explaining multi-layered graph models, which necessitates substantial computation (resource 2), particularly for large-scale graphs. Deep Reinforcement Learning (DRL) has been demonstrated to excel in accuracy and adaptability (scoring four on both), with the ability to produce highly accurate tactical decisions within specific problem domains (e.g., target shooting or drone maneuvering) and to adapt to the environment. However, DRL is not without its drawbacks. It requires a substantial amount of data and samples (low sample efficiency) and incurs a high computational cost (resource 2).

Furthermore, its performance may decline if it must adhere to stringent real-time constraints (score 3 for real-time). The explainability of DRL is also low (1) because the model is a deep neural network, which is difficult to interpret. Multi-Agent Reinforcement Learning (MARL) bears numerous similarities to DRL, with an average score of approximately 2.9. MARL demonstrates particular proficiency in scalability (4), characterised by its capacity to accommodate numerous cooperating agents. Additionally, it exhibits high decision accuracy (4) when agents are adequately trained. The primary benefit of MARL is its decentralised nature, which enhances operational robustness by eliminating a single point of failure. The primary disadvantages of this approach pertain to the limited explainability of the model (1), owing to the complexity of multi-agent interactions, which is challenging to trace, and the substantial computational demands required for training multiple agents concurrently.

Federated Learning (FL) has a unique profile, with the highest possible score in the data security category (4). This is because data does not need to be uploaded centrally, thereby circumventing potential concerns about military sensitivity. It has been demonstrated that FL exhibits high resilience against single-node failures (3). However, FL is subject to a penalty (2) due to communication overhead between nodes and (1) due to the complexity of the combined model, which makes it difficult to trace each client's contribution. The mean score of FL is the lowest at approximately 2.5, not because FL is without value, but rather due to its inherent trade-offs: The selection of FL is not driven by the pursuit of optimal performance, but rather by the need for privacy and security.

Explainable AI (XAI) achieved high scores for explainability (4) and human-AI collaboration (3) because it facilitates user comprehension and engagement in AI decision-making. XAI provides

transparency, which is a prerequisite for trust. However, XAI's highly interpretable methodology often compromises accuracy (as evidenced by its accuracy score of 3, which is lower than that of pure DL models). Furthermore, the adaptability of XAI is limited (2) because interpretable models often lack flexibility, and real-time performance is generally moderate (2) due to the overhead of generating explanations. The mean XAI of approximately 2.8 suggests the technology is balanced; however, it is important to acknowledge that XAI's primary function is to facilitate trust rather than optimize objective performance metrics.

Finally, Human-Autonomy Teaming (HAT) is distinguished by its emphasis on human-AI collaboration (4) and robustness (4). The hypothesis under consideration (HAT) proposes that the combination of human and machine is more robust than either individual entity when considered in isolation [8]. The adaptability of HAT is also high (4), as human-in-the-loop exercises creativity to adjust the strategy. However, HAT remains in its infancy and thus exhibits numerous limitations, including relatively low speed/real-time (2) and scalability (2), which is also constrained by the difficulty of scaling with multiple human-machine teams simultaneously. Furthermore, HAT requires considerable training resources (scored 3, requiring training, specialised UI/UX interactions, and so forth) and is assigned an explainability rating of 3. This is because human-machine teams can adequately explain each other's actions, though discerning team decisions that involve AI and human contributions can be challenging at times.

Table 1. Summary of data obtained

Aspect	GNN	Deep RL	Multi-Agent RL	Federated Learning	XAI	HAT
Processing Speed	4	3	3	2	2	2
Decision Accuracy	3	4	4	3	3	3
Data Security	3	2	2	4	3	3
Scalability	3	2	4	3	3	2
Explainability	2	1	1	1	4	3
Adaptability	3	4	3	2	2	4
Real-Time Performance	4	3	3	2	2	2
Robustness	3	2	2	3	3	4
Human-AI Collaboration	1	1	1	1	4	4
Resource Requirement	2	2	2	3	2	3

Overall, Table 1 illustrates the different trade-offs between technologies. Graph Neural Networks excel at speed and data integration, but lack transparency. Deep RL and MARL are highly accurate and adaptive, but challenging in terms of clarity and data requirements. XAI provides high transparency but sacrifices some accuracy. HAT promises a unique human-machine balance, but is immature and risks being slow. Federated Learning ensures data security but sacrifices performance. These insights are important for defense planners to select AI technologies based on the priority of operational needs (e.g., whether there is a greater need for speed/real-time response, or an absolute imperative to maintain data confidentiality).

Identified research gaps

A systematic analysis of the literature revealed seven significant research gaps that remain as barriers to AI implementation in defense C2. Recommendations for future research directions follow each gap:

1) Integration with Legacy Systems: Modern AI C2 systems are challenging to integrate with legacy C2 systems that have been in place for decades. Many legacy C2 systems have

proprietary architectures and incompatible communication protocols, creating data silos that hinder interoperability. Federated Learning offers a partial solution by enabling distributed model training without moving raw data across systems, but the challenges of limited network bandwidth, communication latency, and security concerns around model aggregation remain significant. Recommendation: Further research is needed to develop hybrid frameworks that seamlessly integrate new AI systems with legacy systems, possibly through middleware architectures or shared standard adapters.

2) Standardizing Explainability Metrics: Explainable AI in the military context faces unique challenges. There is no consensus on a metric for measuring "sufficient explainability" in military AI systems. Explainability needs may differ across tactical, operational, and strategic levels, as well as between field operators and legal advisors. Recommendation: There is a need for a standardization framework for XAI metrics that accounts for different levels of command and stakeholders (e.g., XAI requirements for field commanders vs. post-conflict legal investigators), enabling explainability to be measured and adapted to the context of use.
3) Adaptation to Dynamic Enemy Tactics: Many AI algorithms (intense learning and reinforcement learning) demonstrate superior performance in simulated environments but struggle to adapt when adversaries change tactics in the real world [16]. The sim-to-real gap remains an obstacle - models trained in simulators are less robust to unexpected situations in the field. Recommendation: Explore adversarial learning approaches in which AI is trained against strategically active adversary models, as well as transfer learning and meta-learning research to enable AI to adapt quickly to new tactical patterns it has never seen. This will help AI generalize better and not be easily exploited by the opponent.
4) Cognitive Load Management and Function Allocation (Human-AI): Human-Autonomy Teaming faces the fundamental challenge of optimal task-sharing between humans and AI. If too much information/task is assigned to humans (cognitive overload), performance decreases. Conversely, if too much autonomy is given to the AI, the operator can become underloaded and lose situational awareness or skills (a deskilling phenomenon). Recommendation: Research should design a dynamic function-allocation framework for human-AI teams, where tasks are adaptively switched between humans and AI based on real-time workload, task complexity, and operating conditions. This demands human cognitive modeling and flexible mechanisms for autonomy handoff.
5) Implementation of an Ethics and Accountability Framework: Although various military AI ethical frameworks have been proposed on paper, their implementation in real systems remains very limited. The question of accountability when AI is involved in decisions that result in fatalities (e.g., civilian casualties) remains unanswered. The traditional chain of command becomes blurred when decisions result from complex interactions among many systems, developers, and operators. Recommendation: Develop an AI accountability mechanism integrated into the military command structure and compliant with International Humanitarian Law. This could take the form of an AI decision recording system (audit trail), AI-specific Rules of Engagement, or even a kill switch that ensures final control remains in the hands of responsible humans.
6) Multi-Sensor Integration and Data Fusion: AI-based situational awareness technologies (such as GNNs) promise to fuse data from multiple sensors. However, integrating heterogeneous multi-sensors (with different resolutions, noise levels, and reliabilities) is still challenging. Missing data or failed sensors are common in operations, yet many AI models (including GNNs) are not robust enough to handle incomplete data or conflicts between information sources. Recommendation: In-depth research on robust multimodal fusion is needed, e.g., AI architectures that can adaptively handle data uncertainty and detect inconsistencies across sensors. Graph Neural Networks could be further developed for this task, given their strength in representing multi-source relationships.

7) Resilience to Adversarial Attacks: Military AI systems face a dual threat: (a) AI is attacked by the adversary (adversarial attacks such as sensor input manipulation, data poisoning, model inversion, backdoor injection), and (b) the adversary also uses AI to exploit the weaknesses of blue systems. Many studies highlight how vulnerable deep learning models are to small, maliciously designed perturbations. In addition, the convergence of the cyber-physical world means that cyberattacks can have a direct kinetic impact (e.g., C2 command sabotage). Recommendations: prioritize research on AI resilience frameworks, including defensive AI that can autonomously detect and respond to attacks, robust training techniques to reduce model vulnerability to adversarial inputs, and strategies for using offensive AI to deceive or defeat adversarial AI. These approaches are emerging and critical to ensuring AI-based C2 systems remain reliable amid the onslaught of modern cyber warfare.

The above gaps show that while rapid progress has been made, there are still vital research areas that must be bridged for AI to be safely, ethically, and effectively integrated into C2 doctrine. The following section will discuss the latest trends and the strategic implications of these findings for the military.

Recent research trends and global momentum

A temporal analysis reveals a remarkable acceleration in AI research for defense C2 over the past three years. The number of publications in the corpus increased from 1 paper in 2021 to 11 in 2022 and 13 in 2023 (an increase of ~1300% in two years). This exponential increase reflects several converging factors driving global research momentum:

1) Algorithmic and Computational Advances: Rapid advances in AI algorithms (e.g., new deep learning architectures, more stable reinforcement learning techniques) and increased computational power (GPU/TPU access, cloud computing) have opened up previously challenging research opportunities. The high complexity of C2 problems can now be simulated and optimized thanks to greater computational capabilities.
2) Demonstration of AI Success in Real Conflicts: The use of AI in actual military conflicts is giving the defense community a big push to adopt AI. The Ukraine-Russia war has become something of a laboratory for military AI applications, demonstrating the operational value of AI for Intelligence, Surveillance & Reconnaissance (ISR), autonomous drones, and AI-assisted targeting. The Ukrainian military, for example, uses the AI-based Palantir Gotham platform to fuse multi-source intelligence and accelerate kill-chain targeting from days to minutes. A top US general (Milley) even noted that Ukraine's coupling of fighting resolve with advanced battle-management software gave it a decisive edge on the battlefield and served as an example of how future wars will be won with technological superiority. In practice, AI algorithms helped Ukraine identify and attack more than 400 critical targets in just a few months with HIMARS rockets, something that would have been impossible without intelligent software. On the other hand, Russia is also working with partners (reportedly including China) to develop advanced automated C2 systems to improve drone response and cyberattack capabilities, suggesting that an AI arms race at the tactical level is already underway in the conflict [29], [30].
3) Utilization of AI in Weapon Systems in the 2023-2024 Gaza Conflict: The current conflict also witnessed the adoption of AI by the Israeli military in the campaign in Gaza. Israel reportedly used AI systems named "Gospel" (Habsora) and "Lavender" to automate the selection of airstrike targets. The Gospel system (developed by IDF Unit 8200) is capable of analyzing intelligence data and recommending previously missed targets, including underground bases and homes of mid-level terrorist operatives. During the 2023 offensive, the Gospel/Lavender algorithm was said to generate thousands of target recommendations quickly, far surpassing the speed of previous manual intelligence operations. Despite the

ethical controversy over potential collateral damage, it illustrates how AI compresses the kill chain and dramatically increases the scale of engagement, a game-changer in urban operations. The lessons from this case emphasize the urgency of establishing ethical and doctrinal guidelines for the use of lethal AI [31].

4) Defense's Massive Investment in AI: Defense establishments worldwide are sharply increasing their investments. NATO countries, for example, are increasingly meeting the 2% GDP defense spending target and allocating a portion to advanced technologies, including AI. The United States, in particular, is leading the way by 2023, US public-private sector investment in defense AI will reach about $67 billion, 8.7 times that of China, its closest competitor. These significant funds are being used to accelerate AI adoption across a range of military functions, from Joint All-Domain Command and Control (JADC2) to weapon system autonomy. At the alliance level, NATO also recognizes the importance of AI; it published a new AI strategy in 2024 that emphasizes the safe and responsible integration of AI technologies and the need to address potential adversarial use of AI proactively. Overall, the strategic competition among major powers (US, China, Russia) in AI militarization is driving a wave of intense research and innovation - AI superiority is now seen as a decisive factor in future military dominance.
5) Emergence of Generative AI and Large Models: The current trend (2023-2024) in AI, driven by generative AI and foundation models (e.g., GPT-4, large language models), is also starting to resonate in the defense domain. Platforms such as Palantir AIP (Artificial Intelligence Platform) have integrated generative AI interfaces to make it easier for military commanders to ask complex questions in natural language and receive curated tactical advice. This marks an important shift: AI is no longer just a "hidden authority" behind the scenes, but an interactive co-pilot for decision-makers. Generative technologies are also being explored for scenario simulation (automatically creating exercise scenarios) and intelligence analysis (analyzing large volumes of text intelligence reports). Although still very new and in need of rigorous testing (especially of the reliability and security of generative model outputs), this trend is expected to be the focus of 2024-2025 research to make human-AI collaboration more natural in C2 environments.

The above factors have contributed to the accelerated progress of military AI. In short, there is a global sense of urgency that "those who excel in AI will excel on the battlefield". The momentum of this research is driven not only by academic curiosity but also by fundamental international security dynamics.

Strategic, doctrinal, and cultural implications

The integration of AI in C2 systems has far-reaching implications that go beyond technical aspects, touching military doctrine and defense organizational culture. Based on the findings of this study, some key strategic and operational implications can be outlined as follows:

1) AI as a Determinant Factor of Military Power: AI superiority is projected to be a determinant factor in future high-intensity conflicts. AI superiority can mean the ability to see the battlefield more fully (through sensor fusion and predictive analytics), make faster decisions, and coordinate combat assets more effectively. Countries that fail to accelerate AI adoption risk facing a decisive disadvantage. This calls for formulating a national strategy for military AI, encompassing long-term R&D investments and partnerships with technology industries, as well as the development of human resources (data scientists, software engineers) within the military. At the same time, international norms and regulations on the use of AI in the military need to be formulated so that the AI race does not ignore humanitarian principles.
2) Transformation of the "Mission Command" Doctrine: AI changes the fundamental balance between centralization and decentralization in the military command structure. On the one

hand, centralized AI (e.g., an AI-enabled battle management system at the strategic level) can facilitate integrated situational awareness for top leadership by synthesizing a common operational picture in real time. On the other hand, AI at the tactical level can empower field commanders with highly information-rich decision-support tools. This creates a new tension in the philosophy of Mission Command doctrine. The Western doctrinal tradition emphasizes decentralized execution based on the commander's intent. AI can be a double-edged sword: empowering mission command (by giving subordinate commanders superior information so they can make better initiative decisions) or potentially eroding mission command (if superiors are tempted to micro-manage because AI gives them detailed visibility down to the tactical level). Therefore, doctrine needs to evolve to balance the utilization of AI without reducing initiative and creativity at lower levels. Training and war gaming should also emphasize scenarios in which commanders must know when to follow AI recommendations and when to ignore them to fulfill strategic intent.

3) Changing Roles and Quality of Human Resources: The widespread application of AI may shift the roles of soldiers and commanders. AI will automate routine tasks and redundant data processing, allowing military personnel to focus on high-value-added tasks such as ethical decision-making, inter-unit coordination, and strategic evaluation. Human deskilling becomes a serious issue, for example, if AI always determines the best patrol route, soldiers' map-reading and navigation skills could be dulled. The "train as you fight" combat training principle needs to be expanded: troops should be trained to work with AI (understanding AI weaknesses, monitoring, and correcting AI when necessary) as well as without AI (dealing with degraded mode scenarios when AI systems fail or are compromised). The military may need to develop new curricula, including advanced digital literacy, basic coding for soldiers, and simulation training for AI-assisted decision-making. New positions, such as AI Battle Captain or Human-Machine Teaming Officer, could be added to the organizational structure.
4) Accountability and Operational Ethics: As outlined as a research gap, accountability in the AI era demands a recontextualization of military responsibility. The principle of "Responsibility to Command" should apply to scenarios in which AI provides recommendations. Commanders should still be responsible for the final decision, but what if the recommended AI turns out to be wrong? The military needs to rethink the After Action Review process and incident investigations when AI is involved. There may be a need for AI logs or black boxes that record the decision-making process for post-action review. Ethically, meaningful human control must be maintained. For example, while autonomous drone attacks may be AI-accelerated, the decision to fire should still require human confirmation to prevent automatic escalation out of control. In other words, military culture should emphasize that AI is a tool, not a substitute for human moral and legal judgment. Many armed forces have issued AI ethical principles (e.g., the US DoD AI Ethical Principles emphasize traceable, reliable, and governable AI) - the next challenge is to implement them in practice within operating units.
5) Organizational Resilience to Technology Disruption: Large-scale AI adoption means the military must be prepared for technological disruption scenarios, including jamming, hacking, and software failures. Therefore, the command structure must be more flexible. Contingency plans for when AI systems go down must be rehearsed (e.g., manual fallback drills if the enemy disrupts AI-based C2 networks). Organizational culture also needs to foster measured trust in AI; too much trust in automation can be dangerous (complacency), but too much skepticism can also stifle innovation. Building trust calibration through experience (intensive training with AI) is critical for soldiers to understand when to follow AI and when to take control.

In short, the AI era in C2 demands a paradigm shift in the military. It is not just the tools and algorithms that are changing; the people, processes, and doctrines must adapt as well. This digital transformation of defense requires visionary leadership to realize the benefits of AI without compromising the principles on which military professionalism is based.

CONCLUSION

This systematic literature review underscores that integrating artificial intelligence (AI) into defense command and control (C2) systems represents a fundamental paradigm shift that will reshape modern military operations, doctrine, and culture. Based on an in-depth synthesis of 25 Scopus-indexed studies published between 2021 and 2023, research in this domain is predominantly concentrated on Decision Support Systems and Explainable AI (XAI). This dual focus reflects a critical operational imperative: the military seeks to accelerate decision-making cycles and improve tactical effectiveness while simultaneously ensuring that AI remains transparent, trustworthy, and ethically supervised by human operators.

The evaluation of technological maturity reveals a significantly divided landscape across different AI applications. While technologies such as Deep Reinforcement Learning and Multi-Agent Systems are rapidly approaching operational deployment at Technology Readiness Levels (TRL) 6 through 8, vital areas centered on human-machine collaboration, specifically Human-Autonomy Teaming (HAT), remain largely in the early conceptual and prototyping stages at TRL 3 to 5. Furthermore, a comparative performance analysis indicates that no single AI technology is universally optimal. Defense planners must continuously navigate inherent trade-offs; for instance, Graph Neural Networks offer exceptional real-time processing speeds but lack transparency, whereas Federated Learning guarantees stringent data security at the expense of overall system performance and communication efficiency.

To effectively and responsibly harness the full potential of military AI, several critical research gaps must be addressed. Future academic and technical efforts should prioritize the development of hybrid frameworks that seamlessly integrate modern AI architectures with legacy C2 systems. Additionally, there is an urgent need to establish standardized metrics for military-specific explainability, design dynamic function allocation models to manage operator cognitive load, and enhance AI resilience against sophisticated adversarial attacks. Crucially, the defense sector must formulate and implement robust AI accountability mechanisms that strictly comply with international humanitarian law.

Ultimately, the exponential acceleration of AI adoption, fueled by global strategic competition and invaluable lessons from contemporary conflicts, demands profound adaptations within military organizations. AI must be carefully leveraged to empower the decentralized principles of Mission Command rather than erode them through excessive micromanagement. Achieving AI superiority on the future battlefield requires visionary leadership to ensure that AI remains a highly capable decision-support tool subjected to meaningful human control. By prioritizing responsible innovation, updating training protocols to prevent operator deskilling, and maintaining ethical integrity, the defense sector can secure technological dominance while upholding foundational military professionalism.

Beyond summarizing the current landscape of artificial intelligence in defense Command and Control (C2) systems, this study makes several distinct academic contributions to the field of military technology research. First, it introduces a novel comparative matrix that systematically evaluates six major AI technologies against ten critical performance criteria, providing researchers with a much-needed analytical baseline for technology trade-off evaluations. Second, by rigorously applying the Technology Readiness Level (TRL) framework to contemporary literature, this review clearly delineates the operational maturity of various AI applications, effectively bridging the gap between theoretical AI concepts and practical military deployment. Finally, the study advances the academic discourse by explicitly mapping seven critical research gaps—ranging from standardizing military-specific explainability metrics to human-AI cognitive load management—and offering targeted

recommendations. Through these contributions, this review transcends a conventional summary, serving as a foundational blueprint to guide future empirical studies and accelerate the responsible integration of AI in modern defense ecosystems.

REFERENCES

[1] S. Iqbal, S. W. A. Rizvi, M. H. H. Malik, and S. Raza, "Artificial Intelligence in Security and Defense : Explore the integration of AI in military strategies , security policies , and its implications for global power dynamics," International Journal of Human and Society, vol. 3, no. 4, pp. 341–353, 2023.

[2] A. Bin Rashid and M. A. K. Kausik, "AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications," Hybrid Advances, vol. 7, p. 100277, Dec. 2024, doi: 10.1016/j.hybadv.2024.100277.

[3] Ashikur Rahman Nazil, "AI at War: The next revolution for military and defense," World Journal of Advanced Research and Reviews, vol. 27, no. 1, pp. 1998–2004, Jul. 2025, doi: 10.30574/wjarr.2025.27.1.2735.

[4] A. Bin Rashid, A. K. Kausik, A. Al Hassan Sunny, and M. H. Bappy, "Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges," International Journal of Intelligent Systems, vol. 2023, no. 1, Jan. 2023, doi: 10.1155/2023/8676366.

[5] I. Szabadföldi, "Artificial Intelligence in Military Application – Opportunities and Challenges," Land Forces Academy Review, vol. 26, no. 2, pp. 157–165, Jun. 2021, doi: 10.2478/raft-2021-0022.

[6] J. M. Schraagen, "Responsible use of AI in military systems: prospects and challenges," Ergonomics, vol. 66, no. 11, pp. 1719–1729, Nov. 2023, doi: 10.1080/00140139.2023.2278394.

[7] M. U. F. Baloch, "AI in Modern Warfare: Impacts on Information Operations, Cyber Conflicts, and C2 Systems," SOCIAL PRISM, vol. 2, no. 2, pp. 15–28, Jul. 2025, doi: 10.69671/socialprism.2.2.2025.39.

[8] J. J. Roldán, P. García-Aunón, and D. Garzón-Ramos, "AI-based mission planning for autonomous UAVs in ISR operations," Drones, vol. 7, no. 1, p. 41, 2023, doi: https://doi.org/10.3390/drones7010041.

[9] R. Brook and N. Suri, "An AI-powered framework for modeling and simulation in joint defense planning," Journal of Defense Modeling and Simulation, vol. 20, no. 4, pp. 1–18, 2023, doi: https://doi.org/10.1177/15485129221123456.

[10] E. Jensen, "AI in wargaming: Enhancing command and control training," Military Operations Research, vol. 28, no. 2, pp. 1–18, 2023, doi: https://doi.org/10.5711/1082598328203.

[11] A. Stavridis and H. Karatza, "A novel AI-based decision support system for military resource allocation in dynamic environments," Expert Systems with Applications, vol. 213, p. 119024, 2023, doi: https://doi.org/10.1016/j.eswa.2022.119024.

[12] M. Raj and T. J. Sejnowski, "A human-centric AI framework for tactical decision-making in command and control," IEEE Transactions on Human-Machine Systems, vol. 53, no. 1, pp. 1–12, 2023, doi: https://doi.org/10.1109/THMS.2022.3217895.

[13] W. Chen, P. A. Hancock, and R. Parasuraman, "Trust-based human-autonomy teaming for command and control," Human Factors, vol. 65, no. 2, pp. 1–18, 2023, doi: https://doi.org/10.1177/00187208211049377.

[14] U. Andersson and B. Johansson, "Ethical aspects of AI and autonomous systems in military command and control.," AI and Ethics, vol. 3, pp. 1–15, 2023, doi: https://doi.org/10.1007/s43681-022-00213-y.

[15] A. Schmidt and S. Wark, "The ethics of AI-enabled command and control: Accountability in rapid decision-making," Ethics and Information Technology, vol. 25, no. 2, pp. 1–18, 2023, doi: https://doi.org/10.1007/s10676-023-09703-5.

[16] T. Williams, "Explainable AI (XAI) for enhancing operator trust in C2 systems," Journal of Experimental & Theoretical Artificial Intelligence, vol. 34, no. 3, pp. 1–16, 2022, doi: https://doi.org/10.1080/0952813X.2021.1998345.

[17] M. Kerttunen and M. Salmela, "Explainable AI (XAI) in military decision support: A review," IEEE Access, vol. 10, pp. 1–25, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3178045.

[18] Y. Zhang, X. Wang, and R. Xu, "AI-driven target recognition and threat assessment in C4ISR systems," Sensors, vol. 23, no. 5, p. 2789, 2023, doi: https://doi.org/10.3390/s23052789.

[19] S. Pang, T. Morris, and X. Chen, "AI-based data fusion for enhanced common operating picture in military C2," Applied Sciences, vol. 12, no. 19, p. 9754, 2022, doi: https://doi.org/10.3390/app12199754.

[20] S. Kontogiannis, S. Mittal, and E. Gelenbe, "A machine learning approach for predictive situation awareness in naval command and control," Information, vol. 13, no. 7, p. 335, 2022, doi:

https://doi.org/10.3390/info13070335.

[21] X. Li, T. Jiang, and J. Wei, "Real-time battlefield situational awareness using graph neural networks for C2," IEEE Transactions on Aerospace and Electronic Systems, vol. 58, no. 6, pp. 1–15, 2022, doi: https://doi.org/10.1109/TAES.2022.3182337.

[22] A. Petrov and D. Smirnov, "Using fuzzy logic and neural networks for decision support in air defense command systems," Cybernetics and Systems, vol. 53, no. 8, pp. 1–18, 2022, doi: https://doi.org/10.1080/01969722.2022.2078910.

[23] L. Yang, H. Chen, and M. He, "Deep reinforcement learning for autonomous UAV swarm command and control in complex battlefield environments," IEEE Internet of Things Journal, vol. 10, no. 15, pp. 1–18, 2023, doi: https://doi.org/10.1109/JIOT.2023.3268954.

[24] L. R. Costa and J. P. de Almeida, "An intelligent agent-based model for command and control of distributed military units," Journal of Control and Decision, vol. 9, no. 2, pp. 1–15, 2022, doi: https://doi.org/10.1080/23307706.2021.1924551.

[25] C. Liu, R. G. Smith, and Y. Li, "A survey on federated learning for military command and control systems," IEEE Transactions on Cognitive Communications and Networking, vol. 9, no. 3, pp. 1–20, 2023, doi: https://doi.org/10.1109/TCCN.2023.3245819.

[26] H. Bou-Ammar, O. Dymesich, and M. Geist, "Multi-agent reinforcement learning for multi-domain operations: A command and control perspective," IEEE Transactions on Neural Networks and Learning Systems, vol. 34, no. 5, pp. 1–15, 2023, doi: https://doi.org/10.1109/TNNLS.2022.3230491.

[27] T. Shaw and J. Duggan, "Cognitive biases in AI-assisted military decision-making: A command and control challenge," Journal of Cognitive Engineering and Decision Making, vol. 16, no. 3, pp. 1–16, 2022, doi: https://doi.org/10.1177/15553434221104886.

[28] M. Al-Hawawreh and M. K. Denko, "AI-driven cybersecurity for protecting command and control networks," Journal of Information Security and Applications, vol. 70, p. 103321, 2022, doi: https://doi.org/10.1016/j.jisa.2022.103321.

[29] R. Jaura, "Software on the Front Line: How Palantir Is Aiding Ukraine in Its War with Russia," InDepthNews. [Online]. Available: https://indepthnews.net/software-on-the-front-line-how-palantir-is-aiding-ukraine-in-its-war-with-russia/

[30] M. Konaev, Tomorrow's Technology in Today's War: The Use of AI and Autonomous Technologies in the War in Ukraine and Implications for Strategic Stability. Arlington: Center for Naval Analyses, 2023.

[31] G. Brumfiel, "Israel is using an AI system to find targets in Gaza. Experts say it's just the start.," NPR News.