systems

MDPI

Review

AI Integration in Tactical Communication Systems and Networks: A Survey and Future Research Directions

Victor Monzon Baeza [1,*], Raúl Parada [2], Laura Concha Salor [1] and Carlos Monzo [1]

[1] Faculty of Computer Science, Multimedia and Telecommunications, Universitat Oberta de Catalunya, Rambla del Poblenou 156, 08018 Barcelona, Spain; cmonzo@uoc.edu (C.M.)
[2] Centre Tecnològic de Telecomunicacions de Catalunya, Av. Carl Friedrich Gauss, 7-Edifici B4, 08860 Castelldefels, Spain; rparada@cttc.es
* Correspondence: vmonzon@uoc.edu

Abstract

Nowadays, integrating Artificial Intelligence (AI) in military communication systems is reshaping current defense strategies by enhancing secure data exchange, situational awareness, and autonomous decision-making. This survey examines advancements of AI in tactical communication networks, including UAV networks, radar-based transmission, and electronic warfare resilience, thereby addressing a key gap in the existing literature. This is the first comprehensive review of AI applied exclusively to current tactical communication systems, synthesizing fragmented literature into a unified defense-oriented framework. A key contribution of this survey is its cross-sectoral perspective, exploring how civilian AI techniques are applied in military contexts to enhance resilient and secure communication networks. We analyze state-of-the-art research, industry initiatives, and real-world implementations. Additionally, we introduce a three-criteria evaluation methodology to systematically assess AI applications based on system objectives, military communication constraints, and tactical environmental factors, enabling a study of AI strategies for multidomain interoperability. Finally, we draft future research directions, emphasizing the need for AI standardization, enhanced adversarial resilience, and AI-powered self-healing networks. This survey provides key insights into the evolving role of AI in modern military communications for researchers, policymakers, and defense professionals.

Keywords: Artificial Intelligence; tactical communications; information network; improved tactical scenarios; defense

check for updates

Academic Editor: Francis Heylighen

Received: 27 July 2025
Revised: 21 August 2025
Accepted: 28 August 2025
Published: 30 August 2025

Citation: Monzon Baeza, V.; Parada, R.; Concha Salor, L.; Monzo, C. AI Integration in Tactical Communication Systems and Networks: A Survey and Future Research Directions. *Systems* **2025**, *13*, 752. https://doi.org/10.3390/systems13090752

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The integration of Artificial Intelligence (AI) into military communication systems, driven by the surge in data availability and computing power, is reshaping modern defense strategies and signaling a pivotal shift toward the convergence of military and civilian communications in the digital age. AI-driven advancements have demonstrated a transformative impact in civilian domains [1] from healthcare [2], transportation and manufacturing [3], including from ground to space environments [4], consolidating methodologies and standardized testing frameworks. However, in the military domain, there is a lack of a unified review that captures tactical communication advancements. Indeed, integrating AI into defense environments remains fragmented, underexplored, and hindered by operational and ethical challenges. To date, no existing survey has consolidated the full range of AI integration in tactical communication systems across all operational environments (land, sea, air, space, and cyber) into a unified framework. This survey bridges

that void. The full range of AI-enabled tactical communication technologies—spanning surveillance systems, radar, electronic warfare, Unmanned Aerial Vehicle (UAV), and information systems—has not been consolidated into a unified reference. All of them are required for military operations in multidomain interoperability, so a tactical-focused review is urgently needed.

Information and communication technology has been a fundamental pillar in pursuing safer environments in the military domain [5]. However, the same evolution has not been observed with AI. Despite the successes in civil environments, the military or tactical sector has been slower to adopt AI, hindered by unique challenges [6]. AI is pivotal in optimizing these systems by enhancing adaptive signal processing, facilitating multi-agent coordination for network resilience, and leveraging AI-driven electronic countermeasures. Regardless, military AI research remains fragmented despite these advances, with limited consolidation of existing methodologies and applications. Ethical concerns, such as the use of AI in autonomous weaponry, provoke global debates over accountability and morality. At the same time, the separation between civilian and defense communications limits opportunities to adapt proven AI methods for tactical purposes. Algorithmic biases, interpretability challenges, and regulatory hurdles compound these issues.

The reluctance to adopt AI in military contexts is evident in the lack of comprehensive studies to guide its integration. Unlike the civilian sector, military AI requires strict validation due to the high stakes involved. To address this, games and simulations have become valuable platforms for testing AI in realistic scenarios, advancing military research [7,8]. Emerging technologies like 5th Generation (5G) and Digital Twins (DT) also support this progress [9,10]: 5G enables real-time, low-latency communication, while DT enhances planning, predictive maintenance, and safe simulation [11]. These tools create a digital environment well suited for AI adoption in tactical communications.

Several leading nations already utilize limited AI in military operations, encompassing areas such as Intelligence Surveillance and Reconnaissance (ISR), logistics, and Command and Control (C2) systems to enhance security [12]. For example, the United States (U.S.) Army applies AI to optimize logistics and supply chains [13]. The Department of Defense's JADC2 initiative also seeks to connect sensors across military branches into an AI-driven network for better decision-making [14].

Closing the gap between civilian and military research enhances innovation and leverages existing expertise for defense applications. Civilian advances, like AI-based radar or machine learning in electronic warfare, can enhance tactical capabilities. Thus, a comprehensive survey of current AI applications in military communications is key to aligning both fields and guiding future research.

1.1. Related Works and Limitations

The first strategies for incorporating AI into this sector emerged in the 1990s in the U.S. [15]. Progress has been gradual, with various works contributing milestones toward AI integration in tactical communication systems, especially following a resurgence of interest around 2021. To date, none of these works offer a systematic survey, present or test modern AI techniques, or provide comparisons, highlighting the need for this review.

Starting with exploring AI techniques to enhance military simulations, ref. [15] focuses on terrain analysis to incorporate realism into training. Still, it is not until 2021 [16] that a significant leap occurs, marking a turning point where AI applications in defense begin to have a substantial and practical impact. The research progresses to broader analyses of AI's impact on military security [16], providing a tight view of AI's role in cybersecurity, logistics, and object detection. A shift toward specialized applications emerges with Deep Learning (DL) in Electronic Warfare (EW) [17], which reformulates traditional problems

using these AI models, debating the impact on tactical autonomy. This addresses the challenges of developing trustworthy, explainable AI systems for defense operations [18].

The focus expands to include modern warfare, targeting, cybersecurity, and military decision-making [19]. In 2023, AI and robotics were explored for defense decisions [20]. Naval forces are leading in adopting AI, focusing on autonomous systems for intelligence and surveillance [21].

The narrative continues in 2024 with the rise of trends in Unsupervised Learning (UL) algorithms and Machine Learning (ML) Operations (MLOps) techniques for defense, highlighting approaches to manage large, unlabeled datasets effectively in [22]. The strategic impact of AI and Large Language Model (LLM) on military and economic data analysis is examined in [23]. Human–AI collaboration in tactical planning and decision-making is explored in air battle systems as examined [24]. User trust and mental state tracking during cyber attacks are studied for the Royal Canadian Navy [25]. A focused review on AI in U.S. cyber warfare appears in [26]. Finally, Neuro-Symbolic AI has emerged as a key milestone, combining neural and symbolic reasoning to boost autonomy and military decisions [27], marking the evolution of AI in tactical operations.

The analysis of existing works reveals three persistent limitations in the current literature that this survey aims to overcome:

1. **Limited scope and fragmentation:** Most studies focus on isolated use cases such as EW [17], simulation [15], or mission planning [20], without providing a unified perspective across the full range of tactical communication systems. No prior survey has integrated AI applications across radar systems, surveillance, electronic warfare, UAVs, and information networks within a single defense-oriented framework.
2. **Conceptual or outdated approaches:** Many works emphasize theoretical or strategic constructs without recent empirical validation [16,18,19]. Several surveys do not reflect current AI capabilities, such as Generative AI (LLM) or Federated Learning (FL), which limits their applicability to modern defense scenarios.
3. **Lack of real-world connection:** While some papers explore technical innovations or ethical implications [23,25], they often lack operational insights, practical deployments, or industry-linked case studies. This disconnection between academic models and deployed defense systems leaves military professionals without actionable guidance.

In terms of comparison by technology and application areas shown in Table 1, our survey encompasses all branches of the armed forces (air, naval, land, and space), with a focus on communication systems, such as UAVs, radar, information systems, surveillance networks, and EW, as the foundation of the analysis. It highlights the five most widely used technology families that underpin tactical communications, as explained in the survey, as a reference and a contribution to previous works. Within the scope of this review—defense-domain, system-level tactical implementations (Q1 2025)—we did not identify published studies reporting end-to-end AI-assisted radar systems. Most available works are component-level algorithms rather than tactical, system-integrated deployments. Moreover, the key studies analyzed include future research directions, but they are now outdated (✗) [16,22,25,26]. While some are presented in survey format [20,25], they do not detail specific AI techniques as our proposed work does. It has also been noticed that most of the work is for the land army. Moreover, this work is designed for a broad technical and general audience, unlike previous studies that target particular specialties. As a result, it is relevant to both the military and civilian sectors, from academia to Industry.

Table 1. Coverage of defense AI characteristics in prior works and surveys vs. this work.

Ref.	Army/Defense				Tactical Technologies					Military Technological Description	Future Research Lines (Update ✓ or Outdated ✗	Survey Mode (Including AI Techniques)
	Air	Naval	Land	Space	UAV	Radar	Info Syst	EW	Surv. Image			
[15]	✓		✓				✓					
[16]	✓		✓								✓(✗)	
[17]								✓				
[18]	✓		✓									
[19]			✓					✓				✓(✗)
[20]	✓				✓					✓		
[21]		✓			✓				✓			
[22]			✓								✓(✗)	
[23]												
[24]	✓											
[25]		✓									✓(✗)	✓(✗)
[26]	✓	✓	✓		✓						✓(✗)	
[27]			✓									
[28]			✓									✓(✗)
This Survey	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓(✓)	✓(✓)

1.2. Scope and Contributions

This survey reviews AI-driven advances in tactical communications and fills a gap by integrating insights from civilian and military research. We introduce a framework, built on three key criteria, to evaluate system-level AI deployments in modern tactical networks. Radio-centric tasks (e.g., spectrum sensing, link optimization, interference identification) are excluded to keep the focus on system-level implementations. Our contributions include:

1. First integrated tactical AI survey across domains (civil–military): Unlike previous fragmented studies, this is the first to unify AI integration across all tactical communication subsystems (e.g., radar, EW, UAVs).
2. A framework without diluting focus with civil or generic AI applications, accessible to both defense experts and non-specialists.
3. Identifying how advanced AI methods from civilian industries can enhance tactical communications.
4. AI research status in tactical communications, serving as a foundational reference.
5. Assessment of defense industry projects: Reviewing major industry initiatives to demonstrate AI-driven tactical networking and military operations improvements.
6. Exploration of standardization and ethical challenges to contribute to the regulatory framework.
7. Future research directions: Identifying research gaps and outlining emerging AI trends to guide further advancements in resilient and intelligent military communications.

We clarify with respect to scope that the works are analyzed on system-level applications reported in the literature. This does not comprehensively analyze evolving standards (e.g., 5G-NTN/STANAG families) or radio/PHY/link-layer task taxonomies; these are acknowledged briefly for context and left to future, dedicated surveys.

This paper is structured as illustrated in Figure 1. After introducing the necessity and motivation for this study, we outline the information flow of the following sections. Section 2 provides an overview of AI concepts relevant to tactical applications. Section 3 introduces the five core communication systems prone to improvement with AI. Section 4 defines the novel proposed methodology for classifying the AI integration. Section 5 revisits the five systems, analyzing how AI is considered using the proposed methodology. Section 6 explores real-world defense initiatives incorporating AI in tactical communica-

tions. Section 7 consolidates insights from the previous sections. Section 8 highlights key challenges, emerging trends, and research gaps. Finally, Section 9 concludes this survey.

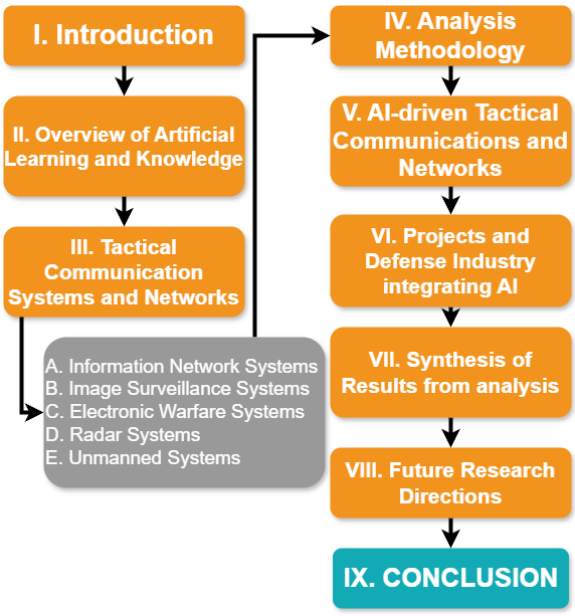


Figure 1. Structure of this survey.

2. Overview of Artificial Learning and Knowledge

AI technology is revolutionizing R&D and has brought a completely different perspective to wars and military strategies from the point of view of communication systems and networks using artificial knowledge. Its impact on warfare is so significant that it has redefined military theories and operational concepts [29]. AI explores areas like cognitive science and information processing, and its rapid expansion suggests it could transform the future of defense. The growing role of AI in military research highlights its dominance in the arms race, where machines will observe, orient, decide, and act autonomously [29]. AI-driven systems, whether operating independently on the battlefield or assisting commanders in decision-making, will be a game-changer in modern warfare.

2.1. Levels of Intelligence

Knowing the three levels of intelligence helps us understand AI in military systems: (i) The first level, cognitive intelligence, focuses on understanding, reasoning, and decision-making. It utilizes neuro-linguistic programming and, in some cases, surpasses human capabilities. For instance, AlphaStar has outperformed professional players in StarCraft II [30]. (ii) The second level, perceptual intelligence, involves sensory-based perception with subjective interpretation. While taste recognition is underexplored, the senses of sight, touch, hearing, and smell have undergone significant increases. Deep Neural Networks (DNN) and Big Data have revolutionized this area, outperforming humans in image recognition (Google Lens), facial emotion detection (Google Vision API), speech recognition (Windows Speech Recognition, Dragon Naturally Speaking) [31,32], and language translation with error rates around 5% [33]. These examples are helpful for military networks. (iii) The third level, computational intelligence, handles data storage and processing, where AI has far exceeded human capabilities. Focused initially on arithmetic and logic, it now includes learning, adaptation, and fuzzy logic. Modern supercomputers such as MareNostrum 5 (314 petaflops) [34], IBM Summit (200 petaflops) [35], and Tianhe-3 (1.3 exaflops) [36] exemplify this rapid evolution.

These three intelligence levels play a crucial role in military communications and networking. Cognitive intelligence enhances battlefield decision-making through AI-powered command and control systems, improving tactical awareness. Perceptual intelligence enhances real-time data analysis, signal recognition, and adaptive sensing, which are critical for electronic warfare, radar, and UAV-based surveillance. Computational intelligence enables high-speed data processing and secure information transmission, supporting encrypted military networks, distributed AI architectures, and resilient communication frameworks. The convergence of these AI-driven intelligence levels shapes next-generation defense communication systems, ensuring faster, more reliable, and adaptive military operations.

2.2. Method for Achieving the AI

AI achieves intelligence through solution search, knowledge inference, and machine learning, as detailed in [29].

Solution Search plays a crucial role in military communications and network optimization, helping to determine the most efficient routing, frequency allocations, and secure pathways for information transmission. AI-driven pathfinding algorithms analyze different states of a communication network, assessing factors such as signal strength, spectrum availability, latency, jamming risks, and operational constraints. In contested environments, AI enables real-time rerouting of data to ensure robust and uninterrupted military communication, adapting to electronic warfare conditions.

Knowledge Inference enhances situational awareness in military networks by enabling autonomous decision-making based on incomplete or uncertain information. AI inference systems process vast amounts of battlefield and network data to predict potential threats, optimize encryption protocols, and suggest adaptive defense mechanisms. For example, in electronic warfare scenarios, inference engines evaluate radio frequency patterns to detect jamming attempts and dynamically adjust cognitive radio networks to mitigate interference. The success of these inference models depends on their ability to search for patterns efficiently, establish causal relationships, and refine decision logic to ensure reliable and secure communication. AI inference for military networks faces two key challenges: (i) guaranteeing logical consistency when interpreting data from satellite feeds, radar systems, and encrypted transmissions, and (ii) minimizing computational overhead while rapidly adapting to dynamic combat environments. Rule-based AI supports expert-driven decision-making in C2 networks, while fuzzy logic enhances adaptability in autonomous UAV swarms, enabling resilient battlefield communications.

Lastly, ML revolutionizes military-grade network security, real-time signal processing, and predictive maintenance of defense communication infrastructure. ML-driven models analyze historical communication traffic to detect anomalies, such as cyber intrusions or unauthorized access attempts, and proactively reinforce defensive cybersecurity measures. In tactical edge networks, ML optimizes satellite link efficiency, predicts spectrum congestion, and assists in self-healing network architectures, ensuring military units maintain continuous and secure communication across multidomain operations.

2.3. Summary of Types of Learning

Extensive literature covers ML and learning types, as noted in [37,38].

- **Supervised Learning (SL):** The algorithm is trained with labeled data from known categories, enabling tasks like spam filtering, numerical value prediction (e.g., vehicle valuation), and data analysis from Internet of Things (IoT), social networks, or facial recognition, useful for tactical missions.

- **Unsupervised Learning (UL):** The system learns without labeled data, identifying patterns through grouping, visualization, dimensionality reduction, and association rules, widely used in data mining. Applications include person identification in image datasets, graphical representation of unlabeled data for traceability, user blog clustering, feature simplification, anomaly detection in production chains, and discovering relationships through association rules.
- **Semi-supervised Learning (SSL):** Used when most data are unlabeled, some partially labeled, and a few labeled. For example, the system groups photos where Person 1 appears (unsupervised) and, after tagging one, automatically labels the rest, simplifying the search.
- **Reinforcement Learning (RL):** This is based on observation, choosing a policy of action, and maximizing rewards or penalties. The vast majority of AI systems specialized in gaming use this approach.

On the other hand, algorithms can also be classified according to the availability of data, their generalization capabilities, or the number of layers required for learning.

- **Batch learning:** The system learns from all available data but always starts from scratch. If trained with 2000 samples, adding 500 more requires retraining with 2500 samples. This method, typically offline, demands significant computing power and time.
- **Online or incremental learning:** New data are continuously added, enabling immediate learning. Key benefits include memory efficiency (no need to store past data) and rapid change adaptation. However, errors in new data (e.g., faulty sensors) can degrade performance, requiring a rollback to a previous state. Commonly used in the stock market.
- **Instance-based learning:** The system learns from memorized examples and then discerns new incoming cases based on a measure of similarity.
- **Model-based learning:** It involves studying the data, selecting a model, training it to minimize a cost function, and applying the algorithm to predict new events.
- **Deep learning (DL):** It features multiple layers where parameters learn from preceding layers rather than directly from raw data. Each layer may use different ML techniques, typically Multi-Layer Neural Networks (MNN), mimicking the human brain in processing images, sounds, and texts.

3. Tactical Communications Systems and Networks

Before analyzing AI integration, examining the core military communication and networking technologies underpinning modern defense operations is crucial. This section outlines five key tactical communication technologies that shape military capabilities, providing context for their AI-driven enhancements. As shown in Figure 2, these include tactical information networks, image surveillance, EW, radar, and Unmanned Systems (USs).

3.1. Information Network Systems

Information systems are tools designed to collect, process, analyze, and distribute relevant information in real time or near real time within military or high-security contexts. Their primary goal is to provide commanders and operational units with accurate data to inform decisions during tactical operations, where speed and precision are crucial. Primarily, they are situated in C2 centers, serving as the starting point for tactical communications and networking for a mission. Information is power [39]. Accessing practical, accurate, and truthful information is the most critical factor in any decision, whether establishing a business plan or defining a military strategy (communications and networking). Since the

beginning, acoustic and visual signals have provided commanders with battlefield updates, evolving from horseback messengers with sealed letters to the invention of terrestrial radio communications, satellite links, and numerous other innovations in communication, all the way up to the present day.



Figure 2. Core military technological systems.

Data collection utilizes various sources, including sensors, drones, satellites, ground-based communications, and portable devices. The processing component analyzes large data volumes in real time to identify patterns, threats, or environmental changes. Information is shared through secure communication networks. For example, the Navy's LINPRO processor [40] facilitates real-time data exchange via protocols such as Link 11, Link 16, Link 22, Variable Message Format (VMF), or the Joint Range Extension Application Protocol (JREAP). These capabilities enable tactical information transmission over long distances, using satellite networks while aligning with North Atlantic Treaty Organization (NATO) standards like STANAG. A robust tactical information system must ensure scalability and adaptability for different operational scenarios, from ground to aerial or naval combat.

3.2. Image Surveillance Systems

An image surveillance system is a network technology designed to monitor, capture, and analyze visual data from strategic areas, enhancing situational awareness and decision-making. These systems use advanced cameras, sensors, drones, and satellite imaging to provide real-time or near-real-time visual intelligence, identify threats, track movements, and ensure perimeter security.

It was around 1969 when the first domestic closed-circuit television (CCTV) system was recorded [41], although similar systems had already been used in military projects years earlier. Technological advancements since then have been remarkable, improving image quality, incorporating infrared (IR) vision, enabling thermal data options, operating with servers and digital recordings, implementing facial recognition, motion-triggered pixel activation, vehicle license plate recognition, video tracking, and much more, as noted in [42]. All this technology has brought significant changes to surveillance systems, as the types of sensors used for data capture are highly diverse [43], and data-recognition and -processing software offer extensive capabilities. Fundamental for novel tactical wireless sensor networks.

3.3. Electronic Warfare Systems

EW uses technology to detect, exploit, disrupt, or deny an adversary's use of energy spectrums, like the electromagnetic spectrum, while securing its own [44]. It notably affects radio communications, surveillance radar, and electronic fire control systems.

Given the variety of scenarios and systems, EW is broadly classified into three main components:

- **Electronic Support Measures (ESM):** actions to search for, intercept, identify, or locate sources of emitted electromagnetic energy to gain immediate recognition of potential threats.
- **Electronic Countermeasures (ECM):** actions aimed at denying or reducing the enemy's use of the electromagnetic spectrum. This includes jamming, deception, and various decoys used for missile defense.
- **Electronic Protective Measures (EPM):** measures to ensure the reliable use of the electromagnetic spectrum for friendly forces, for instance, fire-control radars are equipped with frequency-hopping agility.

The origins of EW systems date back to the WLR-1, developed by the U.S. in the 1950s. Italy introduced the Beta Mk1000 in the 1970s, while Spain began its ESM development with the DENEB program in the 1980s. The Spanish Navy later equipped vessels with ALDEBARAN and REGULUS on F100-class frigates and RIGEL on LHD Juan Carlos I and BAM ships. Indra is advancing RIGEL i110 and REGULUS i110 for the next-generation F110-class frigates [45,46].

Most ESM systems share a typical architecture, including an operator console with a signal library, a signal-processing rack for analyzing intercepted signals, and a module on the superstructure for initial filtering and direction detection. The system also features three antennas: one omnidirectional and two directional, positioned on either side of the platform, to capture energy from different sectors.

3.4. Radar Systems

Military radars, like those in civil environments, detect, track, and identify distant objects by transmitting radio waves and analyzing the reflections. They are essential for surveillance, target acquisition, missile defense, navigation, and situational awareness in complex environments. Classified by function—search, tracking, or fire control—they enhance threat detection and operational effectiveness, even in adverse conditions. Radar is one of the most essential communication systems for military networks.

The British developed military radar in 1934 [47], leading to significant technological advancements. The basic design remains consistent, but progress has been made in antenna types, signal processors, radio frequency levels, oscillators, and classifications by technology (e.g., primary, secondary) or application (e.g., air traffic control, meteorology) [48].

One of the most advanced and versatile radars in the military domain is the SPY-7 developed by the American company Lockheed Martin, as presented in [49]. This S-band digital radar, built using gallium nitride solid-state technology, features a modular and scalable software-defined architecture. It can detect, track, and engage sophisticated ballistic missile threats, even simultaneously managing multiple targets. Moreover, it is interoperable with most existing defense radars and platforms. Since it is still under development, limited literature is available on the SPY-7. However, some insights can be drawn from its predecessor, the SPY-6.

The SPY-6 [50] is an Active Electronically Scanned Array (AESA) radar consisting of three main components: an S-band Air and Missile Defense Radar (AMDR) that provides volume search, missile tracking, and discrimination; an X-band AMDR, which provides horizon and surface search, precision tracking, and terminal illumination; and an AMDR Radar Suite Controller that coordinates and integrates both radars. This AMDR is the first radar built using $2' \times 2' \times 2'$ Radar Modular Assemble (RMA) building blocks, allowing for scalability and utilizing Gallium Nitride (GaN) in its construction to require less power and enhance cooling efficiency.

This radar supports digital beamforming for accurate tracking, a greater range, and 30 times the sensitivity of other radars. The SPY-6 also has offensive capabilities, conducting electronic attacks with its AESA antenna. It targets airborne and surface objects using focused, high-power radio wave beams that can blind adversaries.

Situational awareness in military contexts is crucial for tactical decision-making. A radar system is key in providing this information. In a recent case [51], an over-the-horizon radar system enhances detection accuracy and data features. However, optimization and detection processes lack AI methods.

3.5. Unmanned Systems

Unmanned Systems (USs) refer to vehicles, aircraft, or vessels that operate autonomously or remotely without a human onboard, both in military and civil contexts. Unmanned vehicles can be aerial (UAV, although if the control and communication system is included, it would be a Unmanned Air Vehicle (UAS), commonly called a drone), maritime (Maritime/Naval Unmanned Systems (MUS)), or ground-based (Unmanned Ground Vehicle (UGV)). Within this classification, a second subdivision can be made according to the type of mission assigned (surveillance, attack, suicide, etc.) or the type of technology applied (remote control, autonomous, fixed-wing, rotary-wing, etc.). Given that UASs have been making headlines in recent years due to technological advancements and their military use, it seems appropriate to focus this study on them. A diagram of drone terminology is presented to aid in understanding (see Figure 3).

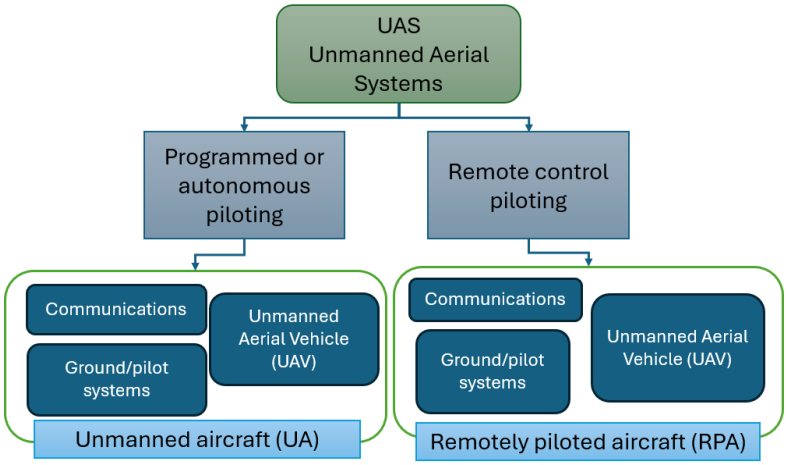


Figure 3. US terminology.

Unmanned aviation is as old as manned aviation. Still, in recent years, it has undergone the most significant evolution, mainly driven by new technologies, new materials, new energy storage systems, and the new roles these devices have played in the military world, according to reference [52]. The most notable projects are the Black Hornet 3 mini-drone from FLIR systems, for its surveillance capabilities, lightweight, and high-resolution camera, as described in [53]; the Turkish armed drone SONGAR, for its integrated 5.56 mm caliber weapon and its infantry support; and the American Predator C Avenger drone, for its reliability and its payload capacity for weaponry.

4. Analysis Methodology

The methodology applied in this survey to conduct the investigation is based on an analysis composed of three criteria, as shown in Figure 4, as follows:

- Criterion 1: Covers general data from the selected references.

- Criterion 2: Evaluate the notable and decisive factors relevant to the application in a military domain.
- Criterion 3: Assesses the critical tactical environmental factors affected by the application.

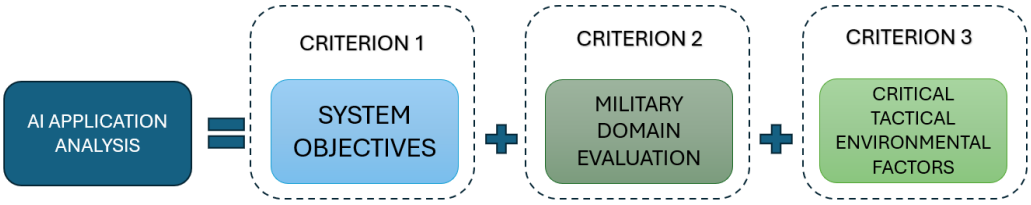


Figure 4. Three criteria-based methodology scheme used for reference analysis.

Before applying the proposed three-criterion framework, an initial search was conducted to identify relevant works for this review. The process and results are shown in Figure 5. First, we gathered publications using a pseudo PRIMSA method because the goal is to propose a new methodology, as explained below. The search on tactical communications and networked systems involving AI from major academic databases and institutional sources (IEEE Xplore, Scopus, Web of Science, MDPI, SpringerLink, and pre-prints, ResearchGate) with a search window through Q1 2025, returned 415 records. After removing duplicates, 109 unique references remained. Among these, we identified 13 studies categorized as surveys or reviews, which we later used for comparison in the Introduction. We filtered the 109 records separately to keep only those relevant to the five system domains analyzed in this study. To this number, we added 20 web-based references related to projects, companies, and standards, which were searched separately to help address research gaps identified in the review. Additionally, we included 11 references to show the basic system without AI.

Once the set of studies for review was selected, we applied the proposed methodology described in detail in this section. Each of the five technological systems presented in the previous section will be analyzed using this three-criteria approach through a series of tables. Consequently, the analysis of each system consists of three dedicated tables, one for each criterion. Combining these three branches creates a comprehensive framework for evaluation.

4.1. Criterion 1: System Objectives

General and foundational information is provided under this criterion, which is essential for any study. Figure 6 visually represents the concept map around "Criterion 1" that will later be used to define this criterion in detail.

These concepts classify the references under study as follows:

- **Application**: It aligns with the reference title and relates to this publication's purpose, answering what is intended to be achieved.
- **Objective**: implemented advantages, improvements, and procedures, detailing the steps to enable their application in tactical communication and networks.
- **Innovation**: It is helpful to determine whether the reference introduces any concept that has not been seen before or is seldom used, which might be worth noting.
- **AI Type**: Identify the type of learning model and the algorithm utilized. Adapting a commercial design for a defense system differs significantly when the developed algorithm operates offline and is non-incremental.
- **Training Data Information**: Understanding the training data is crucial, as it can be inadequate, gathered under controlled conditions, or specific to a scenario. This is vital for supervised algorithms, as the characteristics of the training data can limit the system's scope and applicability.

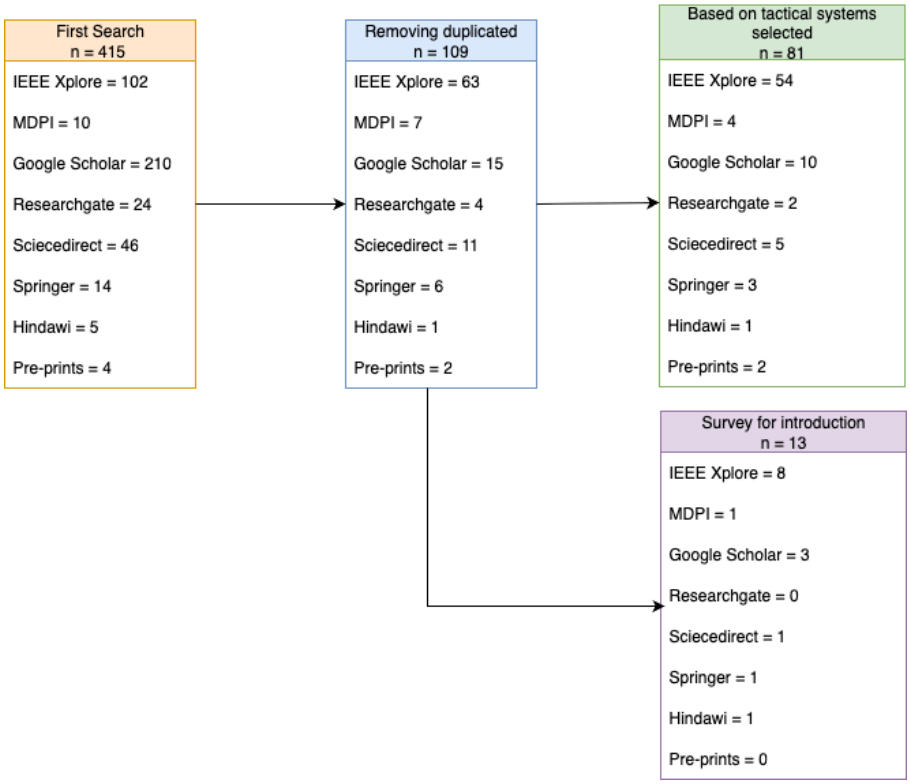


Figure 5. Pseudo PRISMA method results.

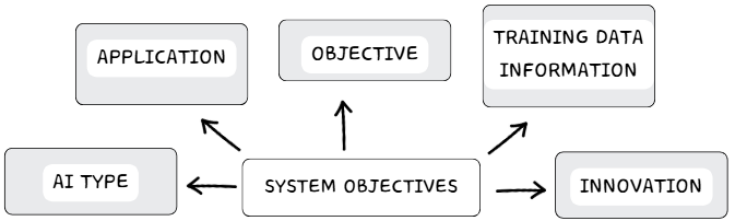


Figure 6. System objectives of the references.

4.2. Criterion 2: Military Domain Evaluation

The decisive factors, highlighted as "Criterion 2", require special attention when implementing a new technique in a system, as they help identify the algorithms' potential or limitations. Based on the literature review and assimilation of the data presented in the state of the art, the necessary background has been acquired to propose the observation of factors illustrated in Figure 7. These decisive factors must be considered when applying AI technology in military tactical environments:

- **Data Fusion**: These systems merge information and data from different sources and can process them comprehensively to obtain an accurate and reliable description of the environment. They can describe aspects of a target (speed, heading, size, armor . . .) or an event (involved personnel, security perimeter, topography, hostile areas . . .).
- **Tactical Scenario Inference**: The system must perceive and understand scenario elements, their spatial-temporal placement, and environmental intent. Modern warfare relies on integrated joint combat, coordinating soldiers, drones, tanks, aircraft, ships, and satellites. Combat is multidimensional, requiring commanders to access real-time battlefield data. Effective information processing and distribution across systems is crucial for operational success.
- **Command Assistance Element**: The decision support system consists of structured and unstructured components. The structured part involves human–machine interac-

tion and data processing, while the unstructured part addresses uncertain and complex scenarios where traditional models cannot effectively represent knowledge. Intelligent systems assist by analyzing warfare models qualitatively. As decision complexity grows, commanders will face an increasing gap between available information and their choices.

- **Offer Roadmaps against Threats**: AI assists in threat and obstacle avoidance, ensuring fast, efficient path selection. Current methods, such as genetic algorithms and dynamic planning, face challenges when extended to 3D scenarios, as large datasets slow convergence.
- **Ergonomic Human–Machine Interface**: Command interfaces should deliver timely, intuitive visual information over complex data tables, enhancing operator comprehension and decision-making.
- **Universal Language with Other Systems**: Unlike human languages in NATO operations, AI-driven machine language ensures seamless interoperability, reducing misinterpretations in multi-system environments.
- **Human Rules of Warfare**: While AI can enhance autonomy in tactical systems, critical war-related decisions must remain human-controlled, preventing reliance on purely rule-based learning.
- **Availability**: AI must ensure continuous system uptime and real-time data access; otherwise, its integration adds no operational advantage.
- **Resource Optimization**: Multi-dimensional combat generates vast data inputs, so AI must balance detail and efficiency to avoid unnecessary computational overload. For example, it would not be necessary to go into maximum detail of a war scenario, training the system with millions of variables, unless absolutely necessary, as this would slow down the system and increase resource consumption.
- **Scalability of Structures**: As warfare evolves, AI systems must adapt, integrating new actors, data, and strategies without performance degradation.
- **Integrity**: AI must detect data-manipulation attempts, ensuring consistency, validity, and security during training and operation.
- **Reaction speed**: AI's effectiveness in military operations depends on real-time decision-making; delayed responses negate its tactical advantage. The application of AI in military environments is justified if it improves the reaction speed of the command in response to a threat.

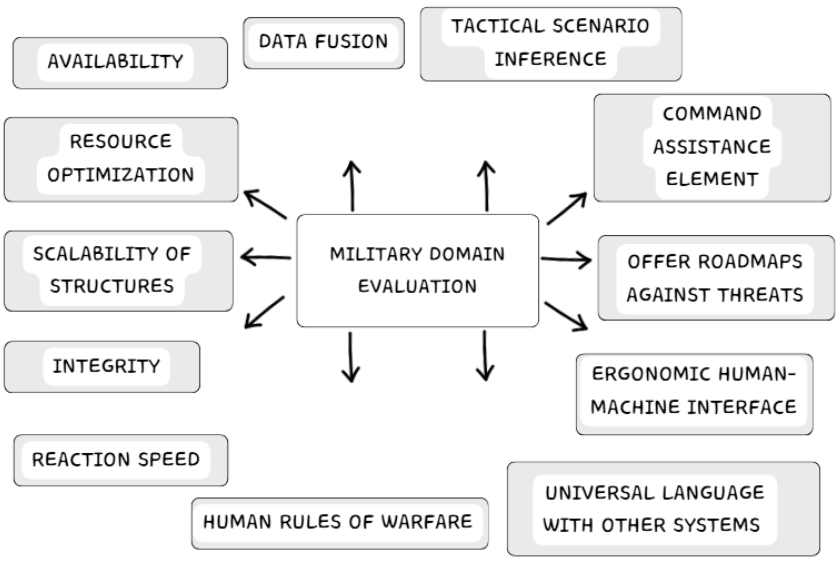


Figure 7. Key factors in applying AI in military domain evaluation.

4.3. Criterion 3: Critical Tactical Environmental Factors

When applying AI to military systems, assessing its impact on defense, particularly communications and networks, is crucial. Additionally, exploring new applications can reveal enhancements beyond a reference's initial focus.

Figure 8 illustrates military areas impacted by AI, including potential improvements identified through synergy and direct consequences for communication systems and networks.

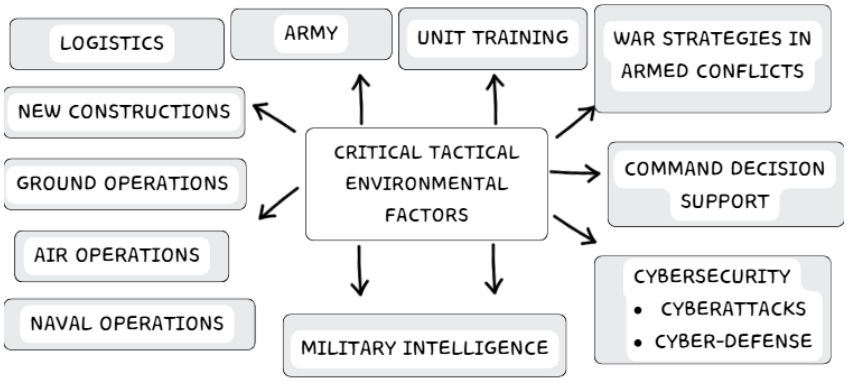


Figure 8. Key elements to evaluate critical tactical environmental factors.

- **Army**: The General Directorate of Armament and Material, under the Secretary of State for Defense, oversees defense projects, aligning military needs with broader defense policies. The army defines technical and operational standards for new systems across air, naval, and ground domains.
- **War Strategies in Armed Conflicts**: War strategy involves planning military campaigns and troop movements to defeat adversaries. According to International Humanitarian Law (IHL), armed conflict refers to large-scale confrontations causing destruction. This study examines how ML enhances military strategies when integrated into tactical systems.
- **Command Decision Support**: In potential conflicts, decision-making relies on a secure, collaborative power structure for effective horizontal and vertical communication. AI-driven systems enhance real-time data processing, ensuring timely and accurate decisions.
- **Cybersecurity—cyber attacks and cyber defense**: Recognized as the fifth military domain at the 2016 NATO summit, cyberspace spans battlefield sensors to C2 networks [54,55]. Traditional security measures (e.g., antivirus, firewalls) now integrate ML for intrusion detection, network access control, and data protection [56]. However, ML is dual-use, serving both cyber defense and offensive cyber attacks, while also being vulnerable to adversarial manipulation.
- **Military Intelligence**: AI processes vast military datasets (structured, semi-structured, and unstructured) to extract actionable insights. ML clusters intelligence from messages, identity records, and communications to detect military patterns. In aerial and space surveillance, computer vision enables target identification and tracking from satellite and UAV imagery.
- **New Constructions**: AI applications in warfare predictions may drive adversaries to develop unforeseen strategies and structures, exploiting weaknesses in trained models. AI also enhances manufacturing processes, such as DT simulations, to improve production efficiency.
- **Air Operations**: Conducted in the aerial domain, these operations involve highly mobile and flexible units for threat deterrence, rapid deployments, and strategic positioning.

- **Ground Operations**: The primary domain of human activity, hosting key political, economic, and strategic centers [57]. AI-driven analysis supports combat, defense, and stabilization efforts, securing military advantages while fostering conflict resolution strategies.
- **Naval Operations**: Naval forces provide mobility, availability, and interoperability [58]. Their planning and execution emphasize flexibility, goal alignment, security, and efficiency across various operational levels.
- **Logistics**: Military logistics involve supply transport, personnel movement, and equipment maintenance. AI optimizes fleet management, predicts anomalies, and improves resource allocation, generating economic savings and operational efficiency.
- **Unit Training**: Physical military training is costly and inherently risky. AI enables virtual and augmented reality simulations, allowing customized training based on individual combatant performance, improving readiness, and reducing risks.

4.4. Organizing Criteria Answers: A Tabular Approach

The different types of responses present in the tables of this work have been classified. Now, for the explanatory section, we describe each response type and its purpose:

- **Short Text**: Responses of brief description, typically model names, acronyms, or general categories. This is used when a concise label sufficiently conveys the information without additional explanation.
- **Descriptive Text**: a more detailed explanation is needed without being too lengthy, for example, in descriptions of methodologies or advantages of particular approaches: application and objectives descriptions, or complex descriptive key factors.
- **Yes/No**: Used for binary responses to indicate the presence or absence of a feature. This is useful for quick verifications, such as whether a model supports a specific functionality.
- **Numerical Values**: Quantitative indicators such as accuracy, success rates, or performance metrics.
- **N/A (Not Available)**: Used when information is unavailable and/or does not apply to the category. This is common in comparative tables when specific methods are not implemented across all technologies.

5. AI-Driven Tactical Communication and Networks

In this section, we revisit the military technologies and systems described in Section 3, incorporating advancements and considerations where ML has been applied to specific components. These updates align with the criteria outlined in the methodology, highlighting how ML enhances functionality and addresses challenges within these systems.

5.1. Information Network Systems

As presented in Section 3.1, information systems in tactical or military environments are critical tools designed to support decision-making and situational awareness, C2. These systems manage data from the rest of the systems compiled in this survey; therefore, they are fundamental in full tactical systems.

ML can significantly enhance these systems by automating complex decision-making processes, extracting actionable insights from large datasets, and adapting to evolving threats. Some benefits of incorporating ML include:

- **Enhanced Situational Awareness:** ML algorithms can process sensor data to identify patterns, detect anomalies, and predict adversarial actions, improving battlefield awareness.

- **Autonomous Systems:** ML enables autonomous drones, surveillance systems, and robotic units to operate with minimal human intervention from information systems.
- **Decision Support:** ML provides commanders with data-driven recommendations by integrating predictive analytics.
- **Cybersecurity:** ML fortifies systems against cyber threats by detecting and mitigating unusual network behaviors.

In addition, these benefits bring transformative advantages for information systems like C2, such as (i) speed, which accelerates decision-making by analyzing data in real time; (ii) accuracy, which reduces human errors in intelligence assessment; (iii) scalability, which handles vast amounts of data efficiently; (iv) adaptability which learns and evolves with new data to counteract emerging threats.

Various publications aim to improve information systems in military tactical environments by leveraging ML. Table 2 presents an analysis based on Criterion 1, highlighting the most relevant publications alongside the concepts discussed in the previous section and identifying the military areas they may impact focused on information systems. Table 3 provides an analysis based on Criterion 2, while Table 4 focuses on Criterion 3.

RL techniques have significantly enhanced tactical communication in information systems for modern warfare scenarios. RL-based algorithms optimize decentralized multi-agent communication within tactical networks, leveraging Cooperative Learning (CL) agents and tactical replay databases to manage critical metrics such as signal-to-noise ratios. In contrast, environment-dependent communication improves command support and scalability [59]. For the Internet of Battle Things (IoBT), ML classifiers like Support Vector Machines (SVM) and Random Forest (RF) prioritize battlefield data processing in C2, Communications, Computers (C4ISR), although the absence of comprehensive military datasets limits their optimization potential [60]. Similarly, ML models address spectrum scarcity in software-defined radio (SDR) applications, with Naïve Bayes and Gradient Boosting enhancing spectrum detection and resource allocation, albeit with constrained performance for wide-spectrum detections [61]. In predictive systems, Artificial Neural Networks (ANN) and DL forecast enemy movements, as demonstrated by augmented reality-enabled predictive mapping of naval adversaries. DL in enemy naval positions, trained on game-derived datasets, highlighting applications in forecasting adversarial intentions [62]. However, scalability and broader scenario adaptability remain challenges in [62]. RF-based warfare simulations analyze armored and naval combat, optimizing resource efficiency but lacking comprehensive environmental analysis or scalability [63]. The Tactical Assault Kit-ML (TAK-ML) framework, integrating battlefield sensors with ML, facilitates real-time data harmonization and secure communication, supported by TLS/SSL configurations [64]. Intelligent aerial combat maneuvers benefit from Long Short-Term Memory (LSTM)–Deep Q-Network (DQN) models, enabling precise short-range engagements despite speed limitations in deductive decision-making [65]. Hybrid RL and probabilistic approaches in missile defense systems enhance real-time efficiency and scalability, although they face challenges related to the unpredictable nature of attacking missile trajectories [66]. Reconfigurable Intelligent Surfaces (RIS) extend tactical wireless networks, boosting spectral and energy efficiency but requiring continuous Channel State Information (CSI) for optimal functionality [67]. Hybrid AI models combining Graph Neural Network (GNN) and Deep Reinforcement Learning (DRL) improve Quality of Service (QoS) in adversarial environments, advancing routing and adversarial flow management [68]. Finally, RL-based enhancements in C2 systems automate decision-making processes and enhance operational scalability, though the lack of strategic mapping remains a limitation [69].

Table 2. Criterion 1 for information network systems.

Ref.	Application	Objective	Innovation	AI Type	Training Data Information
[59]	Decentralized multi-agent architecture to optimize communication for military applications in DIL tactical networks using CL techniques enhanced with ML.	Decentralized reinforcement-based ML approach to enhance the network, where each node is optimized by a CL agent employing RL to act based on its local observations.	DIL Networks; C2IS service layers; GNN architectures.	RL based on CL observations.	The actions performed by tactical agents, as well as the SNR ratios calculated between each pair of units and positions, are stored in the Tactical Replay database.
[60]	Introduction of a ML classifier to determine what type of IoBT device data to transmit on the battlefield and under what conditions.	Transforming real-time data from C4ISR IoBT devices into secure, reliable, and actionable information, as IoBT devices must exchange data and receive feedback from other devices, such as tanks and C2 infrastructure in real time.	C4ISR devices, IoBT devices, JointField blockchain network.	SVM, Bayes Point Match, Boosted Decision Trees, Decision Forests, and Decision Jungles.	No specific military database was found. The study recommends conducting tests in a real-world environment.
[61]	Enhancing free spectrum detection using ML for SDR applications.	Providing flexibility and configurability to address spectrum scarcity in wireless communication systems.	SDR and CR networks.	Comparison of 4 supervised ML models: Native Bayes classifier, SVM, Gradient Boosting Machine, and Distributed Random Forest.	No specific military database was found.
[62]	Predicting enemy location in naval combat using DL.	Forecasting enemy naval positions and movements based on known locations.	Inferring adversarial intentions.	ANN and Random Forest implementations.	Models trained and tested with "World of Warships" gameplay data from former naval officers.
[63]	Warfare simulation to predict the winning warship using Random Forest.	Predicting the winner based on seven characteristics: size, speed, capacity, crew number, attack, additional attack, and defense.	OODA loop.	Supervised ML using Random Forest.	Using 9660 battleship datasets (7728 training—1932 testing).
[64]	Describing the TAK-ML framework for data collection, model building, and deployment in soldier-proximal tactical environments.	Exploiting battlefield sensor data to provide services for other applications.	Every Soldier is a Sensor (ES2), TAK ecosystems, SA.	TAK-ML harmonizes ML libraries, sensors, hardware, and applications on TAK servers.	TAK servers collect, fuse, and analyze data to enable ES2 battlefield operations.
[65]	LSTM-DQN algorithm and deep network to solve BVR maneuver planning issues.	Avoid enemy threats and gather advantages to threaten targets, enabling intelligent aerial combat.	BVR aerial combat; reactive and deductive decision-making.	DQN and Based on LSTM cells, where the perception layer converts basic states into high-dimensional SA.	Not specified.
[66]	Missile defense decision-making system in incomplete information scenarios.	Facing massive missile attacks in a short time frame.	N/A.	Hybrid method combining a prior probability hypothesis of attack and RL framework.	Recommends adding factors like missile angle and increasing missile/asset types and scales.
[67]	ML for RIS to enhance network capacity and coverage.	Maximizing wireless communication advantages with increased interactions.	Introducing RIS technology	SL, UL, RL, and FL.	Not specified.
[68]	Enhanced QoS of information operating in hostile environments that may host active adversaries	Improving QoS in tactical MANETs.	A hybrid AI model combining GNN and DRL	RNN, GNN, DRL	Not specified.
[69]	enhancing information in C2 systems under modern operations	automating and enhancing military decision-making in C2 systems.	decision-making with capabilities of RL.	RL	Not specified.

Table 3. Criterion 2 for information network systems.

Ref.	Data Fusion	Tactical Scenario Inference	Command Assistance Element	Offer Roadmaps Against Threats	Ergonomic Human–Machine Interface	Universal Language with Other Systems	Human Rules of Warfare	Availability	Resource Optimization	Scalability of Structures	Integrity	Reaction Speed
[59]	N/A	Environment-dependent communication.	Yes	Yes, decentralized architecture.	N/A	Yes, requires CL communication.	N/A	Varies by topology and link quality.	Yes, optimizes network use.	Yes, extends to nodes.	Nodes vulnerable to attacks.	Depends on nodes and CL.
[60]	Yes, large IoBT data.	Yes, prioritizes battlefield data.	Yes	No, lacks threat roadmap.	N/A	Yes, devices intercommunicate.	N/A	Decision Jungles are optimal.	Yes, filters massive data.	Yes, applies to scenarios.	Dynamic threat routes.	Decision Jungles optimal.
[61]	N/A	Yes, studies spectrum use.	Yes, finds free spectrum.	Yes, proposes zones.	N/A	Yes, 4 valid SDR algorithms.	N/A	Naïve Bayes preferred.	Yes.	Yes.	Yes.	Low for wideband.
[62]	Predictive map of enemy in AR.	Locates enemy.	40% prediction with 3 games.	Only predicts position.	Overlay AR map.	N/A.	Ex-officers' decisions.	ANN superior.	ANN superior.	6 ships, no unit expansion.	Study false signals.	ANN superior.
[63]	Needs 7 battleship features.	No scenario.	Missing factors.	No roadmap.	Win/loss only.	N/A	7 features based.	Simple algorithm.	Simple algorithm.	Future work.	Too few features.	Simple algorithm.
[64]	Shares map, chat, video in battle.	Depends on TAK-ML app.	Image recognition.	Terrain learning.	Visual apps.	TAK-ML info-sharing.	Depends on app.	Depends on coverage.	Harmonizes data.	Harmonizes ML and apps.	TLS/SSL in TAK-ML.	Depends on app and coverage.
[65]	Used in flight and motion models.	Basic combat model: flight, motion, missile.	Assists pilot.	Evades threats, guarantees position.	Graphical.	Automatic alternative.	Motion models, missile envelopes.	Short-range combat focus.	N/A	N/A	Calculates best tactics.	Slow if using deductive decisions.
[66]	Merge attack, defense, and missile layers.	Unknown missile distribution.	Attack alternatives.	Optimizes defense missile allocation.	Graphical.	Integrates defense system.	Needs asset list.	Hybrid method surpasses heuristic methods, DQN.	Uses only necessary defense.	Adapts to available missiles.	Low, missile distribution unknown.	Hybrid method enables real-time deployment.
[67]	RIS retransmits data.	Poor CSI must be addressed.	Extends battlefield wireless network.	N/A	N/A	Interacts with other systems.	N/A	Needs accurate channel info.	Improves energy efficiency.	Scalable RIS structure.	Enhances link quality.	Needs real-time data.

Table 3. *Cont.*

Ref.	Data Fusion	Tactical Scenario Inference	Command Assistance Element	Offer Roadmaps Against Threats	Ergonomic Human–Machine Interface	Universal Language with Other Systems	Human Rules of Warfare	Availability	Resource Optimization	Scalability of Structures	Integrity	Reaction Speed
[68]	Adversary flow data.	Active adversary data.	No specification.	Improves defense.	Graphical implied.	Must communicate with C2.	N/A	Not specified.	QoS optimization.	No	Predicted by network.	Slow info update.
[69]	From various operations.	Central C2 system.	Through C2.	Should consider it as C2.	C2 system.	Not specified.	N/A	Not specified.	No	Yes	Very robust.	Fast, real time.

Table 4. Criterion 3 for information network systems.

Ref.	Army	War Strategies	Command Support	Cybersecurity	Military Intelligence	New Constructions	Air Operations	Ground Operations	Naval Operations	Logistics	Unit Training
[59]	Land	Yes	Yes	Study node/CL manipulation	Yes	N/A	Possible, few nodes	Yes	Possible, few nodes	Yes	Yes
[60]	Land	Yes	Yes	Use game theory for data deception	Yes	N/A	N/A	Yes	N/A	Yes	Yes
[61]	Land	N/A	Yes, free spectrum system	Study spectrum manipulation	Yes, free spectrum system	N/A	Possible	Yes	Possible	Possible with fewer devices	Possible
[62]	Navy	Yes	Yes	False signals for deception	Prediction with satellite/UAVs	New naval platforms incentive	Algorithm modifiable	Algorithm modifiable	Yes	Yes	Yes
[63]	Navy	Yes, Random Forest 80% accuracy	Yes	N/A	Yes	New naval platforms incentive	Algorithm modifiable	Algorithm modifiable	Yes	Yes	Yes
[64]	Land	Yes, depends on application	Yes, depends on application	Study false signals or TLS/SSL enabled	Yes, depends on application	Yes, new applications possible	No, primarily	Yes	Yes, for asymmetric warfare	Yes, depends on application	Yes, depends on application

Table 4. *Cont.*

Ref.	Army	War Strategies	Command Support	Cybersecurity	Military Intelligence	New Constructions	Air Operations	Ground Operations	Naval Operations	Logistics	Unit Training
[65]	Air and Space	Yes, aerial strategy for missile launch	Yes, action plan for aircraft	Study interference in decision-making	N/A	N/A	Yes	Algorithm modifiable	Algorithm modifiable	N/A	Yes, adapts to simulations
[66]	Land	Yes, prioritize assets	Yes, missile allocation	N/A	Converge with military intelligence	N/A	Yes	Algorithm modifiable	Algorithm modifiable	N/A	Yes, adapts to simulations
[67]	Land	Yes, wireless network for battlefield info	Yes, real-time battle info	Study wireless interference	Yes, RIS with UAVs	N/A	Yes	Yes	Yes	N/A	Yes, train network usage for battle
[68]	Land	No	Yes	No	Yes	N/A	Yes	Yes	Yes	N/A	N/A
[69]	All	Yes	Yes	No	No	N/A	Yes	Yes	Yes	No	No

The studies [59–69] for information systems predominantly focus on ground and navy operations, with fewer addressing air and space systems as compiled in Table 4. Most references support systems for real-time command and battle information sharing. Diverse approaches, including using game theory for deception and studying spectrum manipulation, are considered for cybersecurity. Military intelligence emphasizes satellite or UAV data to enhance predictions and integrate intelligence into tactical decisions.

Maintenance, new constructions, and logistics are less frequently covered but include emerging technologies like DT [64] for maintenance and adaptable frameworks for logistic support. Some studies suggest unique methodologies like deception tactics using false signals or prioritization models for asset defense. A few highlight potential gaps, e.g., the absence of applications in asymmetric warfare scenarios.

We also highlight another work in our analysis. However, it is not included in the main tables, as these are preliminary proposals that do not yet consistently encompass the full scope of tactical communications and networking data. This is the case, for example, recent research efforts have started to investigate the application of blockchain technology in tactical networks [70], to enhance security in interoperability environments and safeguard information exchanged between allied coalition systems.

5.2. Image Surveillance Systems

An image surveillance system integrated with AI algorithms can detect anomalies, classify targets, and predict potential risks. Thus, it is critical for reconnaissance, battlefield monitoring, and securing military installations.

Nowadays, in the commercial world, surveillance systems are installed in companies or governments that utilize ML techniques [71]. For example, there are CCTV systems where the processing and control units apply methods such as facial recognition, fingerprint identification, and automatic detection of aggressive human behavior or theft. These systems can directly request the presence of state security forces in the area, among other applications. However, the reviewed literature contains very few specific references to defense systems. Therefore, the three most relevant studies have been selected. These studies would be highly useful in specific military environments. ML enhances military image surveillance by processing vast visual data, enabling:

- **Enhanced Threat Detection:** ML models, such as CNNs, can identify and classify objects like weapons, vehicles, or intruders in real time. For instance, ref. [72] utilized You Only Look Once (YOLO) version 2, YOLOv3, and Faster Region-based CNN (RCNN) Faster-RCNN for automatic weapon detection, demonstrating the potential for rapid and accurate threat identification using CCTV feeds.
- **Improved Accuracy:** ML aids in reducing false positives and negatives by learning from diverse datasets, including thermal and infrared images. Thermal imaging applications, such as those in [73], leverage models like YOLOv8, achieving a mean Average Precision (mAP) of 96%, even in challenging environmental conditions.
- **Anomaly Detection:** Algorithms like AutoEncoder (AE) can identify unusual activities or objects, enhancing perimeter security. This capability has been effectively demonstrated in radar-based applications [74], where noise-removal AE improved underwater image quality for better anomaly detection.
- **Operational Efficiency:** Autonomous systems, powered by ML, can monitor areas continuously with minimal human intervention, optimizing resource utilization. For example, the drone detection systems in [75] employed Faster-RCNN and YOLOv3 models to enable high-accuracy UAV tracking in diverse aerial scenarios.
- **Data Fusion and Tactical Insights:** ML enables the fusion of multimodal data, such as infrared and visible images, to provide more precise and informative surveillance

outputs. As shown in [76], Deep Supervised Generative (DSG)-Fusion techniques allow for integrating multiple image sources, aiding tactical scenario analysis.

- **Resource Optimization and Scalability:** These systems can scale efficiently to handle increasing data loads while maintaining high performance. For instance, ref. [77] demonstrated real-time military aircraft detection using TensorFlow-based CNNs on large annotated datasets, ensuring scalable and reliable surveillance operations.

These advantages make ML essential for modern military surveillance, tackling varied terrains, environmental factors, and emerging threats. New ML architectures, like Generative Adversarial Network (GAN) and advanced pre-processing techniques, facilitate the creation of robust, efficient, and scalable systems for military use. Incorporating ergonomic human–machine interfaces [75] and real-time alert systems [72] highlights how ML can comprehensively enhance military surveillance capabilities.

Various publications aim to improve image surveillance systems by leveraging ML. Table 5 presents an analysis based on Criterion 1, highlighting the most relevant publications alongside the concepts discussed in the previous section and identifying the military areas they may impact. Table 6 provides an analysis based on Criterion 2, while Table 7 focuses on Criterion 3.

5.3. Electronic Warfare Systems

ML has a wide field of applications in EW. Within the ESM field, it could automate the identification and search for radioelectric emissions by studying and learning the available libraries. In the ECM area, it could recommend the type of countermeasure the strategy to be used and, finally, related to EPM, based on the disturbance received, it could automate the frequency hopping of the agile frequency transmitting radars to avoid being canceled. Given that, incorporating ML in EW systems offers several significant advantages that can be summarized as follows:

- **Enhanced Threat Detection:** ML algorithms improve threat detection and classification by analyzing vast datasets to identify patterns and anomalies that may indicate hostile activities. This capability allows for real-time adaptive responses, improving the system's effectiveness in dynamic environments.
- **Automation:** ML facilitates the automation of signal-processing tasks, reducing the cognitive load on human operators and increasing operational efficiency. By learning from historical data, ML models can predict and counteract enemy tactics, providing a strategic advantage.
- **Adaptation:** ML-driven EW systems can continuously evolve, adapting to new threats and technologies without requiring extensive reprogramming. This adaptability ensures that military forces maintain a technological edge over adversaries.
- **Integration:** The integration of ML into EW systems supports the development of more sophisticated jamming and deception techniques, enhancing the ability to disrupt enemy communications and radar systems. ML significantly increases EW operations' capability, adaptability, and resilience.

Thus, different works in the literature aim to improve EW by leveraging ML. Table 8 presents an analysis based on Criterion 1, highlighting the most relevant works alongside the concepts discussed in Section 4 and identifying the military areas they may impact focused on EW. Table 9 provides an analysis based on Criterion 2, while Table 10 focuses on Criterion 3. Note that some of the publications presented show an N/A in some criteria due to their lack of relevance.

Table 5. Criterion 1 for image surveillance systems.

Ref.	Application	Objective	Innovation	AI Type	Training Data Information
[72]	Automatic weapon detection in real time using CCTV videos.	Balances real-time performance with accuracy.	ROI-based object detection.	VGG16, YOLOv3, YOLOv4, etc.	Custom dataset from web and videos.
[73]	Thermal human detection for security operations.	Achieves 96% mAP.	YOLOv8 for thermal imaging.	YOLOv7, YOLOv8.	Augmented thermal datasets.
[74]	Improving laser-coded images for underwater systems.	Resolves turbid environment challenges.	Noise removal autoencoder.	Shallow and deep networks.	Lab-collected images.
[75]	Autonomous drone detection and tracking.	High accuracy with optimized memory.	Unified Object Scale Optimization.	YOLOv3, Mask R-CNN.	Kaggle/custom drone images.
[76]	Fusion of infrared and visible spectrum images.	Texture retention in fused images.	Double-flow guided filter.	VGG, GAN.	Not specified.
[77]	Military aircraft detection for real-time surveillance.	Reliable under varying conditions.	TensorFlow-based pre-processing.	CNN.	Large dataset with annotations.
[78]	Foreign object detection in radio imaging.	Accurate in noisy environments.	YOLOv3 applied to radar images.	CNN, YOLOv3.	Synthetic RF radar images.
[79]	Military vehicle recognition using small datasets.	High resource demand for neural networks.	Transfer learning with ResNet50.	ResNet50, Xception.	Social media images with augmentation.

Table 6. Criterion 2 for image surveillance systems.

Ref.	Data Fusion	Tactical Scenario Inference	Command Assistance Element	Offer Roadmaps Against Threats	Ergonomic Human–Machine Interface	Universal Language with Other Systems	Human Rules of Warfare	Availability	Resource Optimization	Scalability of Structures	Integrity	Reaction Speed
[72]	Multi-angle images	Weapon occlusion issues	Defense system applications	Alerts in case of threat	Not indicated, but should be ergonomic	Associated with lighting/weapons	N/A	Real time	N/A	More classes needed	99% confidence score	Improve precision
[73]	Thermal imaging datasets	Robust in fog/smoke	Improves human detection	Enhances threat awareness	Interpretable thermal imagery	Security infrastructure integration	N/A	Real time with YOLOv8	Processing efficiency	Supports larger datasets	96% mAP	Real-time alerts
[74]	Laser images	Better scattering suppression	Enhances underwater imaging	N/A	Ergonomic and visual interface	Sonar compatibility	N/A	Improves image quality by 25%	Extends detection range in turbid zones	N/A	No behavior under disturbance	Not indicated

Table 6. *Cont.*

Ref.	Data Fusion	Tactical Scenario Inference	Command Assistance Element	Offer Roadmaps Against Threats	Ergonomic Human–Machine Interface	Universal Language with Other Systems	Human Rules of Warfare	Availability	Resource Optimization	Scalability of Structures	Integrity	Reaction Speed
[75]	Multi-frame fusion for drones	Effective in aerial scenarios	Enhances real-time drone detection	Warns UAV threats	User-friendly platform	Compatible with multi-sensor tracking	Designed for military compliance	High frame rate	Memory optimization	Tracks multiple drones	High UAV detection reliability	Low-latency detection
[76]	Infrared and visible fusion	Influenced by atmospheric conditions	Aids in target identification	N/A	Good visual interface	Fire control/CCTV application	N/A	Real time	N/A	Scales to CCTV systems	No countermeasures for heat deception	Low latency
[77]	Diverse perspectives	Aircraft detection in varied conditions	Precise localization	Aerial threat alerts	Simplifies detection	Coordinates with monitoring systems	Standards compliance	Rapid detection	Resource-efficient	Large-scale monitoring	Reliable in challenges	Fast processing
[78]	Radar imaging	Reliable in noisy environments	Detects concealed objects	Identifies explosives	Intuitive radar interface	Adaptable for radar warnings	N/A	Real-time imaging	Minimal dataset reliability	Various radar applications	Reliable detection	Quick response
[79]	Augmented datasets	Identifies vehicles in dynamic settings	Aids tactical decisions	Vehicle threat insights	Enhances situational awareness	Integrates with vehicle systems	Standards compliance	Real-time processing	Efficient dataset use	Scales to fleets	High accuracy in conditions	Minimal latency

Table 7. Criterion 3 for image surveillance systems.

Ref.	Army	War Strategies	Command Support	Cybersecurity	Military Intelligence	New Constructions	Air Operations	Ground Operations	Naval Operations	Logistics	Unit Training
[72]	Land	CCTV detects armed personnel.	Confirms threats using data.	CCTV dependent systems.	Aids monitoring in zones.	N/A	N/A	N/A	N/A	N/A	Systems trained for monitoring.
[73]	Land	Thermal systems detect threats.	Alerts for low visibility risks.	N/A	Identifies targets in fog.	N/A	Rescue aid in missions.	N/A	N/A	N/A	Thermal training improves.
[74]	Land	Supports command weapon data.	Improves tactical decisions.	N/A	Captures in turbid conditions.	N/A	N/A	N/A	N/A	N/A	Training for imaging systems.
[75]	Land	Tracks UAVs in combat.	Drone data aids command.	N/A	Predicts aerial threats.	N/A	Improves UAV usage in combat.	N/A	N/A	N/A	Drone training readiness.

Table 7. *Cont.*

Ref.	Army	War Strategies	Command Support	Cybersecurity	Military Intelligence	New Constructions	Air Operations	Ground Operations	Naval Operations	Logistics	Unit Training
[76]	Land	Captures clearer images.	Better tactical insights.	N/A	Alternate viewpoints support missions.	N/A	N/A	N/A	N/A	N/A	Operational training needed.
[77]	Land	Aircraft tracking aids ops.	Precise aerial surveillance.	Relies on secure channels.	Supports tactical analysis.	N/A	Insights for aerial ops.	N/A	N/A	N/A	Aerial imagery training.
[78]	Land	Radar images find IEDs.	Supports precise commands.	Enhances detection.	Tracks threats with accuracy.	N/A	Urban detection tools aid ops.	N/A	N/A	N/A	Improves system training.
[79]	Land	Vehicle ID in combat.	Better fleet decisions.	Secure data usage.	Military vehicle insights.	N/A	Scalable tracking systems.	N/A	N/A	Logistics aid fleet tracking.	Fleet-based training.

Table 8. Criterion 1 for electronic warfare systems.

Ref.	Application	Objective	Innovation	AI Type	Training Data Information
[80]	Integrated ML-assisted system.	Detect and combat hostile radars, ML to classify signals, CEW system.	Cognitive and multimode radar systems.	Automatic decision tree generator, diffuse logic model and LSTM.	Decision tree is automatically generated from simulated EW encounters and data.
[81]	3D Explorer Space Program to Simulate CEW Environments.	Stand-alone threat detection decision process, classification and countermeasure selection.	CEW tasks with DRL Algorithm.	Variational Bayesian method.	Deep Deterministic Policy Gradient Algorithm (DDPG).
[82]	Reduced electromagnetic wave shape model construction, for radar and EW simulations.	Improve computational efficiency of radar and EW simulations.	Coupling between representation and algorithms operating on representation.	Supervised and Unsupervised Machine Learning.	It is not contemplated. Underlying sources of error were identified.
[83]	CNN-based method for classifying radar interference signal.	1D-CNN designed to classify radar interference signals.	Siamese-CNN (S-CNN)	SVM, Decision Tree Classifiers, Logistic Regression and RF.	Limited training samples. A CNN-based simesan network.
[84]	ML-based GNSS models to improve robustness and position signal performance.	Deliver low-cost, high-performance solution.	Positioning, Navigation and Timing, Time to First Correction (TTFF)	213 application studies from 2000 to 2021. Mostly used RF, SVM, ANN and CNN.	
[85]	Two deep learning-based methods for predicting the proper interference technique.	DNN on manually extracted feature values from the PDW list and using LSTM that takes the PDW list as input.	Press Description Word (PDW), Long Short-Term Memory (LSTM).	DNN of different structures and LSTM.	Training data built from the library. Trained ML model to predict interference technique.
[86]	CNN-based radio fingerprinting.	Timely interception of tactical and strategic transmissions.	Transform the identification and classification of RF signals.	CNN.	IQ Data and Image Processing.

Table 9. Criterion 2 for electronic warfare systems.

Ref.	Data Fusion	Tactical Scenario Inference	Command Assistance Element	Offer Roadmaps Against Threats	Ergonomic Human–Machine Interface	Universal Language with Other Systems	Human Rules of Warfare	Availability	Resource Optimization	Scalability of Structures	Integrity	Reaction Speed
[80]	Yes, environments difficult to analyze.	Yes, systems must accurately model their environment.	Yes, system detects, acquires and follows goals, and guides the platform.	Yes, the Electronic Attack (EA) assessment model recommendations.	The interface is not specified by supposedly visual.	Yes, with other radar systems and countermeasures.	Observed radar threat level determined by distance and mode.	Satisfactory results in a simulated environment against multiple multifunction radars.	Better result with short-term memory neural network.	Yes, focus allows automatic updates in progress.	Each case was simulated 100 times and successful missions were recorded.	Depends on the distance at which the location of the threat is assumed.
[81]	UAV speed and direction of motion need to be controlled while verifying the integrity of the CEW system function.	You can search for the station in the mission map + Bayesian inference or applying evolutionary computing method.	Yes, to locate ground stations that are transmitting.	No, it is not contemplated.	No, it is not considered.	Both the UAV and ground station use radar-like observation sensors.	In this case, it is a game-like simulation.	Partial observability of the environment, and physical UAV maneuverability restrictions.	No, it is not considered.	Detection sensor modules and countermeasure weapons can be expanded.	The interaction between each part and the environment has a clear mathematical model.	UAV movement prioritizes physical restrictions of movement over CEW system operation.
[82]	Yes, there is a representative coupling of the sampled signal and morphism.	N/A	N/A	N/A	N/A	Seeks to formulate learning problem in a unified way to increase efficiency.	N/A	Loss of information due to morphism and error in the approximations of the supervised learning algorithm.	Yes, morphism avoids computational bottleneck.	Learning problem should be formulated in a unified way to increase the effectiveness of the outcome.	Worsens by being more truthful about sampled representations than morphism.	Improvement with approximate morphism based on features of a reduced model.
[83]	S-CNN to classify different interference signals with limited samples.	N/A	Yes, this electromagnetic signal classification method can give enemy information.	N/A	N/A	N/A	N/A	Yes, 1D-CNN experimental result. S-CNN result under limited training samples.	N/A	N/A	12 typical types of radar interference signals.	N/A
[84]	N/A	Yes, GNSS in both indoor and outdoor environments.	Yes, early detection of faults and errors can lead to timely correct it.	N/A	N/A	N/A	N/A	Reduce maintenance effort and downtime.	Yes, it is the goal with ML.	N/A	Sources of errors exist for satellite-based positioning.	Dependent, SVM speed does not meet the real-time requirements for interference monitoring.
[85]	Yes, ML model generates interference techniques for incoming threat signals.	N/A	Yes, predicts proper interference technique in the face of a threat.	Yes, suggest an interference technique before a threat.	N/A	N/A	N/A	Interference method can be predicted for unknown radar signal with an average accuracy of about 92%.	Yes, the predicted interference method will be used first.	N/A	Prediction accuracy of the LSTM model was higher.	DNN-based method is faster than LSTM method.

Table 9. *Cont.*

Ref.	Data Fusion	Tactical Scenario Inference	Command Assistance Element	Offer Roadmaps Against Threats	Ergonomic Human–Machine Interface	Universal Language with Other Systems	Human Rules of Warfare	Availability	Resource Optimization	Scalability of Structures	Integrity	Reaction Speed
[86]	IQ Data and Image.	Hybrid multi-level approach for fingerprinting and confirming transmitter identification.	Yes, confirming transmitter identification in a dynamic and wider spectrum.	Yes, identifying high-value targets and assisting in Identification Friend or Foe, anti-spoofing.	N/A	N/A	N/A	Presented concepts and solutions can be a game changer for both military and civilian use.	Yes, the hybrid approach reduces computational load.	N/A	Consistency in accuracy in SNR levels and BW. IQ and Image processing-based models showed an exponential decline in accuracy.	N/A

Table 10. Criterion 3 for electronic warfare systems.

Ref.	Army	War Strategies in Armed Conflicts	Command Decision Support	Cybersecurity	Military Intelligence	New Constructions	Air Operations	Ground Operations	Naval Operations	Logistics	Unit Training
[80]	Air and Space.	Yes, electromagnetic signal capture and classification is vital.	Yes, an imminent danger detected anticipates decisions.	N/A	Yes, although the algorithm collects real-time data there is a signal database.	Yes, new UAV capability and drives projects like NGJ-MB.	Yes	Could be applied.	Could be applied.	N/A	Yes, operator training would be convenient.
[81]	Air and Space.	Yes, ground station transmission detection-interference is vital.	Yes, an imminent danger detected anticipates decisions.	N/A	Yes, location of transmitting earth stations.	Yes, new UAV capacity.	Yes	Could be applied.	Could be applied.	N/A	Yes, operator training would be convenient.
[82]	Air and Space.	N/A	N/A	N/A	N/A	Yes, it could be considered in new radar and EW processing.	May be applied on radar and EW.	May be applied on radar and EW.	May be applied on radar and EW.	N/A	N/A
[83]	Ground.	Yes, signal classification gives enemy information.	Yes	N/A	Yes, signal classification gives enemy information.	N/A	Yes	Yes	Yes	N/A	N/A
[84]	Ground.	Yes, may cause interference with GPS signal from units.	Yes, an accurate signal is needed.	N/A	Yes, identifies unit positions.	N/A	Yes	Yes	Yes	N/A	N/A
[85]	Ground.	Yes, can cause radar interference or enemy EW.	Yes, it prepares interference system such as a pitcher.	N/A	Yes, it could be associated with the military and with the interference system.	N/A	Yes	Yes	Yes	Yes, you can predict which interference systems to have armed.	Yes, its use should be trained.
[86]	Air, Ground and Space.	Yes, interception of crucial tactical and strategic transmissions.	Yes, RF fingerprinting serves as a cornerstone in ensuring seamless operations.	Security and operational integrity by RF fingerprinting.	Yes, a comprehensive solution for fingerprinting and confirming transmitter identification.	Yes, considering the merits and drawbacks of previous approaches, a hybrid approach is proposed.	Yes	Yes	Yes	Yes, RF fingerprinting in fortifying security and operational integrity within the EW spectrum.	N/A

These publications collectively underscore the advancements in EW systems by integrating ML, improving decision-making, threat detection, and operational efficiency. An integrated ML-assisted EW system that autonomously navigates and assesses threats using cognitive and multimode radar systems is discussed in [80]. In [81], a 3D Explorer Space Program is presented for simulating CEW environments with UAVs, focusing on threat detection and countermeasure selection using DRL algorithms. Ref. [82] addresses the construction of reduced electromagnetic wave shape models to improve computational efficiency in radar and EW simulations. A Convolutional Neural Network (CNN)-based method is presented in [83] for classifying radar interference signals, emphasizing using Siamese-CNN for effective classification with limited training samples. Ref. [84] uses various ML techniques to explore ML-based Global Navigation Satellite System (GNSS) models to enhance signal robustness and performance in hostile environments. Deep learning methods are detailed in [85] for predicting interference techniques, employing Deep Neural Networks (DNN) and LSTM networks for accurate threat response. CNN-based radio fingerprinting is focused on [86] to intercept crucial transmissions and segregate radios based on significance, enhancing radio-frequency signal identification and classification.

The technologies used for EW systems integrate with or operate with the other systems, which is explained here. They are mainly combined with the radar system discussed in the following section.

5.4. Radar Systems

Radar systems have undergone significant advancements in recent years. Authors in [87] provide a comprehensive overview of AI approaches to enhance radar data-processing tasks. These approaches can refine existing methods or even replace conventional techniques with more powerful alternatives. For instance, this study [87] explores methods for identifying disruptions in air traffic control, distinguishing legitimate targets from parasitic echoes such as weather phenomena or bird activity. Additionally, it delves into marine environments, focusing on differentiating land clutter, calm sea clutter, rough sea clutter, and composite clutter.

From a radar signal-processing perspective, the authors in [88] analyze the role of ML in military services, among other applications. CNN and SVM are the primary techniques suggested for improving radar signal processing in these contexts.

Integrating ML into radar systems is not merely a technological advancement but a necessity to meet the challenges posed by modern operational environments. Traditional radar techniques, while effective, are often limited in handling the increasing complexity of tasks such as:

- **Clutter Suppression:** Conventional algorithms struggle to differentiate meaningful targets from environmental noise or clutter in dynamic scenarios like urban areas or rough seas. ML models, trained on diverse datasets, excel at recognizing patterns and suppressing noise, thus improving target detection accuracy.
- **Real-Time Adaptability:** Radar systems must adapt to rapidly changing environments, such as varying weather conditions or evolving combat scenarios. ML enables systems to learn and adjust quickly, enhancing situational awareness and decision-making capabilities.
- **Automation of Complex Tasks:** Modern radar systems handle large volumes of data, requiring efficient automation of tasks like anomaly detection, predictive maintenance, and data fusion. ML algorithms provide the computational power and intelligence to automate these processes without compromising accuracy.

We can find the following benefits of ML for radar systems:

- **Robust Performance in Complex Environments:** ML models can adapt to complex scenarios, including multi-path effects, electromagnetic interference, or high-clutter environments, maintaining high performance where traditional methods falter.
- **Enhanced Detection and Classification:** ML algorithms significantly improve the detection and classification of targets by learning from extensive datasets. This is particularly useful in distinguishing between similar objects, such as UAVs and birds, or identifying subtle changes in terrain.
- **Predictive and Proactive Capabilities:** Incorporating ML allows radar systems to predict potential issues, such as equipment failures or evolving threats, enabling proactive measures.
- **Increased Efficiency:** By automating repetitive or computationally intensive tasks, ML reduces the workload on human operators and accelerates processing speeds, making real-time analysis feasible.

In the field of radar systems, there is extensive literature on applications outside the defense domain. However, its application in this context is more limited. For this reason, we have focused in this work on its specific application in tactical environments and conducted a detailed study. Following the established criteria in Section 4 for analyzing ML applications in defense, the analysis for radar systems is summarized in Tables 11–13, corresponding to Criteria 1, Criteria 2, and Criteria 3, respectively.

Table 11. Criterion 1 for radar systems.

Ref.	Application	Objective	Innovation	AI Type	Training Data
[88]	Maintenance of air defense radar systems	Detect faults	Fault detection using multiple ML models	Random Forest, MLP, etc.	Data collected in faulty and normal states
[89]	SAR data analysis for HD imaging	Automatic target recognition	CNN for noise removal and segmentation	CNN, RNN, AE, etc.	Data augmentation for SAR-ATR
[90]	Radar resource management	Improve reaction time and integrity	Multifunction radar with adaptive features	CNN	Limited data from exceptional cases
[91]	Airborne target detection	Classify targets as fixed- or rotary-wing aircraft	Two-stage CNN for noise filtering	CNN	83,740 Doppler images
[92]	Radar scan clustering	Reduce dataset size	Density-based clustering algorithm	Unsupervised learning	Real dataset
[93]	MIMO radar waveform design	Improve localization and clutter mitigation	Deep residual network optimization	DL (CON model)	Adam algorithm with unsupervised COF
[94]	Pulsed Doppler radar detection	Improve CFAR performance	RadCNN for low SNR scenarios	CNN	182,000 files for training/testing
[95]	Situational awareness	Reduce radar cross-section processing time	Optimized ML-based clustering	K-Means	9 homogeneous and heterogeneous clusters

In [88], condition-based maintenance for air defense radar systems is explored utilizing a variety of ML models like RF, Multi-Layer Perceptron (MLP), and XGBoost to distinguish between malfunctions and normal conditions. Another reference, ref. [89] highlights using CNNs in Synthetic Aperture Radar (SAR) for automatic target recognition and classification of land types. Similarly, ref. [90] uses CNNs in radar resource management to enhance performance under high-target loads, while [91] focuses on improving the detection and classification of airborne targets using CNNs for real-time air traffic control. Other references also employ ML techniques, such as unsupervised learning and CNN-based detectors, to address issues like computational complexity, noise reduction, and radar accuracy in various operational scenarios. Ref. [93] focuses on developing unimodular waveforms for Multiple-Input Multiple-Output (MIMO) radar to enhance localization accuracy, clutter mitigation, and Doppler ambiguity reduction. It employs a deep residual network-based optimization

approach and uses the Adam algorithm for unsupervised optimization. A CNN-based detector called RadCNN is introduced in [94], replacing standard Constant False Alarm Rate (CFAR) detectors in pulsed Doppler radar. RadCNN improves performance in low Signal-to-Noise Ratio (SNR) scenarios with significantly reduced computational complexity, leveraging 182,000 training samples for evaluation. Lastly, ref. [95] discusses SAR in fighter aircraft by reducing the time complexity in processing radar cross-section matrices through optimized clustering techniques, utilizing methods like K-Means and Ellipsoidal Radar Cross Section (RCS) modeling to classify data into nine clusters.

Key highlights in Table 12 include data-fusion capabilities, with several approaches integrating multiple data streams and leveraging advanced ML methods, such as CNNs for SAR domains [89] and MIMO radars [90]. Tactical scenario inference is unevenly addressed; while ML aids in overloading scenarios [90], others focus on improving detection accuracy [94]. Command assistance is emphasized in systems improving target classification [91] or enabling real-time responses [94]. Resource optimization and scalability vary significantly, with some approaches emphasizing low computational complexity [94] or adaptive algorithms for efficiency [92]. Integrity and reaction speed are enhanced in systems using noise reduction techniques and high-performance ML algorithms [91,93]. Compatibility with other systems, ergonomics, and adherence to human warfare rules are less consistently addressed, highlighting lines for future advancements.

Table 13 summarizes radar systems' contributions to war strategies, decision support, and operational activities. Notable findings include the use of radar in air and space operations, often integrating advanced image processing, terrain analysis, and target identification techniques for command support and intelligence [89–91]. Some studies emphasize their ability to provide real-time data for secure decision-making [94], while others highlight specific adaptations for combat, such as handling rotary-wing threats [91]. Applications extend to logistics, unit training, and maintenance, although cybersecurity and new construction coverage is limited. Emerging research points to training requirements for algorithm use and deception strategies [92,93]. These systems enhance battlefield communication and precision, aiding pilots and operators in dynamic scenarios [88,95].

5.5. Unmanned Systems

Integrating ML into military drones will create a valuable weapon in armed conflicts. The ideal scenario in a land battle would be a swarm of economic, autonomous, stealthy mini-drones with enemy recognition and lethal capacity. There is still a long way to go before realizing that idea of science fiction. Still, there are already many ML studies to improve the reliability of UAVs concerning their performance and communication delays, the efficiency of resource management, and their performance based on their roles or missions, as seen in [96].

Table 12. Criterion 2 for radar systems.

Ref.	Data Fusion	Tactical Scenario Inference	Command Assistance Element	Offer Roadmaps Against Threats	Ergonomic Human–Machine Interface	Universal Language with Other Systems	Human Rules of Warfare	Availability	Resource Optimization	Scalability of Structures	Integrity	Reaction Speed
[88]	Yes, streams from different states	No	No	No	No	Yes, with EW	N/A	Medium	No	Future works	True positive rate: 0.84	N/A
[89]	Feasibility of transferring CNN learning to SAR	No, potential improvement	Yes, visual info for command	Continuation of development	N/A	Neural networks compatible with systems	N/A	Uses large-scale datasets	Feasibility of CNN learning in SAR	Video application possible	Testing of DL algorithms needed	N/A
[90]	Yes, MIMO radars	Yes, ML for overloaded radars	Yes, exploration system for ESM, EA, communication	N/A	N/A	Yes, integrates ESM/EA	Yes, EA-specific	Low, no physical testing	Radar has multiple functions	N/A	Yes, ML improves integrity	N/A
[91]	Two-dimensional radar, single/series pulses	N/A	Yes, identifies aircraft type	N/A	Two-stage noise removal	N/A	N/A	Higher, reduces filtering stages	Eliminates CFAR/peak detection	N/A	96% target hits, 85% noise	Higher, discards 30% noise
[92]	PDF projects dataset into 1D space	Adaptive cluster extraction	Yes, dense target info extraction	N/A	N/A	N/A	N/A	Higher, reduces time	Determines parameters for clustering	N/A	Efficient density-based scanning	Fast adaptive mean-shift algorithm
[93]	MIMO radar waveform facilitates implementation	N/A	Yes, improved waveform adds capabilities	N/A	N/A	Yes, integrates communication systems	N/A	Superior performance, acceptable optimization time	Solves waveform design problem	Possible use in warfare	Waveform enhances integrity	Feasible within computational complexity
[94]	N/A	Yes, affects detection results	Yes, real-time response	N/A	Real-time noise filtering	N/A	N/A	Outperforms CFAR techniques	RadCNN reduces complexity	N/A	RadCNN superior to state-of-art	Real-time feasibility
[95]	Single data stream	Full SA	No	Yes	No	No	Full	No	No	No	Residual error: 118807.63	N/A

Table 13. Criterion 3 for radar systems.

Ref.	Army	War Strategies in Armed Conflicts	Command Decision Support	Cybersecurity	Military Intelligence	New Constructions	Air Operations	Ground Operations	Naval Operations	Logistics	Unit Training
[88]	Air	No specified	Yes, evaluation of an air defense system	Not included	No	No	Yes	No	No	N/A	N/A
[89]	Air and Space	Yes, they depend on the images.	Yes, decisions based on images.	It will depend on the location of the data processor.	Yes, image segmentation, change analysis, terrain analysis.	N/A	Yes	Yes	Yes	N/A	Yes, its use should be trained.
[90]	Air and Space	Yes, ESM and EA.	Yes, exploration and communication.	N/A	Yes, database.	N/A	Yes	Yes	Yes	N/A	Yes, its use should be trained.
[91]	Air and Space	Yes, the presence of many rotary-wing enemies (including UAVs) changes the command strategy.	Yes, different ways of attacking fixed-wing to rotary-wing targets.	N/A.	Yes, identifies the type of aircraft.	Yes, implies new developments to avoid such classification.	Yes	Yes	Yes	N/A	Yes, its use should be trained.
[92]	Air and Space	N/A	Yes, identifies targets in dense areas.	N/A	N/A	N/A	Yes	Yes	Yes	N/A	Yes, the way to deceive the algorithm could be trained.
[93]	Air and Space	Yes, it can provide communication in battle and greater precision.	Yes, greater security in decision-making.	N/A	Yes, more accurate information.	N/A	Yes	Yes	Yes	N/A	Yes, the way to deceive the algorithm could be trained.
[94]	Air and Space	N/A	Yes, real-time information.	N/A	Yes, more information available with less SNR ratio.	N/A	Yes	Yes	Yes	N/A	Yes, the way to deceive the algorithm could be trained.
[95]	Air	Pilots to assess, anticipate, and respond adeptly to dynamic combat scenarios.	Help to Pilots	No	No	N/A	Yes	No	No	N/A	N/A

Therefore, ML has revolutionized the capabilities of US in military contexts, offering significant advantages in terms of efficiency, decision-making, and operational effectiveness. Some benefits of incorporating ML include:

- **Enhancement of Autonomous Decision Making:** ML algorithms enable US to process large amounts of data in real time, allowing rapid and accurate responses to dynamic battlefield conditions. This capability reduces the reliance on human operators and improves the speed and precision of military operations.
- **Predictive Maintenance:** ML models can analyze data from various sensors to predict equipment failures before they occur, thus reducing downtime and maintenance costs. This predictive capability ensures that US remains operational for extended periods, increasing their availability and reliability in critical missions.
- **Operation:** By integrating data from multiple sources, such as satellite imagery, radar, and on-ground sensors, ML algorithms can provide a comprehensive and coherent picture of the operational environment. This improved situational awareness is crucial for mission planning and execution, enabling more informed and effective decision-making.
- **Adaptation:** ML contributes to developing adaptive and resilient systems. The US, equipped with ML, can learn from past experiences and adapt its behavior to new and unforeseen challenges. This adaptability is essential in complex and unpredictable military environments, where static programming may fall short.

Integrating ML into unmanned military systems offers substantial benefits, including enhanced autonomous decision-making, predictive maintenance, improved situational awareness, and adaptive capabilities. These advancements increase the effectiveness and efficiency of military operations and contribute to the safety and success of missions.

Thus, different publications aim to improve the US by leveraging ML. Table 14 presents an analysis based on Criterion 1, highlighting the most relevant publications alongside the concepts discussed in the previous section and identifying the military areas they may impact, focused on the US. Table 15 provides an analysis based on Criterion 2, while Table 16 focuses on Criterion 3. Note that some publications presented show an N/A in some criteria due to their lack of relevance.

These works highlight the advancements in the US by integrating ML and improving decision-making, communication, and operational efficiency. Ref. [96] focuses on overcoming challenges in UAV mobility, communication, resource management, and security using ML techniques like ANN, CNN, DNN, SVM, and DQN to ensure QoS and Quality of Experience (QoE) in Aerial to Aerial (A2A), Aerial to Ground (A2G), and Ground to Aerial (G2A) communications. The classification of drones using radio-frequency signals with a Hybrid Model featuring a Feature Fusion Network (HMFFNet), employing CNN for feature extraction and SVM for classification, and capturing features with a DL architecture Visual Geometry Group (VGG), within this group, VGG19 in a network is discussed in [97]. Ref. [98] describes an architectural design for automatic AV behavior generation, using a modular behavioral block framework for scalable decision-making, integrating tactical and strategic behaviors with a Behavior-Based Hierarchical Arbitration Scheme.

Table 14. Criterion 1 for unmanned systems.

Ref.	Application	Objective	Innovation	AI Type	Training Data Information
[96]	Overcoming the mobility, communication, resource management and security challenges.	ML focused on meeting network requirements, taking into account the roles, collaboration, cooperation, and changing contexts.	Study A2A, A2G, and G2A communications to ensure QoS and QoE.	Algorithms like ANN, CNN, DNN, SVM, DQN, RandF, KNN are analyzed depending on the type of A2A, A2G, and G2A communication.	Not determined as it is an analysis and collection of different research.
[97]	Classification of drones using radio frequency (RF) signals.	Use of RF signals for drone detection with specific frequency ranges.	Hybrid Model with Feature Fusion Network (HMFFNet).	CNN-based feature extraction followed by feature fusion and SVM-based classification.	Features captured with a Deep Learning VGG19 network and sorting done with SVM.
[98]	Architectural design for automatic AV behavior generation.	Widespread and scalable decision-making framework.	Tactical and Strategic Behaviors in Automated Driving.	Behavior-Based Hierarchical Arbitration Scheme.	Database containing a merged and abstract representation of available sensor data.

Table 15. Criterion 2 for unmanned systems.

Ref.	Data Fusion	Tactical Scenario Inference	Command Assistance Element	Offer Roadmaps Against Threats	Ergonomic Human–Machine Interface	Universal Language with Other Systems	Human Rules of Warfare	Availability	Resource Optimization	Scalability of Structures	Integrity	Reaction Speed
[96]	Alternatives to ad hoc flying networks, caching or UAV processing.	Needed awareness of context changes and adaptability to current service requirements.	Yes, overcoming the 4 challenges already described.	A2A communications (participation threshold based on energy, capacity, mobility) and A2G communications (interference management and spectrum mapping).	N/A	Yes, the UAV network and base stations should be understood.	N/A	ML is a suitable solution for a dense and dynamic environment.	Yes, ML is the right tool for predicting context changes and optimization.	Yes, it should be adapted to the number of UAVs, mobility, communication, resource management, and security.	Dependent on performance, communications delays, and resource management efficiency.	It will depend on the functions and missions entrusted.
[97]	Yes, the characteristics of the 3 stages are merged for better discriminatory property.	N/A	Yes, it is another sound, image, or radar classification.	N/A	Not specified but should exist.	If you want to automate the defense process.	N/A	High.	Yes, audio, image or radar sensors are not required.	N/A	Could be altered with electronic warfare and assume a fake drone.	Fast

Table 15. *Cont.*

Ref.	Data Fusion	Tactical Scenario Inference	Command Assistance Element	Offer Roadmaps Against Threats	Ergonomic Human–Machine Interface	Universal Language with Other Systems	Human Rules of Warfare	Availability	Resource Optimization	Scalability of Structures	Integrity	Reaction Speed
[98]	Merges information from all available sensors.	Contains a fused, tracked, and filtered representation of the world.	Yes, because AV would be autonomous.	A cost-based arbitration scheme is useful when multiple behavioral options are applied.	N/A	The same language between all sensors and the autonomous system.	It contains parking and emergency behaviors and prevents indefinite states.	Robust and efficient modular system.	Human resources would not be necessary.	Structure designed for cars in cities and roads, but could be extended to military vehicles in areas of operation.	Supports different planning approaches.	Immediate to avoid an accident.

Table 16. Criterion 3 for unmanned systems.

Ref.	Army	War Strategies in Armed Conflicts	Command Decision Support	Cybersecurity	Military Intelligence	New Constructions	Air Operations	Ground Operations	Naval Operations	Logistics	Unit Training
[96]	Earth or Air and Space.	Yes, it could be a network of connected UAVs locating real-time targets.	Yes, it will depend on the use of UAVs.	It is necessary to have an autonomous defense system that guarantees the integrity, confidentiality, and availability of the data.	Yes, if it applies to recognition work.	Yes, the UAVs network study may be an inducement for new construction.	Yes	Yes	Yes	The transport of information data affects this area.	Yes, it is necessary to train the use of these networks and their defense.
[97]	Earth.	Yes, the radio spectrum could be analyzed to find out how many drones are in the battle.	Yes, it is a way for classifying.	Study Potential Interference.	Yes, if you can analyze the spectrum and determine no drones.	Yes, encourage to work with other forms of communication.	Yes	Yes	Yes	N/A	Yes, it could be trained in different ways to deceive the RF classification.
[98]	Earth.	Yes, having autonomous vehicles provides new strategies.	N/A	N/A	Yes, they could be used in recognition work.	Yes, the first 100% autonomous vehicle developments are emerging.	Yes	Yes	Yes	Yes	Yes, training is required along with autonomous vehicles.

6. Projects and Defense Industry Integrating AI

This section presents a selection of significant projects, industries, and countries related to defense where AI and ML are applied. Table 17 summarizes their name, what type of initiative they are, their prominent supporters, and the core related technological systems introduced in Section 3 involved in them and with AI integration explained in Section 5.

Table 17. Selection of projects and defense industry initiatives integrating AI.

Initiative	Type of Initiative	Year Starting	Main Supporter	Main Technological System
AIDA	Project	2023	Funded by European Defense Fund.	Information System in Tactical Environments.
ASTRAEA	Project	2006	Consortium of companies and government agencies of the United Kingdom.	Unmanned Systems.
ATLAS	Project	2020	Project developed by the U.S. Army.	Fire and Weapon Direction Systems.
COBRA	Project	N/A	Project developed by Directorate of Armament and Material (DGAM) of Spain.	Information Systems in Tactical Environments.
DARPA	R&D Agency	1958	Agency of the United States Department of Defense responsible for research and development of new technologies and innovative systems to develop disruptive technologies.	Information Systems in Tactical Environments and Unmanned Systems.
General Dynamics	Defense company	N/A	Defense company in the United States.	Information Systems in Tactical Environments.
GIDE	Project	2020	Led by the U.S. Department of Defense.	Information Systems in Tactical Environments.
Iron Dome	Project	2021	Developed by Israel.	Fire and Weapon Direction Systems.
Lockheed Martin	Defense company	N/A	Based in Bethesda, Maryland, U.S. It manufactures some of the world's most advanced stealth combat aircraft in the defense sector.	Fire and Weapon Direction Systems and Unit Maintenance Management Systems and Logistics.
Maven	Project	2017	Project initiated by the U.S. Department of Defense.	Image Surveillance Systems.
NORINCO	Defense corporation	N/A	Chinese state-owned defense corporation that manufactures commercial and military products.	Information Systems in Tactical Environments, Radar Systems, and Unmanned Systems.
Northrop Grumman	Defense company	N/A	American multinational aerospace and defense company.	Information Systems in Tactical Environments, Radar Systems, Fire and Weapon Direction Systems, Unmanned Systems, and Unit Maintenance Management Systems and Logistics.
Russia	Country	N/A	Russian defense companies: Kalashnikov Group and Almaz-Antey.	Information Systems in Tactical Environments, Electronic Warefare System, Fire and Weapon Direction Systems, and Unmanned Systems
SEDA	Project	2018	Spanish initiative based on the COINCIDENTE program of the General Directorate of Armament and Material (DGAM) of Spain.	Image Surveillance Systems.
SOPRENE	Project	N/A	Spanish initiative based on the COINCIDENTE program of the General Directorate of Armament and Material (DGAM) of Spain.	Unit Maintenance Management Systems and Logistics.

6.1. AIDA

Thales Group has been heavily involved in incorporating AI into defense projects, focusing on enhancing military systems' security, efficiency, and autonomy. Some of their notable AI-driven defense initiatives include the Artificial Intelligence Deployable Agent (AIDA) project [99]. The European Defense Fund funded it and aims to develop an autonomous AI agent capable of enhancing cybersecurity in defense systems. Specifically, AIDA is designed to protect aircraft systems from cyber attacks, providing real-time automated threat detection and response. The solution is tested in scenarios involving advanced

cyber-electromagnetic threats and adversarial AI attacks. The project highlights Thales's strengths in onboard systems and cybersecurity, emphasizing autonomous responses to cyber threats in high-intensity environments.

Thales Group is also applying AI to develop advanced radar systems for air defense [99,100]. Thales's radar systems are designed to detect and track various aerial threats, from aircraft to missiles, in complex environments. The AI algorithms are embedded to ensure that the radar systems can autonomously adapt to different scenarios, making them more resilient to EW and capable of working in concert with other defense systems.

6.2. ASTRAEA

The ASTRAEA project (Autonomous Systems Technology Related Airborne Evaluation and Assessment) [101] by BAE systems in the United Kingdom aims to develop advanced AI and ML technologies to improve the autonomy and effectiveness of military systems, making them more capable of operating in complex and dynamic environments without constant human intervention.

The project focuses on the following areas:

- Integrating AI capabilities for decision-making in combat, surveillance, and logistics missions, optimizing the systems' autonomy and ability to adapt to rapid environmental changes.
- Developing technologies for autonomous air and ground vehicles that operate without direct human intervention. These systems are essential for reconnaissance, exploration, and logistical support missions in conflict zones.
- Ensuring the resilience of systems against cyber attacks and providing the ability to self-diagnose or recover from failures is a key component of the project, ensuring that systems remain uncompromised during critical missions.

As a defense and security engineering leader, BAE systems has collaborated with various government agencies and technology companies to advance the ASTRAEA project. This includes partnerships with academic institutions and research laboratories that contribute their AI, robotics, and data-analysis expertise.

6.3. ATLAS

Advanced Targeting and Lethality Automated System (ATLAS) project [102] aims to provide AI and ML to U.S. combat tanks, making it possible to identify and attack three times faster than conventional procedures. For this purpose, the work has been focused on the following technology areas:

- Data collection on potential types of military targets and performing a prior training of the ML algorithm.
- Imaging processing applying ML techniques for objectives classification, recognition, identification, and tracking.
- Shot control. In this area, advanced guiding algorithms, the automation of the shooting process, and weapon recommendations are fundamental to be used according to the identified objective.
- The technical support integrated into the combat vehicle is necessary due to a high voltage power system (600 Vdc) and the integration of sensors and electronics.
- Sensors. To carry out all needed automatization and provide available actual data for the ML algorithm, tanks are equipped with sensors in the visible spectrum, infrared spectrum (NIR, SWIR, MWIR, and LWIR), 360º rotation of the sensors and rangefinder lasers (LADAR and LIDAR).

The ATLAS initiative harnesses the power of ML for image recognition, enabling surveillance systems to detect potential terrorist attacks and anticipate events, as outlined in [103].

6.4. COBRA

The COBRA project will allow us to carry out adaptive and customizable cyber maneuvers of hyperrealistic simulation of Persistent Advanced Threats (APT) and cyber defense training using gamification [104]. This project is a Spanish initiative based on the COINCIDENTE program of the General Directorate of Armament and Material (DGAM) of Spain [105].

The main objectives of this project are presented next:

- To simulate topology networks and real traffic.
- To develop random and parameterizable scenarios.
- To develop adaptive cyber maneuvers using gamification.
- To validate the entire proposal in the Cyber Range of the Joint Cyberspace of the Ministry of Defence of Spain.

This project incorporates AI techniques with adaptive learning. The scenarios can be adapted specifically to each student and can perform adaptive cybermaneuvers with gamification. In addition, different information will be gathered through telemetry and biometric systems.

In addition, ML enables the system to recognize the visual shape of an enemy tank, detect its thermal signature, and establish alarm parameters. When satellite images capture a figure resembling these characteristics, the system promptly alerts the operator.

6.5. DARPA

Defense Advanced Research Projects Agency (DARPA) [106] is an agency of the United States Department of Defense responsible for research and development of new technologies and innovative systems to develop disruptive technologies that can transform the way armed forces operate, giving the United States a technological advantage on the battlefield. DARPA includes several applied projects integrating AI into defense.

- **OFFensive Swarm-Enabled Tactics (OFFSET)** [107]: Aims to develop swarms of small autonomous drones capable of operating together to perform reconnaissance, attacks, and rescue missions.
- **Lifelong Learning Machines (L2M)** [108]: Seeks to use ML to train cybersecurity systems capable of detecting threats and continuously adapting to new attack tactics. Creating autonomous systems that can defend computer networks and protect critical infrastructures against cyber threats.
- **AI for Military Operations (AIMO)** [109]: A program aimed at developing AI technologies that help improve the precision of military operations and optimize resources. The project also addresses how to integrate AI into joint military operations efficiently.

6.6. General Dynamics

General Dynamics is another major defense company in the United States. It is using AI in the development of armored and combat vehicle systems, as well as in enhancing real-time intelligence capabilities for the armed forces. Through its unit General Dynamics Land Systems, the company has been developing autonomous armored vehicles for the U.S. Army under the Robotic Combat Vehicle (RCV) program. These vehicles are designed to operate without direct human intervention and perform tasks such as reconnaissance, target attacks, and logistical support on the battlefield. The incorporation of ML algo-

rithms aims to improve autonomous driving, navigation, and decision-making in armored vehicles [110].

In addition, it has started to expand its development into cybersecurity systems, using AI to detect and neutralize cyber threats.

6.7. GIDE

Global Information Dominance Experiment (GIDE) project is aimed to predict possible threats using AI and ML to analyze the information provided by satellites, radars, drones, underwater capabilities, networks, and others [111]. This technology would allow the U.S. military to view movements several days before the enemy, providing an advantageous tactical environment over any attack.

However, this technology is not novel. Innovative is using AI and ML to change how information and data are used. ML and AI allow a set of different parameter alert configurations and perform tests with another kind of Geospatial Intelligence sensors to closely observe what is happening at a specific location [112].

6.8. Iron Dome

Israel has led the implementation of advanced technologies, including AI, in its defense system. This includes using AI for threat prediction, intelligence data analysis, and the enhancement of missile systems. A notable example is the *Iron Dome* project [113], an air defense system developed by Israel to intercept and destroy short-range missiles, rockets, and artillery shells that threaten civilian areas. Developed by Rafael Advanced Defense Systems and Israel Aerospace Industries, the system has proven highly effective in protecting Israeli populations from aerial attacks from Gaza and other regions.

Its operation involves the following key components:

- **Detection radar:** The system uses advanced radars to detect real-time threats such as incoming rockets and missiles. These radars provide high-precision data about the trajectory of the projectiles.
- **Battle control center:** Once the threat is detected, the system performs an automatic analysis to determine if the projectile is a real threat to the protected areas. If the projectile is deemed capable of causing damage, the system autonomously intercepts it.
- **Interceptors:** The Iron Dome interceptors are launched to destroy the incoming projectile in the air before it can reach its target. The system has a high success rate, intercepting more than 90% of threats aimed at civilian areas.

6.9. Lockheed Martin

Lockheed Martin is one of the largest and most prominent companies in the defense and aerospace sector, based in Bethesda, Maryland, USA. It manufactures some of the world's most advanced stealth combat aircraft in the defense sector, such as the F-22 Raptor and the F-35 Lightning II [114]. It also develops various missile systems, including the Terminal High Altitude Area Defense and Patriot missile defense systems to intercept ballistic and cruise missiles.

Involved in the current development of advanced technologies and innovative projects, Lockheed Martin has been utilizing AI and ML in several aspects of defense, including updates to the F-35 and intelligent missile systems. Additionally, they implement AI in predictive maintenance and data analysis to enhance cybersecurity and space defense through:

- **Autonomy in aircraft and UAV:** The use of AI for real-time decision-making during combat or reconnaissance missions
- **AI for failure prediction:** They use predictive models to anticipate failures in system components, optimizing maintenance.

6.10. Maven

Project Maven [115], initiated by the U.S. Department of Defense, focuses on applying AI and ML to analyze drone footage to identify and track objects of interest, such as potential targets. This project uses computer vision algorithms to sift through massive amounts of video data gathered by drones, significantly improving the speed and accuracy of target recognition compared to manual methods. The primary goal of Project Maven is to assist the military in making faster, more informed decisions by automating the analysis of vast amounts of surveillance footage, enabling a more efficient use of resources in intelligence gathering and combat operations.

The AI-powered system processes video feeds to detect patterns and identify objects, which can be crucial in military operations such as targeting, reconnaissance, and surveillance. This system can identify vehicles, people, or other objects and provide real-time data for further action. Despite concerns over the ethics of AI in warfare, particularly regarding the automation of target identification, Project Maven has sparked significant interest in integrating AI into military applications.

6.11. NORINCO

China has been investing significantly in AI to enhance its defense capabilities, particularly in cybersecurity and military automation. The country has implemented AI in various systems for mass surveillance, troop control, and military vehicle automation. One prominent focus is cyber defense, where AI analyzes vast amounts of intelligence data, detects cyber threats, and improves national security. Additionally, AI is being used to develop autonomous military systems, including drones and unmanned vehicles, designed to carry out combat and reconnaissance missions with minimal human intervention.

In this context, China North Industries Group Corporation (NORINCO) [116] is one of the key players actively developing AI-powered drones and autonomous military vehicles for defense applications. A notable example is their anti-drone technology [117], part of their larger EW systems for armored vehicles, particularly their VT4A main battle tanks. These systems utilize AI and radar technology to detect, track, and neutralize threats from small, slow-moving drones. These AI-driven systems provide layered defense strategies for ground units, enhancing the capabilities of military platforms to defend against modern drone threats. NORINCO also showcased these technologies at the Airshow China 2024, emphasizing the shift toward more digitally empowered and adaptable defense solutions in response to evolving combat scenarios

6.12. Northrop Grumman

Northrop Grumman is a leading defense and aerospace technology company recognized for its innovation in applying AI and ML to modern military systems [118,119]. The company integrates AI across various defense sectors, including space, cybersecurity, and autonomous vehicles. One of the most significant uses of AI by Northrop Grumman is in satellite defense systems, where AI is employed to monitor and protect satellites from potential threats, enhancing space-based security. Additionally, the company has been developing autonomous drones that utilize AI for real-time decision-making during combat and reconnaissance missions. These AI-driven drones aim to increase operational efficiency and reduce human intervention in high-risk environments.

One of Northrop Grumman's ongoing initiatives involves leveraging AI in advanced radar systems and missile defense technologies, including predictive algorithms that improve defense systems' accuracy and response time. This effort aims to increase the precision of military operations, provide faster and more reliable defense mechanisms, and optimize resource allocation during missions.

6.13. Russia

Russia has been increasingly focused on advancing AI technologies to enhance its defense capabilities. The country invests heavily in autonomous robotics, EW, and intelligent missile systems. Integrating AI into military systems aims to improve operational efficiency, precision, and adaptability in dynamic combat environments.

One of Russia's prominent projects involves the development of autonomous combat robots. These include ground-based robots and combat drones that operate independently, leveraging AI algorithms to perform reconnaissance, target identification, and attack operations. AI in these robots allows them to operate in highly complex and unpredictable environments, reducing human risk and increasing combat effectiveness. The Uran-9 combat robot, for example, is a key system developed by Russia that is designed to operate autonomously in combat zones, showcasing the country's ambition to integrate AI into its military assets.

Another critical development area is intelligent missile systems that incorporate AI to improve target precision and adaptability to changing conditions. Russia's use of AI in missile technology improves accuracy, allowing these weapons to adjust in real time to counter defensive measures or alter course in unpredictable battlefield scenarios.

In addition to these projects, Russia has been focusing on EW systems that use AI to detect and counter adversary signals, disrupt communications, and neutralize enemy systems in the electromagnetic spectrum.

Russian Defense Companies Involved:

- **Kalashnikov Group:** known for developing autonomous combat systems, including AI-powered drones and robots [120].
- **Almaz-Antey**, a defense manufacturer that works on advanced missile systems and air defense solutions that integrate AI for more efficient target acquisition and defense [121].

These developments position Russia as a key player in the evolving AI-driven defense sector, emphasizing autonomy, intelligence, and adaptability in warfare.

6.14. SEDA

The SatEllite Data Ai (SEDA) project [122], a Spanish initiative based on the COINCIDENTE program of the General Directorate of Armament and Material (DGAM) of Spain [105], an intelligent geospatial that analyzes and exploits satellite information to detect changes in the temporal status of satellite imagery.

This project combines the potential of DL with data processing and data fusion to automatically analyze satellite information. The resulting tool allows for discovering information that is not fully revealed, such as the movement of troops or war equipment.

6.15. SOPRENE

SOPRENE (Predictive Sustainment of Neural Networks, or SOstenimiento Predictivo de REdes NEuronalesin Spanish) is a Spanish initiative based on the COINCIDENTE program of the General Directorate of Armament and Material (DGAM) of Spain [105] that promotes the use of neural networks in the preventive maintenance of Spanish Navy ships [123].

The most modern ships in the Spanish Navy have installed an integrated platform control system, which mainly controls their propellant plant, power plant, auxiliary machines, and firefighting system. This platform or system is also associated with a Condition-Based Maintenance System. Hundreds of ship sensors are connected, generating thousands of signals and hundreds of megabytes of daily information. These data are sent to the Navy Data Monitoring and Analysis Center to create a Big Data signal architecture of propulsion

motors, electric generators, fire pumps, and other equipment to analyze and predict faults or abnormal performances.

7. Results and Quantitative Insights

This section synthesizes the key findings derived from the comprehensive survey, structured into five core contributions: bibliographic usage trends, performance benchmarking, target metrics for future tactical systems, technique-wise evaluation, and operational impact.

Figures 9 and 10 summarize the AI techniques and military domains most frequently addressed in the literature. CNN, RL, and SVM dominate across multiple applications. Across 110 military studies, the dominance of DL with a 37% is the predominant one due to its effectiveness in image recognition, radar analysis, and autonomous decision-making. FL (1%) remains emerging, with adoption limited by operational constraints and security concerns.

UAVs, radar, and EW emerge as the most common operational technologies according to Figure 11. This confirms a growing focus on autonomy, pattern recognition, and adaptive decision-making under constrained environments. DL techniques such as CNN, DNN, YOLO, and GAN models are the most utilized, particularly in image surveillance and radar systems, where object recognition and threat detection are crucial. RL (DRL, DQN) is predominantly applied in information systems. Also, RL is emerging as a crucial tool for adaptive military strategies, particularly in automated combat and UAV operations. UL (SVM, RF) is widely employed in EW and Predictive Maintenance, ensuring efficient classification and fault detection. At the same time, Hybrid AI Models exhibit a more balanced yet lower application frequency across different military domains.

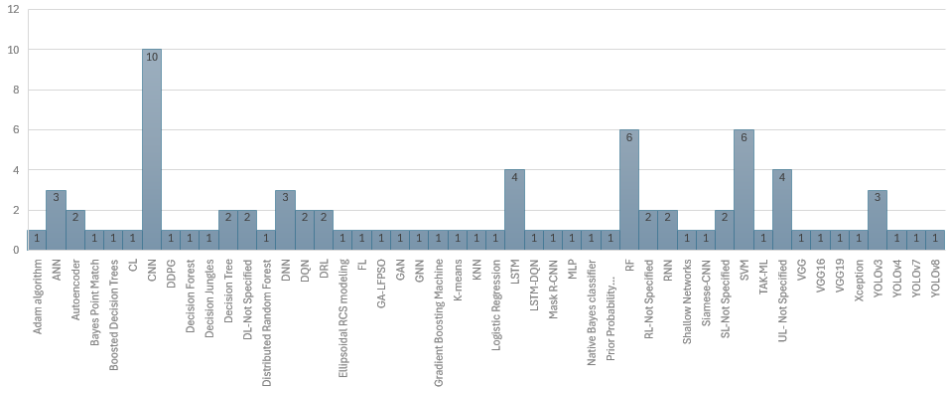


Figure 9. Mapping between the number of references and the type of AI technique used.

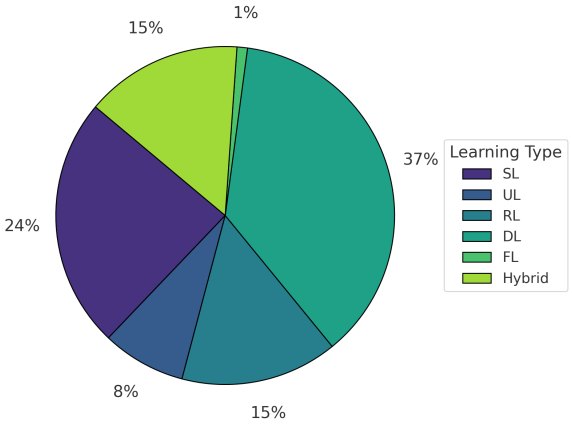


Figure 10. Statistical per learning type.

Key performance parameters commonly used in the design of tactical communication systems are summarized in Table 18, and how AI integration can significantly enhance them. These metrics serve as reference goals for future tactical AI-enabled systems. These parameters define the operational viability of AI-driven defense systems. Ultra-low latency ensures timely tactical responses, while high throughput and energy efficiency support complex, multi-sensor environments with limited resources. Reducing SWaP is essential for deploying AI in mobile or embedded platforms. Robustness, security, and optimized performance per watt ensure reliability, resilience, and autonomy under hostile and resource-constrained conditions. These targets establish a benchmark for future AI-enabled tactical communications and operations. This study outlines critical performance goals, including latency below 5 ms, inference throughput over 1000 qps, and power efficiency exceeding 100 TOP S/W, which support time-sensitive and resource-constrained missions. These benchmarks reflect requirements for edge AI integration, enabling faster responses and longer endurance in unmanned or embedded systems.

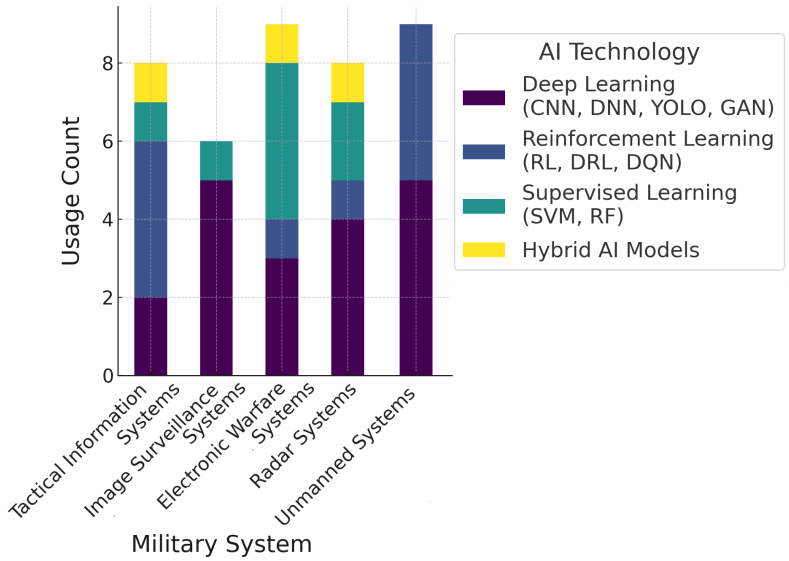


Figure 11. Distribution of AI technologies across military communication systems.

Table 18. Key performance parameters in defense systems and improvement goals with AI integration.

Parameter	Typical Values (Baseline)	Improvement Target with AI
Latency (Edge/Inference)	<10 ms in edge systems (TinyML)	≤5 ms for real-time tactical response
Throughput (e.g., ResNet-50)	∼500 queries/s with optimizations	>1000 qps to support multiple concurrent streams
Energy Efficiency	6× energy savings in optimized architectures	>10× for extended autonomous deployment
SWaP (Size, Weight, Power)	SoC-based chips (Jetson, FPGA)	30–50% reduction in footprint and power
Security and Privacy	Edge processing reduces data exposure	Local encryption + threat detection for resilience
Robustness (Adversarial Evaluation)	Tested via red teaming and offline validation	Continuous adversarial benchmarking
Performance per Watt (TOPS/W)	30–80 TOPS/W in current AI accelerators	>100 TOPS/W in next-gen tactical AI chips

We create a comparative heatmap from the most relevant AI techniques identified in this survey (Figure 12) to evaluate them. CNN, LSTM, RL, SVM, FL, and GNN. These techniques were selected based on their frequency of use, diversity of application, and operational relevance across the reviewed military communication systems. Figure 12 illustrates the perceived impact of each technique on five key tactical system objectives: resilience, latency, autonomy, scalability, and interoperability. Each cell in the heatmap is assigned a value from 1 to 5, where 1 indicates low impact and 5 indicates high impact. These values have been derived through a qualitative synthesis of insights.

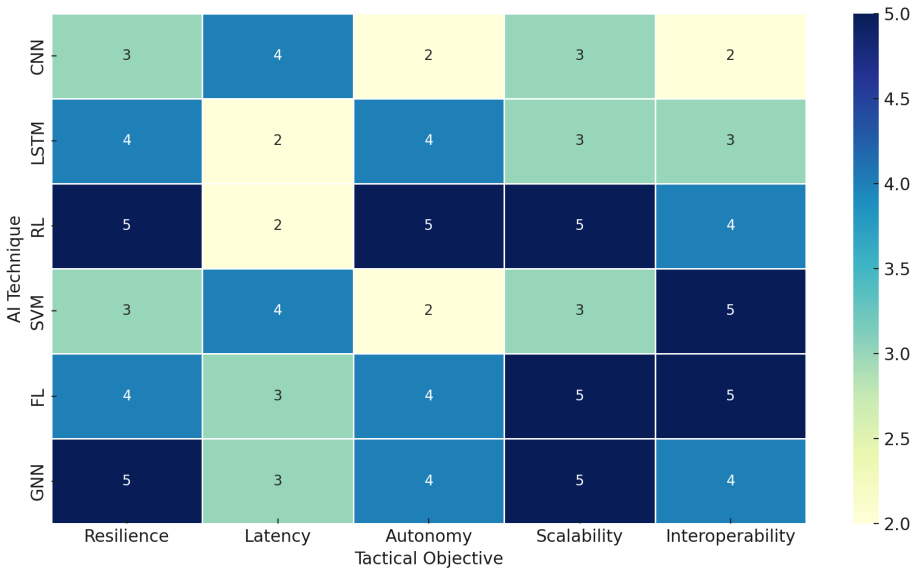


Figure 12. Heatmap showing the relative impact of selected AI techniques on key tactical system objectives.

Table 19 presents a qualitative compatibility analysis between the most relevant AI techniques identified in this survey and a range of military operational environments. The evaluation highlights where each technique is well suited (✓) or presents limitations (✗) across various domains, including UAVs, radar systems, EW, naval operations, surveillance systems, information networks, and space environments. This mapping serves as a practical reference for selecting AI models according to mission-specific requirements.

To orient the reader, the following outlines indicative use cases of standard deep-learning models across system-level tasks:

- CNNs are more used for strong spatial/spectral patterns (e.g., perception from Electro-Optical/IR/SAR; spectrogram-based RF classification) with moderate, controllable inference latency;
- RNNs/LSTMs/Gated Recurrent Unit are more used for sequence modeling for time-correlated behaviors (traffic/load dynamics, policy rollout), increasingly supplanted by attention on long contexts;
- GNNs are proposed in the literature for topology-aware reasoning (routing, coalition formation, jamming propagation) with message-passing overhead proportional to graph density;
- Transformers are proposed as long-range dependency modeling and cross-modal alignment, with higher memory/compute demands mitigated by pruning/quantization/distillation at the edge.

Table 19. Compatibility of AI techniques with various military operational environments.

AI Technique	UAV Ops	Radar	EW	Maritime/Naval	Surveillance Systems	Info Networks	Space Environments
CNN	✓ Object recognition	✓ Target ID	✓ RF classification	✓ Ship detection	✓ Thermal/visual detection	✓ Feature extraction	✓ Image recognition from satellites
LSTM	✓ Flight prediction	✗ Slow for real time	✗ Limited	✗ Motion modeling	✗ Rare	✗ High memory	✗ Temporal modeling limited
RL	✓ Autonomous pathing	✗ Rarely used	✓ Threat response	✓ Route planning	✓ Swarm coordination	✓ Adaptive routing	✓ Orbital coordination
SVM	✗ Not used	✓ Legacy signal ID	✓ Interference detection	✗ Limited	✓ Pattern classification	✓ Traffic classification	✓ Signal filtering
FL	✓ Collaborative learning	✗ Not mature	✗ Deployment limits	✓ Shared models	✓ Model updates	✓ Decentralized training	✓ Privacy-focused federated updates
GNN	✓ Swarm behavior	✗ Complex	✗ Rare	✓ Mesh optimization	✓ Scene graphing	✓ Topological modeling	✓ Graph-based orbit modeling

8. Future Research Directions

Integrating AI into military communications and networking presents significant challenges and opportunities for the future research lines. While AI has demonstrated potential in areas such as decision-making, autonomous systems, and electronic warfare, its full deployment in tactical communication networks and multidomain information sharing requires further advancements. This section explores key challenges, emerging trends, and strategic recommendations to guide future research and innovation.

8.1. Key Challenges in AI-Driven Military Communications

- Interoperability Across Multidomain Operations: AI-driven military networks must integrate seamlessly across land, air, sea, space, and cyber domains. Current AI models often lack the adaptability required to function efficiently in diverse operational environments, necessitating the development of standardized communication protocols.
- Adversarial Threats, Cybersecurity Risks, and Ethical Considerations: AI-enabled defense networks are vulnerable to EW, cyber attacks, and adversarial AI tactics. Future research must focus on robust AI security mechanisms, encryption-enhanced network resilience, and real-time threat detection algorithms. Ethical concerns surrounding AI in warfare require standardized frameworks and regulations to ensure accountability and compliance (see [6]).
- Data Scarcity and Real-World Adaptability: Military AI models require extensive, high-quality data to enhance learning capabilities. However, access to real-world datasets is restricted due to security concerns. The development of synthetic data generation and simulation-based AI training is crucial to overcoming these limitations. Within the broader data-acquisition discussion, PHY-layer artifacts—such as IQ sample capture and CSI estimation—pose their challenges. Tactical radios already employ mature techniques that mitigate many of these issues; nevertheless, an important research avenue is to extend AI to these processes (e.g., robust estimation, denoising, compression, uncertainty-aware inference) to further improve tactical communications performance under mobility, interference, and spectrum congestion.
- Scalability and Latency in Tactical Communications: AI-driven communication systems must operate in low-latency, high-mobility battlefield environments. Future

research should focus on optimizing real-time AI inference, edge computing for tactical units, and decentralized AI architectures to reduce reliance on centralized cloud processing.

- Fusion in information signals: Despite notable progress within single-modality pipelines, we find a persistent gap in end-to-end, AI-enabled multimodal fusion that jointly exploits radar returns, Electro-Optical/IR imagery, and communications-derived metadata to strengthen situational awareness in contested electromagnetic environments. Promising directions include cross-modal Transformers for feature-level alignment/attention and Bayesian fusion networks for uncertainty-aware, decision-level integration. Expected gains are improved interference/clutter suppression, track continuity, and robust target recognition under low SNR and partial observability. However, key barriers remain—precise time/geo-synchronization and calibration across heterogeneous sensors, modality imbalance and missing data, bandwidth/latency limits at the tactical edge, and resilience to deception (decoys/spoofing) in EW/ESM settings. We therefore propose this as a priority future research line for tactical systems, supported by simulation-driven verification with standardized metrics (e.g., probability of detection and/or false alarm under jamming, multi-object tracking, localization Circular Error Probable, end-to-end latency/energy budgets, and uncertainty calibration via Expected Calibration Error/Brier), plus ablations with modality dropouts and spectrum-congestion stress tests, ideally enabled by shareable synthetic multimodal datasets with controllable threat models.

8.2. Emerging Trends in AI for Military Communication Networks

- FL for secure AI model training: Distributed AI training allows allied nations and defense units to develop AI models collaboratively without sharing raw data, improving confidentiality while enhancing AI performance.
- AI-enhanced network resilience and self-healing communications: AI-based autonomous recovery mechanisms can enhance the survivability of battlefield networks by dynamically reconfiguring communication pathways in response to disruptions.
- Cognitive radio and AI-driven spectrum management: AI can optimize spectrum allocation, interference mitigation, and adaptive frequency hopping to ensure uninterrupted military communications in congested or adversarial environments.
- Neuromorphic computing for low-power AI in tactical networks: Neuromorphic computing enables low-power, high-efficiency AI models for real-time signal processing and decision-making in battlefield networks. These architectures offer advantages for on-device intelligence in edge computing environments, allowing UAVs, UGVs, and remote sensors to operate with minimal latency and reduced energy consumption. Future research should explore neuromorphic chips for adaptive AI models in contested electromagnetic environments, ensuring robustness in military operations.

8.3. Strategic Recommendations for Future AI Research in Defense Communications

An important pillar in defense is the identification of information space adversaries or attackers. AI can be a powerful ally for hardening defense communication systems in this area. Table 20 presents our own analysis, distilled from the surveyed literature, mapping the most common attacker models in defense to the AI-enabled defense mechanisms most suitable for system-level deployment.

Table 20. Mapping of attacker models to AI-enabled defense mechanisms in tactical communications.

Attacker Mode	Targeted System/Layer	Typical Threat Scenario	AI-Enabled Defense Mechanism
Jamming	Wireless channels, EW systems	Adversary disrupts communication by overwhelming the spectrum with interference	Deep Reinforcement Learning (DRL)-based anti-jamming for adaptive spectrum access and channel hopping
Spoofing	Radar, UAV control, GPS	Adversary injects false signals (e.g., fake GPS coordinates or radar echoes)	Adversarial detection models with anomaly-based ML; cross-sensor data fusion for signal validation
Evasion Attacks	Image surveillance, radar object detection	Adversarial perturbations designed to fool AI classifiers into mislabeling targets	Adversarial training, robust feature extraction, and XAI for resilient detection
Data Poisoning	Training datasets, tactical information networks	Corrupted training samples degrade ML performance in deployed systems	Robust data sanitization, secure data provenance, and Federated Learning (FL) with anomaly detection
Byzantine Attacks	Distributed learning across coalition networks	Malicious clients send manipulated updates to degrade global models	Byzantine-robust FL algorithms (median-based aggregation, Krum, Trimmed Mean) with trust scoring

Jointly with the fundamental pillar of identification of attackers, other points to research in defense are:

- Developing Standardized AI Interoperability Frameworks: Establishing unified protocols for AI-driven communication systems will enable seamless integration between different military branches and allied forces. Study of CNN/RNN/GNN/Transformer architectures specifically for tactical radio tasks under standardized, threat-realistic benchmarks. For more about tactical radio, the reader can link to [10] for context.
- Enhancing AI Resilience Against EW and Cyber Threats: Research should prioritize adversarial training, AI-driven jamming detection, and AI-based cyber deception strategies to counteract evolving threats.
- Investment in AI-Powered Tactical Edge Computing: The deployment of AI-enabled edge devices will enhance battlefield decision-making capabilities while reducing dependence on centralized computing infrastructures.
- Advancing AI-Driven UAV and UGV Communications for Tactical Networks: While AI-powered UAVs and UGVs have been successfully deployed for tactical communications, challenges remain in optimizing their network coordination, adaptability, and resilience in contested environments. Future research should focus on enhancing real-time adaptive routing, developing self-learning communication protocols, and integrating AI-based dynamic spectrum allocation to improve interoperability across multidomain operations. Additionally, advancements in federated learning and neuromorphic computing could enable greater autonomy and efficiency in UAV-UGV communication networks, ensuring seamless integration with existing defense infrastructure.
- Strengthening Civilian-Military AI Collaboration: Encouraging partnerships between defense agencies, academic institutions, and private AI developers can accelerate innovation in military communication technologies.

Military operations can achieve enhanced security, efficiency, and resilience by addressing these research challenges and advancing AI technologies in tactical communications and networking. Future work must focus on bridging gaps between AI research and real-world deployment, ensuring that AI-driven defense networks remain adaptable, secure, and mission-ready.

9. Conclusions

This survey explores AI applications in tactical communications, highlighting key advancements, limitations, and research gaps. While AI progresses in civilian domains, its deployment in information networks, EW, radar, and battlefield decision-making for the tactical domain remains limited. Cross-domain integration across land, sea, air, and space—supported by simulation-based testing—is critical for reliability. This work offers a comprehensive perspective that combines a technological overview with standardized design metrics, unlike prior surveys focused on isolated areas. To our knowledge, no other survey delivers such an integrated analysis of AI integration in military communications. It serves as a resource for researchers, defense professionals, and policymakers, identifying trends, open challenges, and strategic recommendations. Advancing this field requires secure data sharing, cross-sector collaboration, and investment in robust, autonomous AI systems.

Author Contributions: Conceptualization, V.M.B.; methodology, V.M.B.; validation, V.M.B., R.P. and C.M.; formal analysis, V.M.B.; investigation, V.M.B., R.P., L.C.S. and C.M.; writing—original draft preparation, V.M.B.; writing—review and editing, V.M.B., R.P., L.C.S. and C.M.; supervision, V.M.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The datasets used and/or analyzed during the current study are available from the corresponding author upon reasonable request.

Acknowledgments: The authors would like to express their gratitude for the guidance and insights provided by military personnel, especially E. J. A. Suárez and his final thesis.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

5G	5th Generation	AR	Augmented Reality
A2A	Aerial to Aerial	ATLAS	Advanced Targeting and Lethality Automated System
A2G	Aerial to Ground	C2	Command and Control
AE	AutoEncoder	C2IS	C2 Information Systems
AESA	Active Electronically Scanned Array	C4ISR	C2 Communications Computers ISR
AI	Artificial Intelligence	CCD	Charge-Coupled Device
AIDA	Artificial Intelligence Deployable Agent	CCTV	Closed-Circuit Television
AIMO	AI for Military Operations	CCW	Convention on Certain Conventional Weapons
AMDR	Air and Missile Defense Radar	CEW	Cognitive Electronic Warfare
ANN	Artificial Neural Networks	CFAR	Constant False Alarm Rate
cGAN	Conditional Generative Adversarial Network	MARL	Multi-agent reinforcement learning
CIT	Configured Item Tree	MDM	Mobile Device Management
CL	Cooperative Learning	MIMO	Multiple-Input Multiple-Output
CNN	Convolutional Neural Network	ML	Machine Learning
COF	Cost Objective Function	MLP	Multi-Layer Perceptron
CSI	Channel State Information	MLOp	ML Operations
DARPA	Defense Advanced Research Projects Agency	MNN	Multi-Layer Neural Networks
DDPG	Deep Deterministic Policy Gradient Algorithm	MWIR	Mid-Wave Infrared
DIL	Disconnected Intermittent and Limited	N/A	Not Available
DL	Deep Learning	NAC	Network Access Control
DLP	Data Loss Prevention	NATO	North Atlantic Treaty Organization

DNN	Deep Neural Networks
DQN	Deep Q-Network
DRL	Deep Reinforcement Learning
DSG	Deep Supervised Generative
DT	Digital Twin
ECM	Electronic Countermeasures
EPM	Electronic Protective Measures
ESM	Electronic Support Measures
EW	Electronic Warfare
FL	Federated Learning
FSO	Free Space Optics
G2A	Ground to Aerial
GA	Genetic algorithms
GaN	Gallium Nitride
GAN	Generative Adversarial Network
GenAI	Generative AI
GEOINT	Geospatial Intelligence
GGE	Group of Governmental Experts
GIDE	Global Information Dominance Experiment
GNN	Graph Neural Network
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HMFFNet	Hybrid Model featuring a Feature Fusion Network
ICMP	Integrated Class Maintenance Plan
IDS	Intrusion Detection System
IED	Improvised Explosive Device
IHL	International Humanitarian Law
IoBT	Internet of Battlefield Things
IoT	Internet of Things
IPS	Intrusion Prevention System
IR	Infra Red
ISR	Intelligence Surveillance and Reconnaissance
JREAP	Joint Range Extension Application Protocol
KNN	K-Nearest Neighbors
L2M	Lifelong Learning Machines
LAWS	Lethal Autonomous Weapon Systems
LFPSO	Levy Flight Particle Swarm Optimization
LLM	Large Language Model
LVC	Live-Virtual-Constructive
mAP	Mean Average Precision
NGO	Non-Governmental Organization
NIR	Near Infrared
NLP	Natural Language Processing
PSO	Particle Swarm Optimization
QoE	Quality of Experience
QoS	Quality of Service
RCNN	Region-based CNN
RCS	Radar Cross Section
RCV	Robotic Combat Vehicle
RF	Random Forest
RIS	Reconfigurable Intelligent Surfaces
RL	Reinforcement Learning
RMA	Radar Modular Assemble
RNN	Recurrent Neural Network
ROI	Region of Interest
SA	Situational Awareness
SAR	Synthetic Aperture Radar
SDR	Software Defined Radio
SEDA	SatEllite Data Ai
SL	Supervised Learning
SNN	Spiking Neural Network
SNR	Signal-to-Noise Ratio
SSL	Semi-supervised Learning
SVM	Support Vector Machines
SWIR	Short-Wave Infrared
TAK-ML	Tactical Assault Kit-ML
U.S.	United States
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UGV	Unmanned Ground Vehicle
UL	Unsupervised Learning
US	Unmanned Systems
MUS	Maritime Unmanned Systems
VGG	Visual Geometry Group
VMF	Variable Message Format
XAI	Explainable AI
YOLO	You Only Look Once
LSTM	Long Short-Term Memory
LWIR	Long-Wave Infrared

References

1. Anastasiou, T.; Pastellas, I.; Karagiorgou, S. Adversarial Explanations for Informed Civilian and Environmental Protection. In Proceedings of the 2024 IEEE International Conference on Big Data (BigData), Washington, DC, USA, 15–18 December 2024; pp. 2672–2681. [CrossRef]
2. He, Y.; Huang, F.; Jiang, X.; Nie, Y.; Wang, M.; Wang, J. Foundation Model for Advancing Healthcare: Challenges, Opportunities and Future Directions. *IEEE Rev. Biomed. Eng.* **2025**, *18*, 172–191. [CrossRef]
3. Hamissi, A.; Dhraief, A.; Sliman, L. A Comprehensive Survey on Conflict Detection and Resolution in Unmanned Aircraft System Traffic Management. *IEEE Trans. Intell. Transp. Syst.* **2025**, *26*, 1395–1418. [CrossRef]
4. Fontanesi, G.; Ortiz, F.; Lagunas, E.; Garcés-Socarrás, L.M.; Monzon Baeza, V.; Vázquez, M.A. Artificial Intelligence for Satellite Communication: A Survey. *IEEE Commun. Surv. Tutor.* **2025**, *Early Access*, 1. [CrossRef]
5. Datumaya Wahyudi Sumari, A. Smart Military Society: Defining the characteristics to score the "Smart" of the military services. In Proceedings of the International Conference on ICT for Smart Society, Jakarta, Indonesia, 13–14 June 2013; pp. 1–8. [CrossRef]
6. Alcántara Suárez, E.J.; Monzon Baeza, V. Evaluating the Role of Machine Learning in Defense Applications and Industry. *Mach. Learn. Knowl. Extr.* **2023**, *5*, 1557–1569. [CrossRef]

7. Hu, C.; Zhao, Y.; Wang, Z.; Du, H.; Liu, J. Games for Artificial Intelligence Research: A Review and Perspectives. *IEEE Trans. Artif. Intell.* **2024**, *5*, 5949–5968. [CrossRef]
8. Chen, Z.; Zhu, J. Intelligent inference in combat simulation systems based on key feature extraction and uncertainty interval estimation. *IEEE Trans. Instrum. Meas.* **2025**, *74*, 3507912. [CrossRef]
9. Baeza, V.M.; Salor, L.C. New horizons in tactical communications: An overview of emerging technologies possibilities. *IEEE Potentials* **2024**, *43*, 12–19. [CrossRef]
10. Concha Salor, L.; Monzon Baeza, V. Harnessing the Potential of Emerging Technologies to Break down Barriers in Tactical Communications. *Telecom* **2023**, *4*, 709–731. [CrossRef]
11. Creus, J.G.; Baeza, V.M. Exploiting the Digital Twin Technology Advantages over Telemetry Data in GNSS. *IEEE Netw.* **2025**, *Early Access*, 1. [CrossRef]
12. Mikhailov, D.I. Optimizing National Security Strategies through LLM-Driven Artificial Intelligence Integration. *arXiv* **2023**, arXiv:2305.13927. [CrossRef]
13. Army, U. Smart Logistics: Navigating the AI Frontier in Sustainment Operations. Available online: https://www.army.mil/article/280377/smart_logistics_navigating_the_ai_frontier_in_sustainment_operations (accessed on 15 July 2025).
14. Lingel, S.; Hagen, J.; Hastings, E.; Lee, M.; Sargent, M.; Walsh, M.; Zhang, L.A.; Blancett, D. *Joint All Domain Command and Control for Modern Warfare: An Analytic Framework for Identifying and Developing Artificial Intelligence Applications*; Technical Report; Defense Technical Information Center. 1 July 2020. Available online: https://www.rand.org/pubs/research_reports/RR4408z1.html (accessed on 27 August 2025).
15. Campbell, L.; Lotmin, A.; DeRico, M.M.G.; Ray, C. The use of Artificial Intelligence in military simulations. In Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation, Orlando, FL, USA, 12–15 October 1997; Volume 3, pp. 2607–2612. [CrossRef]
16. Bistron, M.; Piotrowski, Z. Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens. *Electronics* **2021**, *10*, 871. [CrossRef]
17. Ammar, M.A.; Abdel-Latif, M.S.; Badran, K.M.; Hassan, H.A. Deep learning Achievements and Opportunities in Domain of Electronic Warfare Applications. In Proceedings of the Tenth ICICIS, Greater Noida, India, 15–16 March 2021; pp. 41–50. [CrossRef]
18. Rawat, D.B. Artificial Intelligence Meets Tactical Autonomy: Challenges and Perspectives. In Proceedings of the IEEE 4th International Conference on CogMI, Atlanta, GA, USA, 14–17 December 2022; pp. 49–51. [CrossRef]
19. Jyothi, A.P.; Shankar, A.; Narayan, A.J.R.; Bhavya, K.; Reddy, M.S.; Yashwanth, A. AI Methodologies in Upcoming Modern Warfare Systems. In Proceedings of the 2022 IEEE CCET, Bhopal, India, 23–24 December 2022; pp. 1–7. [CrossRef]
20. Ali, A.; Farid, A.; Al-kassem, A.H.; Khan, Z.A.; Qamer, M.; Ghouri, K.F.K. Development and use of Artificial Intelligence in the Defense Sector. In Proceedings of the 2023 ICBATS, Dubai, United Arab Emirates, 7–8 March 2023; pp. 1–10. [CrossRef]
21. Jyothi, A.P.; Shankar, A.; Narayan, A.J.R.; Bhavya, K.; Yadav, S.M.M. AI & ML Methodologies in Navy & their Systems. In Proceedings of the 2023 EASCT, Bengaluru, India, 20–21 October 2023; pp. 1–6. [CrossRef]
22. Oliveira, E.; Rodrigues, M.; Pereira, J.P.; Lopes, A.M.; Mestric, I.I.; Bjelogrlic, S. Unlabeled learning algorithms and operations: Overview and future trends in defense sector. *Artif. Intell. Rev.* **2024**, *57*, 66. [CrossRef]
23. Pakholchuk, V.; Horiacheva, K. Methodological Concepts of Applying AI into Military and Economic Capabilities Data Analysis. 2024. CNDCGS'2024; Num. 1. Volume 1. Available online: https://journals.unob.cz/index.php/CNDCGS/article/view/2088 (accessed on 27 August 2025).
24. Sebastian, L.; Axel, S. Enhancing Tactical Military Mission Execution through Human-AI Collaboration: A View on Air Battle Management Systems. In Proceedings of the IEEE 4th ICHMS, Toronto, ON, Canada, 15–17 May 2024; pp. 1–7. [CrossRef]
25. Arrabito, R.; Hou, M.; Fischmeister, S.; Falk, T.H.; Willoughby, H.; Cameron, M. Tracking user trust and mental states during cyber-attacks: A survey of existing methods and future research directions on AI-enabled decision-making for the Royal Canadian Navy. In Proceedings of the IEEE 4th ICHMS, Toronto, ON, Canada, 15–17 May 2024; pp. 1–4. [CrossRef]
26. Patil, A.T.; Vidhale, B.; Titarmare, A. Strategic Innovations in Defense Systems: A Comprehensive Analysis of Emerging Technologies and Future Trends. In Proceedings of the ISCS, Gurugram, India, 3–4 May 2024; pp. 1–7. [CrossRef]
27. Hagos, D.H.; Rawat, D.B. Neuro-Symbolic AI for Military Applications. *IEEE Trans. Artif. Intell.* **2024**, *5*, 6012–6026. [CrossRef]
28. Hadlington, L.; Binder, J.; Gardner, S.; Knight, S. The use of Artificial Intelligence in a military context: Development of the attitudes toward AI in defense (AAID) scale. *Front. Psychol.* **2023**, *14*, 1164810. [CrossRef] [PubMed]
29. Wang, W.; Liu, H.; Lin, W.; Chen, Y.; Yang, J.-A. Investigation on Works and Military Applications of Artificial Intelligence. *IEEE Access* **2020**, *8*, 131614–131625. [CrossRef]
30. AlphaStar. AlphaStar: Mastering the Real-Time Strategy Game StarCraft. Available online: https://www.deepmind.com/blog/alphastar-mastering-the-real-time-strategy-game-starcraft-ii (accessed on 15 July 2025).
31. Martín, J.A.R. IMF, Blog de Tecnología. Artículo Google Imágenes y el Machine Learning Que Todo Lo Ve. Available online: https://blogs.imf-formacion.com/blog/tecnologia/google-imagenes-cerebro-electronico-lo-ve/ (accessed on 15 July 2025).

32. Gamarra, G. Profesional Review—Artículo las 5 Mejores Aplicaciones de Reconocimiento de Voz. Available online: https://www.profesionalreview.com/2016/08/17/5-mejores-aplicaciones-reconocimiento-voz/ (accessed on 15 July 2025).
33. Kumar, A. Neural Network Types & Real-Life Examples. Available online: https://vitalflux.com/deep-neural-network-examples-from-real-life/ (accessed on 15 July 2025).
34. Center, B.S. MareNostrum5: A new EuroHPC World-Class Supercomputer in Spain. Available online: https://www.bsc.es/news/bsc-news/marenostrum5-new-eurohpc-world-class-supercomputer-spain (accessed on 15 July 2025).
35. Estapé, J.A.P. Computer hoy. Artículo IBM Summit: Así es el Superordenador Más Potente del Mundo. Available online: https://computerhoy.com/reportajes/tecnologia/ibm-summit-superordenador-mas-potente-del-mundo-627963 (accessed on 15 July 2025).
36. Hemsoth, N. NextPlatform. Artículo CHINA YA HA ALCANZADO LA EXAESCALA, EN DOS SISTEMAS SEPARADOS. Available online: https://www.nextplatform.com/2021/10/26/china-has-already-reached-exascale-on-two-separate-systems/ (accessed on 15 July 2025).
37. Geron, A. *Hands-on Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*, 2nd ed.; O'Reilly Media: Sebastopol, CA, USA, 2019.
38. Bobadilla, J. *Machine Learning y Deep Learning Usando Python, Scikit y Keras*; Ediciones de la U: Bogotá, Colombia, 2020.
39. Martínez, A. OSINT—La información es Poder. Available online: https://www.incibe.es/incibe-cert/blog/osint-la-informacion-es-poder (accessed on 15 July 2025).
40. Tecnobit. Procesador Data Link Multi-Protocolo (LINPRO). Available online: https://grupooesia.com/casos-de-exito/instalacion-linpro-armada-holandesa/ (accessed on 15 July 2025).
41. SYSCOM. ¿Quién Inventó el Primer Sistema de CCTV? Available online: https://www.syscomblog.com/2021/11/quien-invento-el-primer-sistema-de-cctv.html (accessed on 15 July 2025).
42. Elias, R. Sistemas de CCTV, Más Allá de la Seguridad. Available online: https://www.interempresas.net/Seguridad/Articulos/247951-Sistemas-de-CCTV-mas-alla-de-la-seguridad.html (accessed on 15 July 2025).
43. Caught on Camera. What Are the Different Types of CCTV Camera? Available online: https://www.caughtoncamera.net/news/different-types-of-cctv/ (accessed on 15 July 2025).
44. Spanish Ministry of Defense Regimiento de Guerra Electronica 31. Available online: https://ejercito.defensa.gob.es/ca/unidades/Madrid/rew31/Organizacion/index.html (accessed on 15 July 2025).
45. García, J.M.N. El sistema de Guerra electróNica de la Fragata F-110. Available online: https://www.defensa.com/espana/sistema-guerra-electronica-fragata-f-110 (accessed on 15 July 2025).
46. de Canales Martínez, M.G. Desarrollo de un Sistema de Guerra Electrónica para la Detección y Perturbación de Radares Marinos en Banda X. Master's Thesis, University of Vigo, Vigo, Spain, 2020.
47. Parker Sanfuentes, J. Radar History. Available online: https://revistamarina.cl/revistas/2000/1/jparkers.pdf (accessed on 15 July 2025).
48. Wolff, C. Radar Tutorial. Available online: https://www.radartutorial.eu/02.basics/rp10.es.html (accessed on 15 July 2025).
49. Martin, L. SPY-7 Is the Backbone of Multiple Defense Systems on Land, Air & Sea. Available online: https://www.lockheedmartin.com/en-us/products/spy-7.html (accessed on 15 July 2025).
50. Wikipedia. AN/SPY-6. Available online: https://en.wikipedia.org/wiki/AN/SPY-6 (accessed on 15 July 2025).
51. Boschetti, N.; Nikas, I.; Sharma, S.; Falco, G. A Global Ionosphere Situational Awareness Architecture for Over the Horizon Radar Operations. In Proceedings of the 2024 IEEE Aerospace Conference, Big Sky, MT, USA, 2–9 March 2024; pp. 1–9. [CrossRef]
52. Cuerno-Rejado, C.; García-Hernández, L.; Sánchez-Carmona, A.; Carrio, A.; Sanchez-López, J.L.; Campoy, P. Historical Evolution of the Unmanned Aerial Vehicles to the Present. *Dyna* **2016**, *91*, 282–288. [CrossRef]
53. Flir, T. FLIR. Available online: https://www.flir.es/products/black-hornet-3/?vertical=uas-norway&segment=uis (accessed on 15 July 2025).
54. Sande, C.A.S. Operaciones en el Ciberespacio. Available online: https://www.ccn-cert.cni.es/pdf/documentos-publicos/xiii-jornadas-stic-ccn-cert/ponencias/4390-s16-11-02-planeamiento-operaciones-en-el-ciberespacio/file.html (accessed on 15 July 2025).
55. Zhang, Y.; Dai, Z.; Zhang, L.; Wang, Z.; Chen, L.; Zhou, Y. Application of Artificial Intelligence in Military: From Projects View. In Proceedings of the 2020 6th International Conference on BigDIA, Shenzhen, China, 4–6 December 2020; pp. 113–116. [CrossRef]
56. Ágreda, A.G. Usos Militares de la Inteligencia Artificial, la Automatización y la Robótica (IAA&R). Available online: https://emad.defensa.gob.es/Galerias/CCDC/files/USOS_MILITARES_DE_LA_INTELIGENCIA_ARTIFICIALx_LA_AUTOMATIZACION_Y_LA_ROBOTICA_xIAAxRx.-_VV.AA.pdf (accessed on 15 July 2025).
57. Benson, C.B. Operaciones Terrestres Unificadas: La Evolución de la Doctrina del Ejército Para Lograr el éXito en el Siglo XXI. Available online: https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/MilitaryReview_20120630_art005SPA.pdf (accessed on 15 July 2025).

58. del Río, J.M.D.D. Concepto de Operaciones Navales. Available online: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2015/ArmadaEspanola_COPNAV.pdf (accessed on 15 July 2025).
59. Möhlenhof, T.; Jansen, N.; Rachid, W. Reinforcement Learning Environment for Tactical Networks. In Proceedings of the 2021 International Conference ICMCIS, The Hague, The Netherlands, 4–5 May 2021; pp. 1–8. [CrossRef]
60. Karim, H.; Rawat, D.B. Evaluating Machine Learning Classifiers for Data Sharing in Internet of Battlefield Things. In Proceedings of the 2021 IEEE SSCI, Orlando, FL, USA, 5–7 December 2021; pp. 1–7. [CrossRef]
61. Aghabeiki, S.; Hallet, C.; Noutehou, E.-R.; Rassem, N.; Adjali, I.; Mabrouk, M.B. Machine-learning-based spectrum sensing enhancement for software-defined radio applications. In Proceedings of the 2021 IEEE Cognitive Communications for Aerospace Applications Workshop (CCAAW), Cleveland, OH, USA, 21–23 June 2021; pp. 1–6. [CrossRef]
62. Freiberg, M.; McLaughlin, K.; Ningtyas, A.; Taylor, O.; Adams, S.; Beling, P.A. Enemy Location Prediction in Naval Combat Using Deep Learning. In Proceedings of the 2021 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 29–30 April 2021; pp. 1–6. [CrossRef]
63. Intizhami, N.S.; Husodo, A.Y.; Jatmiko, W. Warfare Simulation: Predicting Battleship Winner Using Random Forest. In Proceedings of the 2019 IEEE International Conference on Communication, Networks and Satellite (Comnetsat), Makassar, Indonesia, 1–3 August 2019; pp. 30–34. [CrossRef]
64. Chin, P.; Do, E.; Doucette, C.; Kalashian, B.; Last, S.; Lenz, N. TAK-ML: Applying Machine Learning at the Tactical Edge. In Proceedings of the MILCOM 2021—2021 IEEE Military Communications Conference (MILCOM), San Diego, CA, USA, 29 November–2 December 2021; pp. 108–114. [CrossRef]
65. Hu, D.; Yang, R.; Zuo, J.; Zhang, A.; Wu, J.; Wang, Y. Application of Deep Reinforcement Learning in Maneuver Planning of Beyond-Visual-Range Air Combat. *IEEE Access* **2021**, *9*, 32282–32297. [CrossRef]
66. Qu, T.; Xiong, G.; Dong, X.; Li, W.; Tao, H.; Yan, J. Missile Defense Decision-Making under Incomplete Information Using The Artificial Neural Network. In Proceedings of the 2021 IEEE 17th International Conference on Automation Science and Engineering (CASE), Lyon, France, 23–27 August 2021; pp. 1825–1830. [CrossRef]
67. Faisal, K.M.; Choi, W. Machine Learning Approaches for Reconfigurable Intelligent Surfaces: A Survey. *IEEE Access* **2022**, *10*, 27343–27367. [CrossRef]
68. Loevenich, J.F.; Lopes, R.R.F. DRL meets GNN to improve QoS in Tactical MANETs. In Proceedings of the NOMS 2024-2024 IEEE Network Operations and Management Symposium, Seoul, Republic of Korea, 6–10 May 2024; pp. 1–4. [CrossRef]
69. Dimitriu, A.; Michaletzky, T.V.; Remeli, V.; Tihanyi, V.R. A Reinforcement Learning Approach to Military Simulations in Command: Modern Operations. *IEEE Access* **2024**, *12*, 77501–77513. [CrossRef]
70. Álvaro González, J.; García, A.M.S.; Baeza, V.M. Blockchain-Enabled Management Framework for Federated Coalition Networks. *arXiv* **2025**, arXiv:cs.CR/2503.09666.
71. Kadam, P.; Vora, D.; Mishra, S.; Patil, S.; Kotecha, K.; Abraham, A. Recent Challenges and Opportunities in Video Summarization With Machine Learning Algorithms. *IEEE Access* **2022**, *10*, 122762–122785. [CrossRef]
72. Bhatti, M.T.; Khan, M.G.; Aslam, M.; Fiaz, M.J. Weapon Detection in Real-Time CCTV Videos Using Deep Learning. *IEEE Access* **2021**, *9*, 34366–34382. [CrossRef]
73. Elgohary, R.; Mahmoud, A.K.; Khaled, O.; Salah, S.; Badawi, M.B. Enhanced Thermal Human Detection in Military Applications Using Deep Learning. In Proceedings of the 2024 ITC-Egypt, Cairo, Egypt, 22–25 July 2024; pp. 91–98. [CrossRef]
74. Illig, D.W.; Kocan, K.X.; Mullen, L.J. Machine Learning Applied to the Underwater Radar-Encoded Laser System. In Proceedings of the Global Oceans 2020: Singapore—U.S. Gulf Coast, Biloxi, MS, USA, 5–30 October 2020; pp. 1–6. [CrossRef]
75. Ahmad, H.; Farhan, M.; Farooq, U. Computer Vision Techniques for Military Surveillance Drones. *Wasit J. Comput. Math. Sci.* **2023**, *2*, 53–59. [CrossRef]
76. ang, X.; Huo, H.; Li, J.; Li, C.; Liu, Z.; Chen, X. DSG-Fusion: Infrared and visible image fusion via generative adversarial networks and guided filter. *Expert Syst. Appl.* **2022**, *200*, 116905. [CrossRef]
77. Sampath, P.; Haseeb, S.; Jaideep, A.; Kiran, J.P.; Devi, S.A.; Srinivas, P.V.V.S. Revolutionizing Military Surveillance: Advanced Deep Learning Techniques for Aircraft Detection. In Proceedings of the 2023 ICSCSS, Coimbatore, India, 14–16 June 2023; pp. 12–19. [CrossRef]
78. Gacche, P.; Kokare, M.; Rathod, S.M.; Arulprasath, K.; Rathod, S.; Sharma, A. Foreign Object Detection and Classification using AI and ML for Radio Images. In Proceedings of the 2022 International Conference IConSIP, Pune, India, 26–27 August 2022; pp. 1–5. [CrossRef]
79. Legendre, D.; Vankka, J. Military Vehicle Recognition with Different Image Machine Learning Techniques. In *Information and Software Technologies, Proceedings of the 26th International Conference, ICIST 2020, Kaunas, Lithuania, 15–17 October 2020*; Springer: Cham, Switzerland, 2020; pp. 220–242.
80. McWhorter, T.; Morys, M.; Severyn, S.; Stevens, S.; Chan, L.; Cheng, C.-H. Machine Learning Aided Electronic Warfare System. *IEEE Access* **2021**, *9*, 94691–94699. [CrossRef]

81. You, S.; Diao, M.; Gao, L. Deep Reinforcement Learning for Target Searching in Cognitive Electronic Warfare. *IEEE Access* **2019**, *7*, 37432–37447. [CrossRef]
82. Jarvis, D.E. Machine Learning of an Approximate Morphism of an Electronic Warfare Simulation Component. In Proceedings of the 2020 Spring Simulation Conference (SpringSim), Fairfax, VA, USA, 19–21 May 2020; pp. 1–12. [CrossRef]
83. Shao, G.; Chen, Y.; Wei, Y. Convolutional Neural Network-Based Radar Jamming Signal Classification With Sufficient and Limited Samples. *IEEE Access* **2020**, *8*, 80588–80598. [CrossRef]
84. Siemuri, A.; Selvan, K.; Kuusniemi, H.; Valisuo, P.; Elmusrati, M.S. A Systematic Review of Machine Learning Techniques for GNSS Use Cases. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, *58*, 5043–5077. [CrossRef]
85. Lee, G.-H.; Jo, J.; Park, C.H. Jamming Prediction for Radar Signals Using Machine Learning Methods. *Secur. Commun. Netw.* **2020**, *2020*, 2151570. [CrossRef]
86. Satapathy, J.R.; Bodade, R.M.; Ayeelyan, J. CNN based Modulation classifier and Radio Fingerprinting for Electronic Warfare Systems. In Proceedings of the 2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 14–15 May 2024; pp. 1880–1885. [CrossRef]
87. Wrabel, A.; Graef, R.; Brosch, T. A Survey of Artificial Intelligence Approaches for Target Surveillance With Radar Sensors. *IEEE Aerosp. Electron. Syst. Mag.* **2021**, *36*, 26–43. [CrossRef]
88. Lee, H.; Kim, C.F.; Kim, M.-S.; Kim, Y.-H.; Park, H.-K.; Lee, J.-S. Fault Detection of Air Defense Radar Systems Using Machine Learning. In Proceedings of the 2024 18th International Conference on Ubiquitous Information Management and Communication (IMCOM), Kuala Lumpur, Malaysia, 3–5 January 2024; pp. 1–7. [CrossRef]
89. Oveis, A.H.; Giusti, E.; Ghio, S.; Martorella, M. A Survey on the Applications of Convolutional Neural Networks for Synthetic Aperture Radar: Recent Advances. *IEEE Aerosp. Electron. Syst. Mag.* **2022**, *37*, 18–42. [CrossRef]
90. Kellett, J.; Dawber, W.; Wallace, W.; Branson, J. Multifunction Maritime Radar and RF Systems—Technology Challenges and Areas of Development. *IEEE Aerosp. Electron. Syst. Mag.* **2022**, *37*, 6–20. [CrossRef]
91. Rizvi, S.M.D.; Ahmad, S.; Khan, K.; Hasan, A.; Masood, A. Deep Learning Approach for Fixed and Rotary-Wing Target Detection and Classification in Radars. *IEEE Aerosp. Electron. Syst. Mag.* **2022**, *37*, 32–42. [CrossRef]
92. Ma, L.; Zhang, Y.; Leiva, V.; Liu, S.; Ma, T. A new clustering algorithm based on a radar scanning strategy with applications to machine learning data. *Expert Syst. Appl.* **2022**, *191*, 116143. [CrossRef]
93. Hu, J.; Wei, Z.; Li, Y.; Li, H.; Wu, J. Designing Unimodular Waveform(s) for MIMO Radar by Deep Learning Method. *IEEE Trans. Aerosp. Electron. Syst.* **2021**, *57*, 1184–1196. [CrossRef]
94. Yavuz, F. Radar Target Detection with CNN. In Proceedings of the 2021 29th EUSIPCO, Dublin, Ireland, 23–27 August 2021; pp. 1581–1585. [CrossRef]
95. Ozdemir, M.R.; Kucuk, A.F.; Inalhan, G.; Baspinar, B.; Ertekin, S. Machine Learning Based Radar Cross-Section Clustering Towards Enhanced Situational Awareness for Next-Generation Fighter Aircraft. In Proceedings of the 2024 AIAA DATC/IEEE 43rd DASC, San Diego, CA, USA, 29 September–3 October 2024; pp. 1–8. [CrossRef]
96. Aissa, S.B.; Letaifa, A.B. UAV Communications with Machine Learning: Challenges, Applications and Open Issues. *Arab. J. Sci. Eng.* **2022**, *47*, 1559–1577. [CrossRef]
97. Kumbasar, N.; Kılıç, R.; Oral, E.A.; Ozbek, I.Y. Comparison of spectrogram, persistence spectrum and percentile spectrum based image representation performances in drone detection and classification using novel HMFFNet: Hybrid Model with Feature Fusion Network. *Expert Syst. Appl.* **2022**, *206*, 117654. [CrossRef]
98. Orzechowski, P.F.; Burger, C.; Lauer, M. Decision-Making for Automated Vehicles Using a Hierarchical Behavior-Based Arbitration Scheme. In Proceedings of the 2020 IEEE IV Symposium, Las Vegas, NV, USA, 19 October–13 November 2020; pp. 767–774. [CrossRef]
99. Group, T. Thales to Lead European AI-Driven Cyberdefence Project for Aircraft Systems. Available online: https://defence-industry.eu/thales-to-lead-european-ai-driven-cyberdefence-project-for-aircraft-systems (accessed on 15 July 2025).
100. Group, T. Thales Group AI-Enhanced Radar Systems for Air Defense. Available online: https://www.thalesgroup.com/en/airborne-surveillance-radar (accessed on 15 July 2025).
101. Systems, B. ASTREA Project: Autonomous Systems Technology Related Airborne Evaluation & Assessment. *BAE Systems News*, 1 July 2006. Available online: https://web.archive.org/web/20161029203024/http://astraea.aero/ (accessed on 15 July 2025).
102. Govtribe. Industry Day for the Advanced Targeting and Lethality Automated System (ATLAS) Program. Available online: https://govtribe.com/opportunity/federal-contract-opportunity\/industry-day-for-the-advanced-targeting-and-lethality-automated-system-atlas-program-w909my19rc004 (accessed on 15 July 2025).
103. Stutzer, A.; Zehnder, M. *Camera Surveillance as a Measure of Counterterrorism?* Economics of Security Working Paper Series 34; DIW Berlin, German Institute for Economic Research: Berlin, Germany, 2010.

104. Gómez Mármol, F.; Ruipérez-Valiente, J.A.; Nespoli, P.; Martínez Pérez, G.; Rivera Pinto, D.; Larriva Novo, X.A.; Álvarez-Campana, M.; Villagrá González, V.; Maestre Vidal, J.; Rodriguez López, F.A.; et al. COBRA: Cibermaniobras adaptativas y personalizables de simulación hiperrealista de APTs y entrenamiento en ciberdefensa usando gamificación. In Proceedings of the VI JNIC 2021. Available online: https://hdl.handle.net/10578/28661 (accessed on 15 July 2025).
105. Spanish Minsitry of Defense COINCIDENTE (Cooperación en Investigación Científica y Desarrollo en Tecnologías Estratégicas). Available online: https://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Presentacion/ImasD/Paginas/Coincidente.aspx (accessed on 15 July 2025).
106. DARPA. DARPA and Artificial Intelligence for Military Operations. Available online: https://www.darpa.mil (accessed on 15 July 2025).
107. DARPA. DARPA's OFFSET Program: Autonomous Swarming for Combat Operations. Available online: https://www.darpa.mil/research/programs/offensive-swarm-enabled-tactics (accessed on 15 July 2025).
108. DARPA. Lifelong Learning Machines (L2M): Enhancing Cybersecurity Through AI. Available online: https://www.darpa.mil/program/lifelong-learning-machines (accessed on 15 July 2025).
109. DARPA. Artificial Intelligence for Military Operations (AIMO): Optimizing Military Precision with AI. Available online: https://www.darpa.mil/research/programs (accessed on 15 July 2025).
110. Dynamics, G. General Dynamics AI Integration in Defense Technologies. Available online: https://www.klover.ai/general-dynamics-ai-strategy-analysis-of-dominance-in-aerospace-defense-ai/ (accessed on 27 August 2025).
111. Vázquez, D. El Pentágono Desarrolla una IA para Anticipar Problemas Antes de Surjan en Zonas de Conflicto. Available online: https://www.businessinsider.es/pentagono-desarrolla-ia-anticipar-problemas-909385 (accessed on 15 July 2025).
112. Tingley, B. TheDrive. Available online: https://www.thedrive.com/the-war-zone/41771/the-pentagon-is-experimenting-with-using-artificial-intelligence-to-see-days-in-advance (accessed on 15 July 2025).
113. Ross, P.E. What Does Iron Dome Prove About Antimissile Systems? *IEEE Spectr.* 28 December 2012. Available online: https://spectrum.ieee.org/what-does-iron-dome-prove-about-antimissile-systems (accessed on 27 August 2025).
114. Martin, L. Lockheed Martin Leverages AI and Machine Learning to Revolutionize Defense and Space Technology. Available online: https://www.lockheedmartin.com/en-us/news/features/2024/lockheed-martin-leverages-ai-and-machine-learning-to-revolutionize-defense-and-space-technology.html (accessed on 15 July 2025).
115. Department of Defense, U.S. Pentagon's Project Maven: AI for Analyzing Drone Footage. *DefenseOne* **2024**. Available online: https://www.giest.or.jp/en/contents/briefs/2872/ (accessed on 27 August 2025).
116. China North Industries Group Corporation Limited NORINCO Develops AI-Driven Autonomous Military Drones. Available online: http://en.norincogroup.com.cn/col/col441/index.html (accessed on 15 July 2025).
117. NORINCO. Chinese NORINCO Unveils Compact Anti-Drone, Electronic Warfare Systems for Tanks. DefenseMirror. 2024. Available online: https://www.defensemirror.com/news/38127 (accessed on 15 July 2025).
118. Grumman, N. Northrop Grumman's AI Integration in Defense Technologies. *Northrop Grumman News*, 1 July 2024.
119. Grumman, N. Artificial Intelligence Applications in Defense by Northrop Grumman. *Defense News*, 1 July 2024.
120. Group, K. Russia's AI Integration in Autonomous Combat Robots and Missile Systems. *Defense Industry News*, 8 November 2021.
121. Almaz-Antey. Russia's Smart Missile Systems and AI Development in Defense. *Russia Defense News*, 1 July 2024.
122. Hi-iberia. SEDA: SatEllite Data AI. Available online: https://seda.hi-iberia.es/en/ (accessed on 15 July 2025).
123. del Rio Durán, J.D. Mantenimiento Inteligente en la Armada: En Vanguardia y Trazando el Futuro. *Rev. Gen. Mar.* **2021**, *281*, 4.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.