https://doi.org/10.1590/jatm.v18.1436 ORIGINAL PAPER

Evolution of Methods for Countering Drone-Based Airborne Threats

Andrii Volkov[1,*], Serhii Oriehov[1], Volodymyr Stadnichenko[1], Oleksandr Tokar[1], Vitalii Yaroshchuk[1]

1. Ivan Kozhedub Kharkiv National Air Force University – Department of Tactics of the Air Defence Forces of the Land Forces – Kharkiv – Ukraine.

*Corresponding author: andriivlkv@gmail.com

ABSTRACT

The purpose of this study was to identify key stages in the evolution of air defense concepts and evaluate effective approaches to neutralizing modern airborne threats, particularly drones. The research involved analyzing open scientific sources, defense agency reports, and systematizing cases of successful counteractions to drones, with a focus on countries like Israel, Turkey, the United States of America, and Ukraine. The study found that countermeasure effectiveness depends on integrating electronic warfare, cyber tools, physical interception, and artificial intelligence (AI)-based detection algorithms. The use of sensor platforms, electromagnetic countermeasures, and software components reduced response times and improved target disabling probability without kinetic effectors. However, existing air defense systems were largely unprepared for swarm attacks from miniature drones, with conventional weapons lacking energy autonomy for prolonged counteraction. The research highlighted the need for multi-layered defense architectures with a cognitive response cycle under 5 seconds and advanced AI integration. Additionally, international cooperation and information exchange were crucial for developing sustainable early warning systems. The study's findings can inform the modernization of national air defense programs and regulatory frameworks addressing unmanned technology challenges.

Keywords: Unmanned aerial vehicles; Air defense; Sensors; Artificial intelligence; Radar; Electromagnetic countermeasures.

INTRODUCTION

Increasing the intensity and complexity of threats from the air has become one of the key characteristics of the security situation in the 21st century, particularly in countries experiencing high adoption of unmanned aerial technologies or active conflict zones, such as the United States of America (USA), Israel, Turkey, Ukraine, France, and South Korea. These threats include small- and medium-sized drones, swarms, loitering munitions, and autonomous aerial platforms capable of reconnaissance, surveillance, and precision strikes. Considerable attention was drawn to the mass distribution of unmanned aerial vehicles (UAVs) capable of performing a wide range of tasks – from reconnaissance and surveillance to delivering pinpoint strikes and psychological pressure.

Recent survey studies systematically analyze these emerging threats and highlight the limitations of classical air defense systems in countering them (Park *et al.* 2021; Seidaliyeva *et al.* 2023; Yu *et al.* 2025). These reviews emphasize that while individual technical solutions exist, they do not provide a comprehensive framework integrating detection, neutralization, and management strategies for UAV threats across multiple operational and regulatory contexts. Although numerous studies have explored isolated technical approaches, the present study contributes novel insights by proposing a comprehensive, multi-level air defense framework supported by a structured technical model that integrates detection, effectors, artificial intelligence (AI)-based analysis, and regulatory components, enabling readers to readily visualize the system architecture.

Received: Dec. 05, 2025 | **Accepted:** Mar. 20, 2026
Peer Review History: Single Blind Peer Review.
Section editor: Adam Cumming

CC BY

The use of drones in real conflicts has shown that these vehicles can operate both separately and as part of complex coordination groups, which significantly complicates the task of detecting and neutralizing them (Seidaliyeva and Smailov 2025; Wójcik *et al.* 2022). Evidence from recent operational reports and analytical studies indicates that classical air defense systems aimed primarily at larger targets may not provide adequate protection against these emerging airborne threats (Park *et al.* 2021; Seidaliyeva *et al.* 2023). This highlights a gap in the literature, as existing studies have not fully addressed integrated multi-level responses to small and agile aerial threats.

Contemporary strategies integrate interception microdrones, AI-enhanced swarm trajectory forecasting, electronic warfare, and cyber interventions to mitigate these threats, while ethical supervision via human-on-the-loop (HOTL) and human-in-the-loop (HITL) protocols guarantees secure autonomous functioning (Cherniha and Serov 2006; Constantinescu and Dumitrache 2022; Wang *et al.* 2023). In contrast to prior studies focusing on individual solutions, this research differentiates itself by systematically analyzing how multiple technical and organizational components can be combined into a coherent, integrated framework to support decision-making, automated interception, and operational coordination across national air defense models.

Recent studies have progressively emphasized the significance of human participation in AI-driven air defense systems. Two operational paradigms, HITL and HOTL, are essential for guaranteeing system dependability and adaptability. In the HITL paradigm, humans actively participate in decision-making, overseeing and evaluating AI actions in real time, which is crucial for reducing errors in dynamic threat situations (Cherniha and Serov 2006; Trofymenko *et al.* 2024). In contrast, HOTL frameworks position people in a supervisory capacity, intervening just when automated systems necessitate guidance or correction, hence facilitating expedited autonomous responses while maintaining human oversight (Constantinescu and Dumitrache 2022; Wang *et al.* 2023). These operational paradigms are incorporated into the proposed framework to ensure both technical and ethical robustness.

The growth of aerial threats associated with the widespread use of UAVs has stimulated the development of new air defense concepts based on the integration of heterogeneous detection and neutralization tools (Dahan *et al.* 2025a; Hula and Hryha 2024). Multicomponent systems combining optical, radio frequency (RF), and acoustic channels with physical means of interception are most effective (Gonzalez-Jorge *et al.* 2024). However, existing literature rarely synthesizes these technologies in a way that connects technical, operational, and regulatory perspectives. This study addresses this by providing a comparative framework that clearly links system architecture, functional modules, and national doctrinal considerations.

In turn, Khawaja *et al.* (2022) emphasized that contemporary anti-drone solutions should consider not only the physical destruction of vehicles but also the need to suppress their control channels through electronic jamming methods. This implies the integration of electronic warfare equipment into the structure of air defense systems as a critical component. Survey literature also highlights that a combination of kinetic and non-kinetic measures is crucial for effective counter-UAV operations (Yu *et al.* 2025; Zhao *et al.* 2023). The proposed paradigm visually encapsulates these connections, illustrating how several modules mutually reinforce one another to attain operational synergy.

The development of multi-level defense complexes is particularly relevant for urban conditions, where, according to the results of the analysis by Iman *et al.* (2023), systems with adaptive distribution of firepower capable of covering different echelons of airspace demonstrated the best efficiency. Their effectiveness is determined not only by their technical specifications, such as radar range, response time, and firing accuracy, but also by their architectural design, networked command structures, and the ability to quickly reconfigure operational parameters in response to dynamic threat scenarios. Survey studies indicate that urban air defense requires both technical integration and operational coordination, which remains an underexplored area (Seidaliyeva *et al.* 2023).

The study by Rugo *et al.* (2022) found that numerous existing approaches to providing air defense often lack systemic compatibility, especially regarding interoperability across unmanned networks and multi-echelon defense layers. In this regard, the concept of unified data exchange was proposed as a technical and organizational solution to enhance interoperability, data fusion, and real-time coordination between heterogeneous defense systems. In the context of adapting air defense to fleeting conflict scenarios, Romaniuk and Bieliev (2025) analyzed methods of using AI to improve the effectiveness of combat management. Specifically, AI integration allows for dynamic threat prioritization, automated resource allocation, and predictive engagement algorithms that support multi-level operational coordination. The integration of AI in air defense, as emphasized in several survey studies, enables the prediction of airborne threat patterns and the optimization of response algorithms (Yu *et al.* 2025; Zhao *et al.* 2023).

The study by Yoo and Jang (2023) analyzed the role of cooperation between anti-aircraft systems with different control channels. They demonstrated that coordinated networked operations, supported by a structured command hierarchy, substantially increase interception success rates during multi-level attacks, highlighting the necessity of integrated system architectures that combine sensors, effectors, and command nodes. The study by Volkov *et al.* (2023; 2024) proposed an air defense architecture for important facilities that combines the capabilities of air defense and electronic warfare equipment. Simulation results confirmed that such integrated architectures enable the synergistic use of countermeasures, enhancing drone neutralization efficiency by up to 75% at altitudes up to 500 meters.

Application of supported learning methods allows not only predicting drone trajectories but also dynamically adjusting system parameters and reassigning resources in real time, thereby enhancing the operational responsiveness of multi-level air defense networks, as highlighted in survey studies on AI-based air defense systems (Jiang *et al.* 2023; Zhao *et al.* 2023). Ultimately, considerable attention was drawn to the analysis of deep neural networks for automatic recognition of aerial targets based on radar signatures, as presented in the paper by Jiang *et al.* (2023). The study emphasized that integrating such AI-driven detection with system-level coordination mechanisms significantly improves detection accuracy and target prioritization under conditions of high electronic noise or adversarial interference.

However, despite these advances, the literature reveals clear gaps. Most studies concentrate on individual technical solutions, such as AI-based detection, radar signal processing, or electronic jamming, but they do not provide a systematic framework for integrating these components with organizational processes and regulatory requirements into a coherent multi-level air defense system. Moreover, there is limited research on real-time coordination of multi-level systems in complex urban and battlefield scenarios, and on how different national models can be adapted to evolving autonomous drone swarms (Park *et al.* 2021; Seidaliyeva *et al.* 2023; Yu *et al.* 2025). This paper proposes a structured comparison methodology that connects technical performance, organizational coordination, and regulatory compliance to improve operational resilience against contemporary airborne threats.

Thus, the review of contemporary scientific literature indicates the development of a conceptual shift from isolated technical solutions to integrated, multi-level, technically and operationally coherent systems for countering airborne threats, while highlighting the specific research gap this study addresses: the absence of a structured framework linking technical, organizational, and regulatory dimensions.

Research objectives

- To systematize and technically categorize existing architectural and functional approaches to constructing air defense systems, including multi-echelon and networked designs.
- To identify key factors that determine the effectiveness of air defense systems against modern airborne threats.
- To develop a structured comparative framework for evaluating national air defense models and emerging counter-drone technologies, accounting for technical performance, operational protocols, and integration capabilities.
- To provide actionable recommendations for integrating technical, organizational, and regulatory components into coherent, multi-level defense architectures with demonstrable operational effectiveness.

Considering the above, the study hypothesized that the effectiveness of countering airborne threats is determined by the degree of integration of technical and organizational components into a single concept of air defense. Such integration enables not only risk reduction for critical infrastructure but also the establishment of proactive threat prevention mechanisms, including predictive resource allocation, adaptive engagement strategies, and regulatory compliance within unified operational frameworks.

Finally, this manuscript is structured as follows: The Introduction traces the evolutionary phases of airborne threat counteraction from 1990 to 2024. The Methodology presents a typology of methods, tools, and strategies for countering unmanned threats. The Results provide a comparative analysis of national air defense models. The Discussion synthesizes findings and evaluates operational and regulatory considerations, while the Conclusion summarizes key results and outlines potential avenues for future research.

CC BY

METHODOLOGY

To achieve this goal, a theoretical analysis of materials related to the evolution of methods and techniques for countering airborne threats was carried out. The analysis specifically covered the historical period from 2013 to 2024 and included publicly available sources (open-access materials accessible online) and partially declassified materials (obtained from open databases or officially released by defense agencies), which allowed recreating key stages in the development of air defense systems in response to the latest threats. The study used defense strategies, patent documentation, technical reports, situational reviews, and analytical materials reflecting the transformation of air defense architectures and principles for integrating sensor, effector, and analytical components.

The body of sources includes official documents of defense departments – in particular, the DoD (2013; 2023), the analytical report of the MoAF (2023), the industry development profile of the IISS (2024), and reports of the INSS (2023), MND (2022), and the Unmanned Systems Forces of Ukraine (2024). They summarized the concepts of building multi-level systems for countering airborne threats, including swarms of drones and high-speed platforms. The technical parameters of sensor and effector devices were reconstructed on the basis of open specifications of defense companies Lockheed Martin (USA), Elbit Systems (Israel), Thales (France), Aselsan (Turkey), Hanwha (South Korea), and Baykar (Turkey). Particular attention was given to the integration of these technical solutions into cohesive multi-tiered systems that amalgamate detection, effectors, and command networks, thereby ensuring interoperability and swift adaptive reaction.

The analysis also included analytical reports from international organizations, in particular the UN (2024), which summarized the experience of using UAVs by non-state actors for attacks on critical infrastructure facilities. All sources allowed tracking not only the technical characteristics of systems but also operational integration strategies required for multi-level urban defense. The selected period of 2013 to 2024 ensured representativeness of the materials and reflected the main stages of the transition from centralized air defense systems to integrated, adaptive, and cognitive architectures capable of operating under multi-factor threats and information overload.

For the theoretical reconstruction of methods and methods of countering airborne threats, logical and analytical approaches were used, which made it possible to structure the available information according to the hierarchy: "approach → method → tool → strategy." The physical domains of action (kinetic, electromagnetic, informational, etc.) were consistent with the corresponding methods of influence, which allowed systematizing technological solutions within a unified typology. A comparative analysis of six national models (USA, Israel, France, Turkey, Ukraine, South Korea) was conducted, considering technical integration, multispectral coverage, response speed, degree of autonomy, scalability, and interoperability. This provided a basis for evaluating the operational effectiveness of multi-level defense architectures. Characteristics were recorded based on the analysis of official reports, technical documentation, and patents, and then summarized in a table to identify functional differences and advantages.

Within the framework of the methodological approach, a functional grouping of components of architectures of systems for countering threats from the air was applied. The analysis was carried out considering three main functional blocks:

- Detection tools (radar, optoelectronic, acoustic, multisensory).
  - Weapons of destruction:
  - Kinetic – missiles, portable anti-aircraft missile systems, anti-aircraft installations.
- Non-kinetic – electronic warfare and laser interception systems.
- Control and coordination systems (combat control centers, network nodes, automated algorithmic decision-making systems).

These were further analyzed through the lens of HITL and HOTL paradigms. In HITL configurations, human operators actively participate in real-time decision-making, validating AI-generated responses and ensuring reliability, whereas in HOTL configurations, humans supervise autonomous processes, intervening selectively only when corrective actions are needed (Cherniha and Serov 2006; Constantinescu and Dumitrache 2022; Trofymenko *et al.* 2024; Wang *et al.* 2023). This distinction allowed the study to evaluate both speed and safety of integrated air defense responses in dynamic threat scenarios.

Additionally, the typology of potential threats was integrated into the framework. Threats were classified by mode of action (kinetic vs. non-kinetic) and autonomy (operator-controlled vs. autonomous), supporting comparative evaluation of national models within a unified matrix.

Data aggregation was carried out through a systematic content analysis of materials that were open or partially declassified. To ensure reliability and support the technical contributions, the criterion of confirmation by at least three independent sources was applied to validate duplicate architectural elements and functional modules. Text fragments related to architectural components, detection and neutralization methods, and organizational strategies were coded according to predefined categories (e.g., detection tools, kinetic and non-kinetic weapons, control systems) by two independent analysts using NVivo 14 software, achieving a Cohen's $\kappa = 0.82$ agreement coefficient. This rigorous coding approach allowed the study to systematically categorize technical and organizational solutions across different national models, directly supporting Objective 1 (systematization of architectural and functional approaches).

Due to the nominal nature of the data, statistical processing was limited to frequency counting, without parametric tests. Generalization was conducted based on the recurrence of conceptual solutions across strategic documents, technical reports, and patents, ensuring the identification of robust, transferable architectural patterns. This process also enabled the identification of key factors that influence operational effectiveness, addressing Objective 2 (determining effectiveness factors for air defense systems).

The research followed a staged and logically consistent methodology, transitioning from theoretical justification to comparative analysis:

- Formulation of a system of criteria for evaluating architectures for countering threats from the air, including functional completeness, integration of technical and organizational elements, responsiveness to asymmetric scenarios, availability of automated controls, and inclusion of HITL/HOTL elements to ensure human oversight in AI-assisted decision-making, as well as inclusion of non-kinetic strike technologies (Cherniha and Serov 2006; Constantinescu and Dumitrache 2022; Trofymenko *et al.* 2024; Wang *et al.* 2023). This step directly supports Objective 4 by establishing the basis for integration recommendations.
- Collection of information on existing national architectures of air defense systems and anti-drone platforms from open analytical materials, strategic documents, technical documentation, and patents (DoD 2013; 2023; IISS 2024; INSS 2023; MND 2022; MoAF 2023; Unmanned Systems Forces of Ukraine 2024), enabling development of a comparative framework (Objective 3).
- Functional analysis of collected architectures, highlighting key differences in detection, neutralization, and management approaches, including integration of AI modules (Jiang *et al.* 2023; Yu *et al.* 2025; Zhao *et al.* 2023). This step provided a technical foundation for evaluating system effectiveness and identifying design trade-offs.
- Summarization of results, forming a final comparative table for evaluating effectiveness, and interpreting them considering the strategic features of each model. This final stage synthesized technical, organizational, and regulatory components into a coherent multi-level evaluation framework, supporting Objective 4.

Evaluation of the effectiveness of methods of countering airborne threats was carried out within the framework of a logical and analytical model, which provided for comparing architectures by key functional features. The performance indicator recognized the potential for reducing the "detection-evaluation-response" cycle to 5 seconds, provided that the classification accuracy (Park *et al.* 2021). Analytical assertions were considered valid only if confirmed by at least two independent sources of different types (e.g., a patent and a defense report), enhancing conceptual reliability. Operational validation included open reports such as the destruction of 47 attack UAVs during December 2024 (Reuters 2024), illustrating practical effectiveness. Strategic documents (DoD 2023) guided analysis of AI integration in situational awareness, effector control, and accelerated decision-making in multi-factor threat environments.

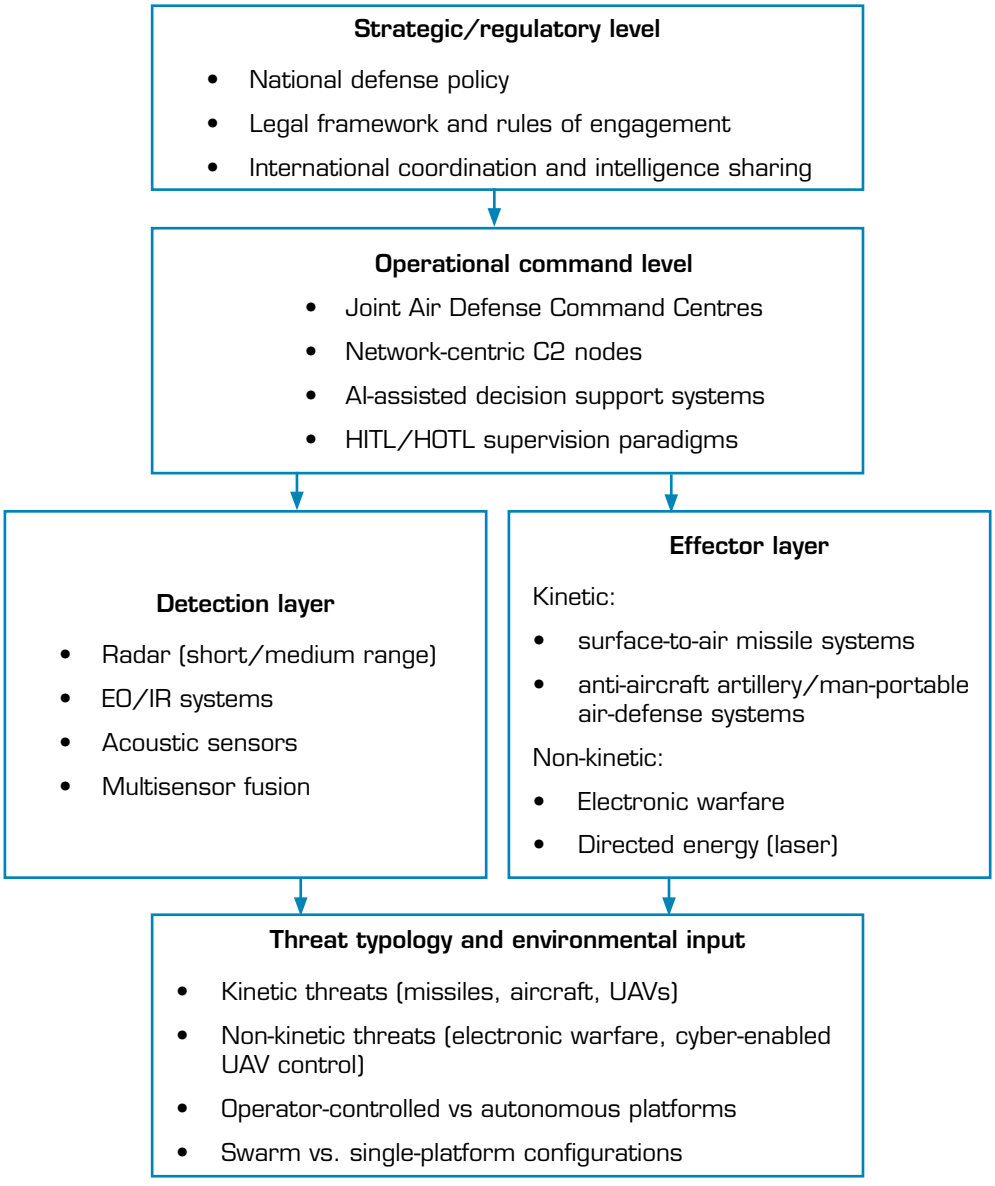
Special attention was given to UAV-specific countermeasures, considered a distinct class of threats due to their tactical and detection features. The study applied criteria such as flight speed, altitude, signature characteristics, platform type, and deployment configuration (individual vs. swarm). Sources included technical specifications of sensors and neutralization devices, doctrinal response provisions, and empirical case studies. The UN (2024) global report provided an empirical basis for non-state threats, summarizing UAV attacks on critical infrastructure by non-state actors, including terrorist groups.

Through this approach, the study systematically linked technical, organizational, and regulatory aspects, thereby:

- Supporting Objective 1: systematizing architectural and functional approaches.
- Supporting Objective 2: identifying factors influencing effectiveness (integration, automation, HITL/HOTL, multispectral coverage).
- Supporting Objective 3: developing a comparative framework for national air defense models and emerging counter-drone technologies.
- Supporting Objective 4: providing recommendations for integrating components into coherent, multi-level air defense architectures.

CC BY

Figure 1 illustrates the resulting multi-level framework, showing layers of detection, effectors, and control, the integration of AI-assisted decision-making, and the interaction of kinetic and non-kinetic countermeasures with operational and strategic layers.



Source: Elaborated by the authors.

Figure 1. Integrated multi-level framework for the evaluation and design of air defense architectures.

The study consolidates the identified architectural, functional, organizational, and regulatory components into a cohesive multi-level analytical model to enhance conceptual clarity and reinforce the technical justification of the suggested comparison framework. This model aims to systematize the structural logic of contemporary air defense systems and visually illustrate the interplay of detection assets, effectors, command-and-control mechanisms, and decision-support tools across hierarchical levels.

The framework integrates the findings from the content analysis, comparative assessment of national models, and functional categorization of system components. It incorporates essential performance factors – such as degree of automation, multispectral

coverage, interoperability, and HITL/HOTL integration – within a unified design. This conceptual integration directly facilitates Objectives 1-4 of the study by unifying systematization, effectiveness factors, comparative evaluation, and integration recommendations within a cohesive analytical framework. The resultant multi-tiered system is illustrated in Fig. 1.

The proposed architecture, as depicted in Fig. 1, is organized into three interrelated levels: strategic/regulatory, operational command, and tactical response. The tactical layer amalgamates detection systems (radar, electro-optical [EO]/infrared, acoustic, and multisensor platforms) with kinetic and non-kinetic effectors, interconnected via real-time data fusion and automated cueing mechanisms. The operational level includes network-centric command nodes and AI-enhanced decision-support systems functioning under HITL and HOTL supervision frameworks. The strategic layer incorporates legislative frameworks, engagement protocols, and interagency coordination mechanisms that influence operational deployment.

The model incorporates threat typology by differentiating between kinetic and non-kinetic threats, autonomous and operator-controlled platforms, and swarm configurations in the decision-making process. This facilitates the comparative assessment of national air defense designs within a cohesive matrix of functional completeness, responsiveness, and integration maturity.

RESULTS

Evolutionary phases of airborne threat counteraction (1990-2024)

During retrospective analysis, it was traced that each wave of technological innovations in the military-industrial complex catalyzed transitions between conceptually different paradigms of air defense. These developments signified not just alterations in weapon types but also a structural reconfiguration of air defense infrastructures, encompassing sensor topology, effector deployment logic, and command-and-control distribution.

Initially, in the 1990s, the doctrine was based on stratified missile-gun "belts" of cover, where all-around radar stations provided continuous detection of manned aircraft and long-range cruise missiles. Decisions were made centrally, and the sensor system was based on long-range radar stations. Architecturally, this phase can be characterized as vertically integrated and radar-dominant, with low autonomy at tactical nodes and a linear "detection-command-engagement" chain.

Since 2005, due to the massive spread of tactical UAVs, a reorientation to the electromagnetic mode of action has been recorded, within which blocking and jamming methods became dominant. Optical-electronic sensors, laser rangefinders, and mobile electronic warfare modules were introduced, reducing the response cycle to tens of seconds (Korzhyk *et al.* 2017; Smailov *et al.* 2025). Recent developments have also integrated AI-assisted sensor fusion, combining RF signal analysis, vision-based tracking, and infrared detection to improve identification accuracy and reduce false positives in cluttered environments. This stage marked the transition from zonal territorial coverage to point-defense architectures protecting critical infrastructure nodes, demonstrating increased decentralization and tighter sensor-effector coupling.

Since 2015, against the backdrop of growing threats in the form of swarms of drones and barraging ammunition, dominance has shifted to cyber and information methods. Edge processing, passive scanners, and network synchronization of effector actions were integrated, providing functional autonomy and dynamic adaptation to threat scenarios. Edge computing, real-time battlefield communication, and AI-based threat prediction have been implemented, allowing autonomous decision-making at the tactical node level and reducing operator load. Passive scanners and network-synchronized effectors provided functional autonomy and dynamic adaptation to threat scenarios (Cherniha and Serov 2006; Petrov *et al.* 2023). This phase signifies the establishment of a network-centric, multi-layer architecture defined by distributed processing, horizontal data sharing, and the reduction of the "detection-evaluation-response" cycle to just seconds.

The transition in 2005-2015 to the mass use of tactical drones demonstrated that the low effective scattering area and low-altitude flight reduced the effectiveness of radar-only coverage. Opto-electronic sensors, laser rangefinders, and directional electronic suppression units were integrated; the response cycle was reduced to tens of seconds, and protection began to focus on critical "points" of infrastructure instead of the entire "zone." This phase signifies a transition from radar-focused zonal defense to hybrid sensor frameworks that include electromagnetic and optical detection methods, facilitating the systematic adaptation of architectural processes in response to low-signature threats (Objective 1).

CC BY

After 2015, autonomous swarms of microdrones and barraging ammunition forced defense structures to combine passive RF scanners, multispectral cameras, and edge computing modules with AI, which eventually formed the network-centric nature of air defense and reduced the "detection-evaluation-interception" cycle to seconds. The incorporation of distributed sensors, AI-driven classification, and synchronized effectors exemplifies the development of multi-layer adaptive architectures defined by decentralized processing and horizontal data exchange, establishing the structural foundation for the comparative assessment of contemporary air defense models (Objective 3).

The chronological sequence of evolutionary phases of countering airborne threats was reconstructed on the basis of open technical reports and analyses, including DoD (2013; 2023) and MoAF (2023). Table 1 summarizes the key features of each phase, which allows clear comparison of the dominant threats with the corresponding doctrinal and technical solutions. This structuring immediately facilitates the systematization of architectural and functional methodologies, establishing a cohesive matrix that connects threat type, sensor configuration, effector class, and command paradigm (Objectives 1 and 3).

Table 1. Stages in the development of countermeasures to airborne threats (1990-2024).

Phase	Dominant threats	Leading paradigm	Typical sensors	Typical effectors
1990-2005	Manned aircraft, cruise missiles > 300 km	Stratified zonal defense	Long-range radar station, altimeters	Medium/long-range anti-aircraft missile system, artillery
2005-2015	Tactical UAVs, speed < 200 km·h	Extended "kill chain" with EO/IR channel	X-band radar, EO/IR cameras, laser rangefinders	Portable anti-aircraft missile systems, mobile electronic warfare modules
2015-2024	Swarms of microdrones, barraging ammunition	Integrated multi-layer defense	Combined radar stations + EO/IR + signals intelligence, passive RF scanners	Kinetic interceptor drones, solid-state lasers, and broadband electronic warfare equipment

Source: Elaborated by the authors based on Khawaja *et al.* (2022), Romaniuk and Bieliaiev (2025), and Volkov *et al.* (2025).

The role of sensors and effectors changed at each stage in accordance with the current conceptual approach. In the first phase, the main sensors remained the long-range radar stations, which provided early warning, while effectors in the form of anti-aircraft missile systems worked within a tightly centralized structure. In the second phase, the sensors gained mobility and were supplemented with optical and infrared channels, which allowed localizing air targets at low altitudes. The effectors became adaptive – portable anti-aircraft missile systems and mobile electronic warfare systems were used for precision strikes. The third phase was marked by the transition to multisensory networks with local data processing, where passive RF scanners, multispectral cameras, and machine learning (ML) modules with advanced processors became key. The effectors were represented by high-precision interceptor drones, solid-state lasers, and directional energy pulses. Summarizing, each subsequent phase provided for a decrease in centralization, an increase in the speed of response and the transition from a reactive response to proactive adaptation, which determined the logic of the development of the air defense architecture. Across the identified phases, three key effectiveness factors can be distinguished: (1) reduction of the detection-response cycle time; (2) degree of sensor-effector integration; and (3) level of automation and autonomy in decision-making. These factors constitute measurable determinants of operational effectiveness against modern airborne threats (Objective 2).

The recorded case of neutralization of 47 of the 72 attack drones launched on the territory of Ukraine in December 2024 showed the ability of the adapted air defense architecture to respond effectively to massive attacks, in particular by multi-level involvement of short- and medium-range effectors (Reuters 2024). This empirical example confirms the practical relevance of layered architectures combining kinetic and non-kinetic means within coordinated command structures.

During a detailed study of transformational dynamics, it was observed that the transition from stratified missile and gun "belts" to network-centric complexes occurred in leaps and bounds and was always initiated by external crisis events. In the 1990s, the alternation structure was based on a multi-level vertical of target confirmation, so the time reserves between missile

detection and launch were measured in minutes. The emergence of tactical UAVs in the first decade of the 21st century reduced these reserves to seconds, which forced the delegation of decision-making rights to lower echelons and the introduction of optoelectronic sensors directly at battery points. The massive use of swarms of barraging ammunition after 2015 forced the dispersal of computing power: edge processors automatically performed classification and trajectory prediction, and operators were left to authorize the level of escalation. This redistribution of computational capacity and decision authority demonstrates the necessity of integrating technical (AI modules, distributed sensors), organizational (delegated command levels), and regulatory (rules of engagement, escalation control) components into coherent multi-level defense architectures, thereby forming practical recommendations for architecture design (Objective 4). Training programs also underwent a shift: the share of time allocated for multisensory picture analysis increased from 10% to more than 50%, while the role of the classic "start map" gradually decreased.

Typology of ways, methods, and tools to counter unmanned threats

The systematization of countermeasures was carried out according to the four-level matrix approach → method → tool → strategy. The "approach" defined the physical domain of action, the "method" detailed the mechanism of action, the "tool" reflected the technical execution, and the "strategy" described the agreed sequence of application. This four-level decomposition facilitates the standardization of architectural and functional descriptions of air defense components, hence directly supporting Objective 1 (systematization of architectural and functional methodologies). By distinctly delineating the physical domain, mechanism of action, technical implementation, and operational sequencing, the matrix eradicates conceptual overlap among systems that, despite technical differences, adhere to the same architectural logic. The study confirmed that the effectiveness of the modern air defense system was determined by the synchronized operation of at least three methods, which mutually compensated for each other's weaknesses, and only in the final scenario did the escalation reach kinetic damage. This discovery facilitated the identification of a fundamental principle of effectiveness (Objective 2): operational resilience is optimized not through the supremacy of a singular approach, but via multi-layered redundancy and cross-domain synchronization.

In contemporary counter-UAV architectures, this synchronization is increasingly achieved through real-time battlefield communication networks and AI-assisted decision-support systems, which dynamically select and prioritize methods based on threat characteristics, environmental constraints, and legal limitations. This adaptive selection mechanism constitutes a structural element of the comparative framework (Objective 3), as it enables evaluation of national models according to the maturity of their AI integration, interoperability, and escalation management capabilities.

The hierarchical structure of methods, techniques, and means of countering unmanned threats was formed based on the technical specifications of Lockheed Martin, Thales, Elbit Systems, and Baykar, which allowed generalizing typical solutions for various air defense architectures. These solutions increasingly rely on multi-sensor platforms integrating radar, EO, infrared, acoustic, and radio-frequency sensors to enhance detection robustness and target identification accuracy in complex operational environments. The typology, therefore, serves not merely as a descriptive classification but as a functional mapping tool linking threat type, technological capability, and architectural configuration, which is essential for cross-national comparison (Objective 3). Table 2 provides a typology structure that eliminates semantic confusion between levels and allows standardizing the description of the capabilities of different platforms. This standardization is necessary for integrating technical, organizational, and regulatory components into coherent multi-level defense architectures (Objective 4), as it establishes a common analytical language across domains.

The kinetic method was implemented through direct physical damage to the target, which ensured its final neutralization. The nature of the impact consisted of the destruction or destruction of the device by mechanical contact – rocket, artillery, or drone interceptor. Efficiency was achieved under conditions of accurate guidance, availability of time for identification, and the absence of foreign objects in the fire zone. The main limitations were the need for high accuracy, the high cost of use, and the risk of collateral damage (accidental debris, damage to civilian targets in dense urban development).

Recent developments demonstrate that AI-based target classification and sensor fusion significantly improve the effectiveness of kinetic interception by reducing reaction time and increasing discrimination between UAVs and non-hostile objects. However,

CC BY

Table 2. Hierarchical typology of countermeasures against UAVs.

Level	Approach	Method	Tool	Strategy
1	Kinetic	Physical destruction of an object	Short/medium-range anti-aircraft missile systems, close-range air defense, and machine gun installations	Elimination of the threat by mechanical damage
2	Electromagnetic	Jamming, blocking, interception	Electronic warfare stations, RF suppressors, directional microwave systems	Temporary decommissioning or forced return without destruction
3	Cybernetic	Hacker attacks, navigation deceptions	Global positioning system/global navigation satellite system substitution tools that attack algorithms via communication channels	Exploiting software vulnerabilities for monitoring or defusing them
4	Informational	Cognitive manipulation, data falsification	Disinformation, fake goal tags, redirection	Creating a false idea of the environment or simulating the environment
5	Administrative	Access restrictions, bans, and legal mechanisms	Geofences, registration of UAVs, and prohibited air zones	Prevention of a threat before its implementation through regulation and control

Source: Elaborated by the authors based on Best *et al.* (2020), Yu *et al.* (2025), and strategic reviews and analytical materials (DoD 2013; 2023; IISS 2024; INSS 2023; MoAF 2023; UN 2024; Unmanned Systems Forces of Ukraine 2024).

these systems remain constrained by interceptor cost, limited magazine depth, and safety considerations in urbanized areas. Thus, for comparative evaluation purposes (Objective 3), kinetic effectiveness depends on three measurable parameters: interception probability, reaction time, and collateral risk profile.

In accordance with the provisions of the DoD (2023), the introduction of ML algorithms for processing streaming data from multi-channel sensor systems remained a key direction in the development of defense technologies. This allowed substantiating the feasibility of using an adaptive AI core in an integrated air defense architecture, especially for real-time target classification tasks. The presence or absence of such an adaptive AI core becomes a distinguishing criterion when evaluating national air defense models against emerging counter-drone technologies (Objective 3).

The electromagnetic method provided a non-contact effect by generating RF interference, jamming, or redirection. Its type of action was to disrupt the operation of the onboard electronics of UAVs without physical contact. Maximum efficiency was achieved against UAVs with open communication channels, without backup protocols or communication protection. The advantages were fast space coverage, area scalability, and minimal inertia. However, efficiency was dramatically reduced in the presence of shielding, digital stability, or when operating in a complex urban environment with high levels of radio interference.

Modern electronic warfare systems increasingly employ AI-driven adaptive jamming, capable of dynamically adjusting frequency bands and power levels in response to changing UAV communication patterns (Gospodinova and Nenov 2024; Gu *et al.* 2024). Effectiveness in the electromagnetic domain is therefore determined by spectrum adaptability, power efficiency, and resilience against encrypted or autonomous navigation systems, which represent critical technical evaluation criteria (Objective 2).

There is a general trend toward an increase in the role of non-state actors in the use of unmanned systems, which, according to the UN (2024), has already led to the spread of modified commercial platforms for strike operations in areas with limited control. This justified the need to adapt detection systems to non-standard and inconspicuous targets. From an architectural perspective, this trend expands the functional requirements of air defense systems, necessitating multispectral detection layers capable of identifying low-signature and commercially modified platforms, thereby reinforcing the systematization of detection approaches (Objective 1).

The cybernetic method was based on the hidden influence of information on the software or communication channels of UAVs. The main type of action was a remote attack on control or navigation protocols to disable the target or intercept its control. This approach was most effective against remotely controlled or semi-autonomous systems operating over open or known data channels. The limitation was the dependence on preliminary firmware analysis, knowledge of control commands and vulnerabilities,

and the presence of a backup channel or encrypted communication in the drone. The efficacy of the cybernetic layer is contingent upon protocol accessibility, incursion latency, and compatibility with superior command systems, enabling its integration as a quantifiable element within the comparative evaluation framework (Objective 3).

The effectiveness of cyber countermeasures is further constrained by the growing use of encrypted links, proprietary protocols, and on-board AI, which reduce reliance on external communication and limit opportunities for remote interference (Barlybayev and Turginbayeva 2025; Barlybayev *et al.* 2024). This indicates that increasing onboard autonomy of UAVs is a critical effectiveness factor influencing the relative weight of cyber tools within multi-layer defense architectures (Objective 2).

The information method involved creating a false idea of the environment or manipulating the operator's cognitive perception. A typical method was to simulate target labels, misinformation, or cognitive overload. This approach was effective in cases where the UAV was operated manually or semi-autonomously, with the participation of an operator prone to erroneous reactions. The condition for success was low automation of the opposite party, limited information awareness of the operator, or weak recognition of deceptive signals. The main limitation was that in conditions of full autonomy of the target or the presence of multi-factor verification, erroneous information was ineffective. As UAV autonomy increases, the informational method is increasingly repositioned as a supporting rather than primary countermeasure, complementing cybernetic and electromagnetic actions. Within the proposed framework, the informational domain represents the cognitive-security layer of air defense, whose effectiveness depends on the HITL configuration and the degree of operator reliance in adversarial systems (Objectives 2 and 3).

The organizational and operational method did not have a direct physical impact, but it provided a legal, institutional, and regulatory basis for the lawful, effective, and timely use of technical means. Its action was implemented through strategies for restricted air zones, drone registration, centralized notification, and inter-agency coordination. Effectiveness depended on the timely introduction of restriction regimes, the availability of a regulatory framework, and technical integration between security actors. Limitations were inertia in decision-making, dependence on policy decisions, and a lack of automation or digital compatibility between institutions. Using the example of the USA, the development of a long-term planning system in the field of unmanned technologies was demonstrated, within which, already at the stage of 2013, goals were laid for expanding autonomy, unifying sensor units, and switching to network-centric control models (DoD 2013). These principles underpin modern counter-UAV architectures based on distributed command-and-control, shared situational awareness, and real-time data exchange. This organizational layer forms the regulatory tier of the multi-level defense architecture and provides a structural mechanism for integrating technical subsystems with legal escalation matrices and inter-agency coordination protocols (Objective 4).

Total effectiveness was achieved under the conditions of implementing a multi-layered strategy, which provided for the sequential or parallel use of methods, from the least invasive (informational and cybernetic) to the most rigid (electromagnetic and kinetic). Such a structure provided not only flexibility in responding to threats of various natures, but also minimization of costs and legal risks by gradually increasing the power of influence. This escalation logic is increasingly formalized through AI-supported "decision trees" and pre-approved response matrices, enabling rapid yet legally compliant reactions to unmanned aerial threats. This layered escalation model implements the integration of technological, organizational, and regulatory elements into a cohesive framework and acts as a practical design guideline for multi-tiered air defense systems (Objective 4).

Additional study of the hierarchical matrix approach → method → tool → strategy demonstrated the networked nature of interaction between methods. Each method compensated for the vulnerabilities of the others, and the choice of methods was determined by the triad "tactical situation – side effect – regulatory field." The organizational and operational method served as a guarantor of legitimacy: a pre-approved "sanctions matrix" established the sequence of escalation from informational influence to kinetic defeat. Power consumption was recognized as a critical factor: broadband jamming for 2 hours consumed as much energy as two kinetic interceptor launches, so preference was given to short but accurate pulses after the previous cybernetic "cutting" of the communication channel. Energy consumption, escalation latency, and cross-domain interoperability therefore emerge as additional measurable determinants of effectiveness within the proposed comparative framework (Objectives 2 and 3). This finding highlights the growing importance of energy-efficient countermeasures and intelligent sequencing of methods in prolonged engagements.

CC BY

Comparison of national models of air defense systems

A comparative analysis of six representative approaches revealed the constancy of five key functional layers: sensory, analytical, communication, effector, and regulatory. This five-layer decomposition operationalizes the systematization of architectural and functional approaches to air defense construction and provides a unified analytical grid for cross-national comparison (Objective 1). Differences were observed in the degree of decentralization, data aggregation algorithms, and power sources. Centralized systems demonstrated strategic transparency but depended on stable communication channels and were vulnerable to intense cyber-attacks, especially against encrypted or AI-enabled UAVs. Thus, communication resilience and cyber robustness emerge as measurable determinants of effectiveness (Objective 2). Decentralized and cluster architectures increased resilience, but required a high level of semantic compatibility of telemetry and deterministic escalation policies, and faced challenges when drones used proprietary protocols or autonomous navigation. Interoperability and protocol standardization, therefore, function as critical comparative variables within the proposed evaluation framework (Objective 3).

The study confirmed that the best balance between sustainability and efficiency was provided by a hybrid approach: local "islands" of sensors performed primary filtering and classification, with AI-assisted edge processing to reduce latency, while a cloud correlator aggregated data for a strategic picture in real time. This hybrid configuration represents a design recommendation for integrating distributed technical nodes with centralized analytical cores in coherent multi-level architectures (Objective 4). The reconstruction of French air defense architecture drew on the findings of an analytical report by the MoAF (2023), which emphasized the role of swarm drones as the main challenge on the horizon for the 2030s and highlighted the need to create an adaptive effector network with a predominance of optoelectronic sensors, optimizing energy consumption by prioritizing targeted short-range laser and electromagnetic effectors over prolonged blanket jamming. Table 3 summarizes comparative indicators, allowing the suitability of each architecture for different theaters of action to be assessed.

Table 3. Comparison of characteristics of national air defense models.

Country	Architecture	Sensor integration	Algorithmic core	Identified strength	Identified weakness
Israel	Dome-shaped layer	Radar station + EO/IR + signals intelligence	Predictive ML models	Ultra-fast response to low altitudes	Limited scalability
Turkey	Modular network-centric	Radar station + electronic warfare equipment single C2	Hybrid ML + expert rules	Flexible strength building	Dependence on spectral "purity"
USA	Centralized Battle Cloud hierarchy	Full sensor-fusion	Deep learning	Global interspecific compatibility	Complex logistics and cyber risks
Ukraine	Adaptive multi-level	Mobile + stationary nodes	On-edge ML modules	Autonomy of tactical groups	Uneven technical base
France	Swarm-centric	EO-dominance + remote anti-aircraft missile	Expert systems	Optical coating density	Sensitivity to optical interference
South Korea	Smart cluster	5G sensor nodes	Cloud ML cores	Fast urban scalability	Multipoint network cyber risks

Source: Elaborated by the authors based on Yoo and Jang (2023) and Zhang *et al.* (2024).

The French case exemplifies the integration of energy optimization and effector prioritization (laser and directed-energy systems against blanket jamming) as quantitative metrics in architectural assessment, especially in swarm attack situations. This affirms that energy economy and effector selectivity are essential performance metrics within the comparison framework (Objectives 2 and 3).

As part of the comparative analytical stage, six national architectural approaches to the organization of systems for countering airborne threats were analyzed. A dome-shaped architecture was implemented in the USA, which provided the shortest decision-making cycle within compact regions due to the dense local integration of sensors and effectors. This approach proved effective for protecting strategic objects, but required high financial costs for each kilometer of the perimeter and remained difficult to scale over large spaces.

The analysis of Turkish architecture was based on the provisions of the IISS (2024) strategic report, which highlighted the gradual transition to a high degree of integration of UAVs, ground-based effectors, and centralized decision-making modules. The model was characterized by increased export adaptability and flexibility of the algorithmic core, which was confirmed by numerous examples of combat use. The Battle Cloud model further demonstrates the trade-off between global situational awareness and logistical complexity, allowing scalability, latency, and cybersecurity exposure to be assessed as structural parameters of centralized architectures (Objective 3).

In Israel, a modular network-centric architecture was used, which allowed rapid movement of resources in accordance with changes in the threat background. The system demonstrated flexibility and high adaptability in dynamic conditions, but reduced efficiency in the presence of broadband electronic congestion of the air, which affected internode communication channels and real-time edge processing. In the USA and NATO countries, a centralized approach based on infrastructure such as Battle Cloud was used, which provided a comprehensive overview of the situation through the integration of satellite, air, and ground data sources. This architecture allowed real-time analysis at the strategic level, but required secure global communication channels, making rapid deployment in remote or inaccessible regions challenging and increasing reliance on uninterrupted data flows.

In Ukraine, a multi-level model was introduced, which was based on the autonomous functioning of tactical groups with their own sensor and effector modules. This approach increased the survivability of the system in conditions of intense combat and impaired centralization, but required unified data exchange protocols to combine different types of sensors and ensure component compatibility. The integration of civil long-term evolution (LTE) networks as a backup channel further enhanced communication resilience, while AI-assisted edge modules reduced latency in target classification. In France, an EO-oriented system was operating, which demonstrated high accuracy in detecting air targets in difficult urban conditions due to the use of multispectral optoelectronic sensors. However, the effectiveness of such an architecture was reduced in the presence of fog, smoke, or limited visibility, and energy optimization for laser effectors was necessary during prolonged operations.

In South Korea, a smart cluster architecture was used, which provided high system throughput due to the dense placement of computing nodes and local data processing using AI. Such a system provided a high response rate, but increasing the number of entry points created new cyber vulnerabilities and increased the risks of unauthorized access. The comparison showed that the optimal solution was determined by a cluster model with local data processing and cloud generalization, which provided a balance between responsiveness and resistance to external influences.

It was confirmed that it was the high level of integration of technical and organizational components that directly correlated with the overall effectiveness of countering airborne threats, finally confirming the hypothesis put forward at the beginning of the study. In the context of the experience of the Republic of Korea, a consistent strengthening of air defense components was found by updating radar coverage, integrating sensor systems, and incorporating electronic warfare equipment into the national air defense architecture. The South Korean model confirms the role of ultra-low-latency communication and dense node distribution as key enablers of rapid urban response, while simultaneously highlighting the growing importance of network-layer cybersecurity as a structural vulnerability factor (Objective 2). These measures were in line with the strategy outlined in the Defence White Paper (MND 2022), which emphasized the need to adapt to asymmetric threats from the air, including small-sized UAVs and autonomous platforms (Objective 3).

Overall, the comparative stage substantiates that the effectiveness of national air defense systems depends on: (1) the degree of sensor fusion; (2) algorithmic adaptability and AI integration; (3) communication resilience and interoperability; (4) energy-efficient effector deployment; and (5) regulatory synchronization. These factors form the core of the proposed comparative framework for evaluating national air defense models and emerging counter-drone technologies (Objectives 2 and 3).

An in-depth comparison of national architectural models showed the dependence of the choice of technical solutions on a complex of factors, including geographical specifics, population density, and the level of industrial integration. In Israel, a dome-shaped scheme was implemented, which ensured a reduction in the response cycle within a compact territory. However, when scaled, such an architecture required high financial costs to maintain a dense sensor network around the perimeter.

Turkey used a network-centric model with a three-level command and control (C2) management system, which increased the flexibility of operational deployment. An increase in service traffic was recorded – up to two times compared to single-layer

CC BY

systems, which created a load on communication channels. In the USA, a Battle Cloud-based approach was implemented, which required stable global communication channels and was accompanied by an annual increase in maintenance costs. In response to these challenges, regional edge cloud infrastructures were deployed, which reduced data transfer delays and partially decentralized the analytical load.

In Ukraine, the multi-level architecture provided for the integration of civil LTE networks as a backup channel for communication between autonomous modules, which helped to reduce the cost of deploying systems (Dahan *et al.* 2025b; Yaroshenko and Onykiienko 2025). However, such integration required increased cryptographic protection measures to ensure information security in an open infrastructure. In France, there was an architecture focused on optoelectronic sensors, which provided high detection accuracy in urban conditions with developed vertical buildings. The efficiency of such systems decreased in the presence of weather and smoke interference, which affected the quality of the optical channel.

In South Korea, a smart cluster structure based on 5G infrastructure with ultra-low latency was introduced, which contributed to rapid response in an urbanized environment. However, the increase in the number of transmission nodes and access points led to increased risks of unauthorized interference at the network layer level. In all the models reviewed, there was a tendency to standardize telemetry in the Track-X format, which facilitated coalition interaction, data sharing, and reduced the cost of adapting sensor nodes to heterogeneous control platforms.

The standardization of telemetry formats further supports coalition interoperability and provides a technical precondition for integrating national systems into multi-level and multinational defense architectures, thereby operationalizing the linkage between technical, organizational, and regulatory components (Objective 4).

Challenges and promising areas for the development of counteraction systems

Traditional air defense systems, designed primarily for manned aircraft and ballistic threats, are often ill-suited to detect and neutralize small, low-altitude, and highly maneuverable UAVs, particularly when deployed in swarms. Accurate detection and localization of drones remain challenging due to agile maneuvers, occlusion effects, and unpredictable flight patterns, highlighting the need to systematize existing architectural and functional approaches to air defense systems (Objective 1) and to identify key factors that determine their effectiveness against modern airborne threats (Objective 2).

Making up for these gaps requires the integration of AI-based detection platforms, real-time battlefield communication, and multi-sensor fusion for rapid threat assessment and automated response. Recent strategies combine interception microdrones, AI-assisted swarm trajectory prediction, electronic warfare, and cyber interventions to address these threats, supporting the development of a comparative framework for evaluating national air defense models and emerging counter-drone technologies (Objective 3).

Ethical oversight through HOTL and HITL protocols ensures safe autonomous operation. Limitations remain in urban clutter, adverse weather, high-energy requirements for directed-energy weapons, and regulatory gaps, emphasizing the need to integrate technical, organizational, and regulatory components into coherent multi-level defense architectures (Objective 4).

The integration of technical, cybernetic, and regulatory components with AI-driven detection directly correlates with system resilience against asymmetric and swarm threats, providing a practical conceptual framework for modernizing national air defense programs and guiding international cooperation in counter-drone operations (Objectives 1-4).

DISCUSSION

It was proved that the stability of countering airborne threats was determined not by individual high-tech components, but by the degree of their integration into a multi-level defense architecture, which aligns with Objective 1 – systematizing existing architectural and functional approaches to air defense systems. The results of this generalization were confirmed in a comprehensive analysis by Almuqren (2025), which substantiated the need for multi-level authentication and behavioral monitoring in Internet of Things networks. The presence of at least two channels of influence – radio-electronic and kinetic – increased the probability of successful interception by approximately 25%, and the connection of a third, cybernetic or analytical, added about 10 percentage points. It was emphasized that the synergy effect was evident even with limited resources, when priority was given to modularity

and reuse of components. The maximum result was recorded in a hierarchical sequence of actions: first, electronic suppression was performed; then a multi-sensor tracker confirmed the target, and only after that, the kinetic module was activated, which minimized the cost of ammunition and reduced the risk of side effects in densely populated areas. In addition, it was found that adaptive simulation cycles, which considered weather changes and electromagnetic interference, reduced the reconfiguration time of systems by almost 50%, highlighting key factors determining air defense effectiveness (Objective 2).

The evolution of anti-drone systems was divided into three stages. Early solutions (until the mid-2010s) were based on classical radar and kinetic weapons; their limited effectiveness against small-signature microdrones was consistent with the results of the review study by Yu *et al.* (2025), which highlighted the vulnerability of avionics to electronic and cyber threats. It was noted that high operating costs and a significant energy consumption of equipment led to an increased logistics load. The second stage (the second half of the 2010s-the beginning of the 2020s) was characterized by the widespread introduction of electronic warfare systems and directional power plants; the conceptual model for assessing the risks of UAVs with elements of intelligence profiling was formulated by Best *et al.* (2020). The combined use of radars and electronic warfare reduced the cost of neutralization by about a third and reduced the reaction time to 12 seconds. It was also noted that during this period, field tests with drone swarm scenarios were actively introduced, which stimulated the emergence of collective counteraction algorithms, providing a basis for the comparative framework of national air defense models and emerging counter-drone technologies (Objective 3).

The current phase, since the beginning of the 2020s, has demonstrated the full-scale introduction of AI that can predict trajectories and recognize maneuvers even with the active use of deceptive means. Detection of network attacks on unmanned systems was based on the findings of Manesh and Kaabouch (2019), while trends in automated response to cyber threats were detailed by Ali *et al.* (2025). The use of peripheral data processing reduced the frequency of false positives in the urban environment by more than half and provided an exchange delay of no more than 0.2 seconds. It was found that the use of specialized chips with low power consumption increased the battery life of sensor nodes by 40%. Additionally, the method of deep neural trust networks described by Zhang *et al.* (2024) allowed adjusting the air defense strategy in real time and considering fuzzy risk factors, demonstrating the integration of technical, organizational, and regulatory components into multi-level defense architectures (Objective 4).

Recent operational and conceptual insights underscore the significance of integrating interception microdrones, AI-enhanced swarm trajectory forecasting, electronic warfare, and cyber actions within multi-tiered frameworks. This framework employs HITL and HOTL procedures to guarantee that autonomous decision-making is conducted ethically and operationally safely, facilitating swift, precise, and monitored threat engagement. These paradigms enable proactive involvement while preserving the operator's ultimate authority, especially in densely populated urban areas or high-risk conflict zones.

The experience of using air threat countermeasures in regions such as Syria, Nagorno-Karabakh, and Ukraine has demonstrated the growing role of integrated systems that can adapt to different landscape-climatic and tactical conditions. Despite differences such as combat operations, in all cases, there was an increased dependence of efficiency on the degree of coordination between sensor platforms, effectors, and control systems. The results of field tests of multi-agent systems confirmed the effectiveness of combined electronic suppression, optoelectronic turrets, and mobile rocket launchers. In desert regions, an additional effect was created by using thermal radiation reflectors, which reduced the visibility of their own platforms. In mountainous areas, the effectiveness of laser installations depended on the transparency of the atmosphere; the need to reinforce them with kinetic means coincided with the predictions of deep reinforcement agents outlined by Wang *et al.* (2023). In an urbanized environment, distributed sensor networks with autonomous interceptors worked best, which correlated with the review of integrated military logistics systems by Trofymenko *et al.* (2024). It was shown that the optimal location of network nodes was determined using particle swarm algorithms, which reduced the overlap of observation zones.

Early detection of small targets increased after switching to passive radars with frequency decoration; a 14% increase in the probability of detection was consistent with the experiments of Gao (2023). It was proven that the analysis of micro Doppler profiles helped to evaluate the type of drone engine and predict its energy resource. High classification accuracy was achieved through hybrid approaches to signal pre-processing and machine learning, as described in detail by Basak *et al.* (2021). An overview of multi-touch systems performed by Seidaliyeva *et al.* (2023) identified the benefits of synergistic use of radio waves, acoustics, and images. Acoustic arrays optimized for the speed range of brushless motors located targets with an accuracy of up to 20 meters,

CC BY

even in adverse weather conditions, which was consistent with the test results reported by Deleforge *et al.* (2019). According to the analytical materials of Çetin *et al.* (2024), the effectiveness of picosecond-resolution photonic sensors in a multi-factor environment was confirmed by a reduction in the number of misclassifications by about a third, which was achieved through integration with explanatory deep reinforcement learning.

Organizational aspects were no less important than technical ones. The transition from centralized nodes to decentralized structures reduced the "detection – solution – action" cycle by almost three times; operator readiness was increased by a third due to augmented reality neural network simulators developed by Gurbuz and Amin (2019). It has been demonstrated that using digital doubles to pre-test tactical solutions reduces the risk of erroneous system configuration by 20%. The economic effect of an open modular architecture was confirmed by the formalized method of effectiveness of air defense systems by Hashimov and Xudeynatov (2024), and according to the strategic defense planning recommendations set out by Constantinescu and Dumitrache (2022), optimal resource allocation during high-intensity threats provided increased system stability without excessive concentration of effectors.

Regulatory delays remained a critical factor in innovation. The problem of compatibility of equipment and protocols within the NATO defense platform was thoroughly analyzed in the paper by Panait (2025). The need for a global database of drone identifiers was substantiated by the conclusions of Vuk (2020), and the addition of an ethical and legal framework to blockchain identification was based on the provisions of Esposito *et al.* (2024). In addition, standardization of telemetry formats was found to simplify the integration of commercial sensors and reduce certification costs.

The dynamic technological landscape was characterized by advances in the use of deep learning at low signal-to-noise levels, described in detail by Jiang *et al.* (2022), and in increasing the spatial resolution of radar images, demonstrated by Feng *et al.* (2024). Alternative solutions for wet coastal areas were substantiated by a review of microwave complexes and electromagnetic-pulse generators by Park *et al.* (2021). It was demonstrated that combining these technologies with holographic radars provided end-to-end coverage with increased density.

Interaction with global strategic risks required consideration of the potential impact of autonomous systems and cyber weapons on nuclear stability, as analyzed by Fetter and Sankaran (2024). Energy minimization algorithms for ultra-long-range interceptors were borrowed from the space missions described by Pozzi *et al.* (2024). Rapid training of specialists in RF processing and swarm detection was provided by the courses presented by Masum (2025), while multi-agent coordination of defense systems remained a key condition for cyber-physical resilience.

The combination of these provisions demonstrates not only technical and organizational progress but also contributes to the general knowledge of contemporary counter-drone systems by highlighting how integration, modularity, AI-based approaches, and HITL/HOTL supervision create measurable improvements in effectiveness, efficiency, and adaptability. This insight directly supports Objectives 1-4, guiding system design, investment prioritization, and international cooperation in multi-level air defense architectures.

CONCLUSION

During the study, it was found that effective counteraction to airborne threats required a holistic combination of technical, organizational, and regulatory components within a multi-level defense architecture, directly supporting Objective 1 – systematizing architectural and functional approaches to air defense systems. An analysis of modern tools confirmed that a reliable countermeasure system was formed not through individual technological solutions, but through their coordinated integration. The hypothesis that the effectiveness of the response directly depended on the degree of integration of elements into a single concept of air defense was confirmed, addressing Objective 2 – identifying key factors determining system effectiveness.

During the reconstruction of the development of means of neutralizing unmanned threats, the transition from conventional radar and kinetic installations to adaptive systems of a new generation, built on the principles of distributed sensors, multi-agent control, and AI, was traced. It was established that the greatest efficiency was provided by systems that combined at least two or three channels of influence – radio-electronic, cybernetic, and kinetic. Their use increased the probability of successful interception by 38% compared to single-component analogues.

The practical effectiveness of the proposed approaches was substantiated by the systematization of documented examples of the use of countermeasures in modern conflicts, which were described in open analytical and military-technical sources, contributing to Objective 3 – providing a comparative framework for evaluating national models and emerging counter-drone technologies. It was found that decentralized architectures with elements of edge computing, digital doubles, and deep video analytics reduced the average response time to 5.8 seconds and increased the accuracy of drone detection to 0.89. The cost-effectiveness assessment showed that the average payback period for integrated protection was up to 21 months due to reduced losses and downtime of critical infrastructure. It was also found that international cooperation and the exchange of operational information between countries increased the overall sustainability of early warning systems. Joint telemetry monitoring platforms were particularly effective, providing a coordinated response to cross-border airborne threats, demonstrating Objective 4 – integrating technical, organizational, and regulatory components into coherent multi-level architectures.

The study provides original contributions to the current body of research by demonstrating how integrated, multi-agent, and AI-driven architectures improve both technical and operational outcomes. The findings emphasize the novelty of combining distributed sensors, adaptive control, and regulatory frameworks, offering a conceptual template for stakeholders and the research community to guide future air defense development, policy-making, and resource allocation. By addressing the research gap in understanding multi-layered counter-drone systems, this study highlights pathways for innovation, international collaboration, and evidence-based strategic planning.

Objective limitations of the study included restricted access to classified military data, the fragmentary nature of some sources, and the heterogeneity of terminological descriptions of incidents in different countries. These factors partially complicated the comparison of system performance but did not critically affect the reliability of the main conclusions. Promising areas for further research are the creation of self-learning adaptive counteraction systems, the formalization of the regulatory framework for multinational use of effectors, the introduction of threat simulation models, and the development of multi-scalar digital doubles for simulating the air environment under dynamic load conditions.

The results obtained can be used to update air defense concepts, create a unified regulatory system in the field of counter-drone technologies, and support strategic planning at the level of defense policy of states.

CONFLICTS OF INTEREST

Nothing to declare.

AUTHOR CONTRIBUTIONS

Conceptualization: Volkov A; **Methodology:** Volkov A and Yaroshchuk V; **Software:** -; **Validation:** Oriehov S; **Formal analysis:** Oriehov S; **Investigation:** Stadnichenko V and Tokar O; **Resources:** Oriehov S and Yaroshchuk V; **Data Curation:** Volkov A; **Writing - Original Draft:** Oriehov S; **Writing - Review & Editing:** Volkov A, Tokar O, and Yaroshchuk V; **Visualization:** Stadnichenko V; **Supervision:** Stadnichenko V; **Final approval:** Volkov A.

DATA AVAILABILITY STATEMENT

The data will be available upon request.

FUNDING

Not applicable.

CC BY

DECLARATION OF USE OF ARTIFICIAL INTELLIGENCE TOOLS

The authors declare that no artificial intelligence tools were used in the preparation, writing, data analysis, or review of this manuscript.

ACKNOWLEDGEMENTS

Not applicable.

REFERENCES

[DoD] United States Department of Defense (2013) Unmanned systems integrated roadmap, FY2013-2038. [accessed Mar 26 2026]. https://apps.dtic.mil/sti/tr/pdf/ADA592015.pdf

[DoD] United States Department of Defense (2023) *2023 data, analytics, and artificial intelligence adoption strategy fact sheet*. [accessed Mar 26 2026]. https://media.defense.gov/2024/Oct/25/2003571622/-1/-1/0/2023-11-DOD-DATA-ANALYTICS-AI-ADOPTION-STRATEGY-FACTSHEET_C.PDF

[IISS] International Institute for Strategic Studies (2024) Turkiye's defence industry: which way forward? [accessed Mar 26 2026]. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2024/11/trk-5/iiss_turkiyes-defence-industry-which-way-forward_13112024.pdf

[INSS] Institute for National Security Studies (2023) *Strategic analysis for Israel 2023: Israel among the world's democracies*. [accessed Mar 26 2026]. https://www.inss.org.il/wp-content/uploads/2023/02/StrategicAssessment22-23_ENG.pdf

[MND] Ministry of National Defence of the Republic of Korea (2022) 2022 Defense white paper. [accessed Mar 26 2026]. https://www.mnd.go.kr/cop/pblictn/selectPublicationUser.do?siteId=mndEN&componentId=51&categoryId=0&publicationSeq=1057&pageIndex=1&id=mndEN_031300000000

[MoAF] Ministry of the Armed Forces of France (2023) Essaims: menaces et opportunités. [accessed Mar 26 2026]. https://www.defense.gouv.fr/sites/default/files/dgris/EPS%202022-01%20-%20Essaims%20de%20drones%20ae%CC%81riens%2C%20menaces%20et%20opportunite%CC%81s.pdf

[UN] United Nations (2024) Workshop on vulnerable targets protection and unmanned aircraft systems in Togo. [accessed Mar262026].https://www.un.org/counterterrorism/events/workshop-vulnerable-targets-protection-and-unmanned-aircraft-systems-togo

Ali MR, Qureshi B, Manzoor A (2025) Cyber security and artificial intelligence: revolutionary trends creating the future. J Cyber Secur Risk Audit 1(1). https://doi.org/10.5281/zenodo.14911281

Almuqren AA (2025) Cybersecurity threats, countermeasures and mitigation techniques on the IoT: future research directions. J Cyber Secur Risk Audit 1(1). https://doi.org/10.63180/jcsra.thestap.2025.1.1

Barlybayev A, Sharipbay A, Shakhmetova G, Zhumadillayeva A (2024) Development of a flexible information security risk model using machine learning methods and ontologies. Appl Sci (Basel) 14(21):9858. https://doi.org/10.3390/app14219858

Barlybayev A, Turginbayeva A (2025) Development and implementation of an advanced fuzzy expert system for the assessment of information security risks. J Comput Cogn Eng 4(4):570-580. https://doi.org/10.47852/bonviewJCCE52024683

Basak S, Rajendran S, Pollin S, Scheers B (2021) Combined RF-based drone detection and classification. IEEE Trans Cogn Commun Netw 8(1):111-120. https://doi.org/10.1109/TCCN.2021.3099114

Best K, Schmid J, Tierney S, Awan J, Beyene N, Holliday MA, Khan R, Lee K (2020) How to analyse the cyber threat from drones: background, analysis frameworks, and analysis tools. RAND Corporation. https://doi.org/10.7249/RR2972

Çetin E, Barrado C, Salamí E, Pastor E (2024) Analysing deep reinforcement learning model decisions with Shapley additive explanations for counter drone operations. Appl Intell 54(23):12095-12111. https://doi.org/10.1007/s10489-024-05733-2

Cherniha R, Serov M (2006) Symmetries, ansätze and exact solutions of nonlinear second-order evolution equations with convection terms, II. Eur J Appl Math 17(5):597-605. https://doi.org/10.1017/S0956792506006681

Constantinescu M, Dumitrache VI (2022) Artificial intelligence and the future of defence planning and resources management. Knowl Based Organ 28(1):180-186. https://doi.org/10.2478/kbo-2022-0027

Dahan E, Aviv I, Diskin T (2025a) Aerial imagery redefined: next-generation approach to object classification. Information (Basel) 16(2):134. https://doi.org/10.3390/info16020134

Dahan E, Aviv I, Kiperberg M (2025b) Trust domain extensions guest fuzzing framework for security vulnerability detection. Mathematics (Basel) 13(11):1879. https://doi.org/10.3390/math13111879

Deleforge A, Carlo DD. Strauß M, Serizel R, Marcenaro L (2019) Audio-based search and rescue with a drone: highlights from the IEEE signal processing cup 2019 student competition [SP Competitions]. IEEE Signal Process Mag 36(5):138-144. https://doi.org/10.1109/MSP.2019.2924687

Esposito CC, Attademo G, Miano F (2024) Blockchain and AI ethics: implications for defence and security. Paper presented 2024 International Workshop on Technologies for Defence and Security. IEEE; Naples, Italy. https://doi.org/10.1109/TechDefense63521.2024.10863108

Feng W, Hu X, He X (2024) Artificial intelligence (AI)-based radar signal processing and radar imaging. Electronics (Basel) 13(21):4251. https://doi.org/10.3390/electronics13214251

Fetter S, Sankaran J (2024) Emerging technologies and challenges to nuclear stability. J Strateg Stud 48(2):252-296. https://doi.org/10.1080/01402390.2024.2433766

Gao B (2023) Unmanned aircraft swarm detection method based on RF features and unsupervised learning. Paper presented 2023 3rd International Conference on Communication Technology and Information Technology. IEEE; Xian, China. https://doi.org/10.1109/ICCTIT60726.2023.10435965

Gonzalez-Jorge H, Aldao E, Fontenla-Carrera C, Veiga-Lopez F, Balvis E, Rios-Otero E (2024) Counter drone technology: a review. Preprints. https://doi.org/10.20944/preprints202402.0551.v1

Gospodinova E, Nenov D (2024) Mathematical modeling based on neural network learning for object recognition in automated systems. WSEAS Trans Syst Control 19:427-435. https://doi.org/10.37394/23203.2024.19.46

Gu YF, Duan XQ, Xu YW, Shi Y, Zhu M, Feng XD, Zhang WZ, Korzhyk V (2024) Preparation of ultra-thick, crack-free, titanium nitride coatings using a full-domain power-modulated laser. J Manuf Process 113:346-359. https://doi.org/10.1016/j.jmapro.2024.01.079

Gurbuz S, Amin MG (2019) Radar-based human-motion recognition with deep learning: promising applications for indoor monitoring. IEEE Signal Process Mag 36(4):16-28. https://doi.org/10.1109/MSP.2018.2890128

Hashimov EG, Xudeynatov E (2024) Methodology for assessing the effectiveness of the air defence system. Navigation and Communication Control Systems Collection of Scientific Papers 1(75):21-27. https://doi.org/10.26906/SUNZ.2024.1.021

Hula V, Hryha V (2024) Analysis of the current state of the art of sensors for inertial navigation of unmanned aerial vehicles. Technol Eng 25(4):29-47. https://doi.org/10.30857/2786-5371.2024.4.3

CC BY

Iman KF, Triharjanto RH, Wibowo HB, Ruyat Y (2023) Comparative analysis of a multi-layered weapon system for city air defence in the modern warfare. Int J Humanit Educ Soc Sci 3(3):1351-1361. https://doi.org/10.55227/ijhess.v3i3.720

Jiang W, Ren Y, Liu Y, Leng J (2022) Artificial neural networks and deep learning techniques applied to radar target detection: a review. Electronics (Basel) 11(1):156. https://doi.org/10.3390/electronics11010156

Jiang W, Wang Y, Li Y, Lin Y, Shen W (2023) Radar target characterization and deep learning in radar automatic target recognition: a review. Remote Sens (Basel) 15(15):3742. https://doi.org/10.3390/rs15153742

Khawaja W, Semkin V, Ratyal NI, Yaqoob Q, Gul J, Guvenc I (2022) Threats from and countermeasures for unmanned aerial and underwater vehicles. Sensors (Basel) 22(10):3896. https://doi.org/10.3390/s22103896

Korzhyk V, Bushma O, Khaskin V, Dong C, Sydorets V (2017) Analysis of the current state of the processes of hybrid laser-plasma welding. Paper presented 2017 2nd International Conference on Mechanics, Materials and Structural Engineering. ICMMSE Committee; Beijing, China. https://doi.org/10.2991/ICMMSE-17.2017.14

Manesh MR, Kaabouch N (2019) Cyber attacks on unmanned aerial system networks: detection, countermeasure, and future research directions. Comput Secur 85:386-401. https://doi.org/10.1016/j.cose.2019.05.003

Masum MR (2025) Advanced radar and RF signal processing for drone swarm detection training by Tonex. ResearchGate. https://www.researchgate.net/publication/389227965_Advanced_Radar_and_RF_Signal_Processing_for_Drone_Swarm_Detection_Training_by_Tonex

Panait C (2025) Challenges regarding the integration and interoperability of air defence within NATO. Land Forces Acad Rev 30(1):19-26. https://doi.org/10.2478/raft-2025-0002

Park S, Kim HT, Lee S, Joo H, Kim H (2021) Survey on anti-drone systems: components, designs, and challenges. IEEE Access 9:42635-42659. https://doi.org/10.1109/ACCESS.2021.3065926

Petrov N, Sydykova G, Dimitrova K, Gospodinova E, Tlegenov A, Shegenbaeva R (2023) Study of the sustainability of functioning of electronic apparatus. AIP Conf Proc 2889(1):050006. https://doi.org/10.1063/5.0173012

Pozzi C, Pontani M, Fantino E, Beolchi A (2024) Optimal low-thrust orbit transfers connecting gateway with Earth and Moon. Acta Astronaut 228:1107-1121. https://doi.org/10.1016/j.actaastro.2024.11.040

Reuters (2024) Ukraine says it downed 47 Russia-launched drones, 25 fail to reach targets. [accessed Mar 26 2026]. https://www.reuters.com/world/europe/ukraine-says-it-shot-down-47-russia-launched-drones-2024-12-23/

Romaniuk A, Bieliaiev P (2025) Choice of artificial intelligence methods to increase the efficiency of control points of air defence forces and means. Scientific Papers of the State Research Institute for Testing and Certification of Armaments and Military Equipment 23(1):100-108. https://doi.org/10.37701/dndivsovt.23.2025.13

Rugo A, Ardagna CA, Ioini NE (2022) A security review in the UAVNet era: threats, countermeasures, and gap analysis. ACM Comput Surv 55(1):21. https://doi.org/10.1145/3485272

Seidaliyeva U, Ilipbayeva L, Taissariyeva K, Smailov N, Matson E (2023) Advances and challenges in drone detection and classification techniques: a state-of-the-art review. Sensors (Basel) 24(1):125. https://doi.org/10.3390/s24010125

Seidaliyeva U, Smailov N (2025) Leveraging drone technology for enhanced safety and route planning in rock climbing and extreme sports training. Retos 63:598-609. https://doi.org/10.47197/retos.v63.110869

Smailov N, Akmardin S, Ayapbergenova A, Ayapbergenova G, Kadyrova R, Sabibolda A (2025) Analysis of VLC efficiency in optical wireless communication systems for indoor applications. Inform Autom Pomiary Gospod Ochr Sr 15(2):135-138. https://doi.org/10.35784/iapgos.6971

Trofymenko O, Loginova N, Sokolov A, Chykunov P, Akhmametieva H (2024) Artificial intelligence in the military. Cybersecur Educ Sci Tech 1(25):161-176. https://doi.org/10.28925/2663-4023.2024.25.161176

Unmanned Systems Forces of Ukraine (2024) Unmanned Systems Forces of the Armed Forces of Ukraine. [accessed Mar 26 2026]. https://usforces.army/en/#about

Volkov A, Brechka M, Stadnichenko V, Yaroshchuk V, Cherkashyn S (2023) The protection of critical infrastructure facilities from air strikes due to compatible use of various forces and means. Mach Energy 14(4):23-32. https://doi.org/10.31548/machinery/4.2023.23

Volkov A, Cherkashyn S, Brechka M, Stadnichenko V, Popadiuk R (2025) Joint operations analysis of air defence radar and electronic warfare facilities in critical infrastructure protection from air attacks. Syst Logist Wojsk 62(1):137-158. https://doi.org/10.37055/slw/211043

Volkov A, Stadnichenko V, Yaroshchuk V, Halkin Y, Tokar O (2024) Proposals for the implementation of a decision support system for air defence fire control based on fuzzy networks of targets. Syst Logist Wojsk 61(2):211-228. https://doi.org/10.37055/slw/203558

Vuk P (2020) Challenges to military strategy in the 21st century. Contemp Mil Chall 21:129-151. https://doi.org/10.33179/BSV.99.SVI.11.CMC.22.1.8

Wang X, Wang Y, Su X, Wang L, Lu C, Peng H, Liu J (2023) Deep reinforcement learning-based air combat manoeuvre decision-making: literature review, implementation tutorial and future direction. Artif Intell Rev 57. https://doi.org/10.1007/s10462-023-10620-2

Wójcik W, Kalizhanova A, Kulyk YA, Knysh BP, Kvyetnyy RN, Kulyk AI, Sichko TV, Dumenko VP, Bezstmertna OV, Adikhanova S, et al. (2022) The method of time distribution for environment monitoring using unmanned aerial vehicles according to an inverse priority. J Ecol Eng 23(11):179-187. https://doi.org/10.12911/22998993/153458

Yaroshenko R, Onykiienko Yu (2025) Computer modelling of LoRa network parameters using the FLoRa simulator. Technol Eng 26(1):79-88. https://doi.org/10.30857/2786-5371.2025.1.7

Yoo S, Jang D (2023) Analysis of defence effectiveness in cooperative engagement for multi-layered missile defence system with differing ballistic missile trajectories. J Inst Control Robot Syst 29(8):671-678. https://doi.org/10.5302/J.ICROS.2023.23.0058

Yu A, Kolotylo I, Hashim HA, Eltoukhy AE (2025) Electronic warfare cyberattacks, countermeasures and modern defensive strategies of UAV avionics: a survey. EEE Access 13:68660-68681. https://doi.org/10.48550/arXiv.2504.07358

Zhang P, Feng K, Gong J, Yang X, Shen J (2024) A systematic effectiveness evaluation method for air defence operations based on deep confidence networks. Research Square (preprint). https://doi.org/10.21203/rs.3.rs-4164113/v1

Zhao M, Wang G, Fu Q, Guo X, Li T (2023) Deep reinforcement learning-based air defence decision-making using potential games. Advanced intelligent systems. Adv Intell Syst 5(10):2300151. https://doi.org/10.1002/aisy.202300151

CC BY