https://doi.org/10.1590/jatm.v18.1457 ORIGINAL PAPER

Review and Simulation-Based Analysis of Artificial Intelligence for Detection and Response to Air Threats

Andrii Volkov[1,*], Mykhailo Brechka[1], Mykhailo Lytvynenko[2], Vitalii Yaroshchuk[1], Serhii Korsunov[1]

1. Ivan Kozhedub Kharkiv National Air Force University – Department of Tactics of the Air Defence Forces of the Land Forces – Kharkiv – Ukraine.
2. Ivan Kozhedub Kharkiv National Air Force University – Department of Mathematical and Software ACS – Kharkiv – Ukraine.

***Corresponding author:** andriivlkv@gmail.com

ABSTRACT

The study aimed to analyze how artificial intelligence (AI) systems could be used to make air defense for critical infrastructure more effective. An analytical review method was used to systematically analyze how AI is used in air defense systems based on open sources from the United States, Israel, Ukraine, Germany, and South Korea, with an emphasis on the automation of processes for detecting, classifying, and prioritizing air threats for the period from 2020 to 2024. The study established that convolutional neural networks provide 92.8% accuracy in air target recognition, with an F1 score of 0.91. Random forest and eXtreme Gradient Boosting models achieved classification accuracies of 90.4% and 93.8%, respectively, at the final threat classification stage. The use of clustering algorithms (k-means, density-based spatial clustering of applications with noise, DBSCAN) reduced the average time to determine coordinates to 1.4 seconds and the full response cycle to 2.1 seconds. The integration of AI into the centralized control system increased the probability of successful interception of air threats by 12-15%. The study provides analytical and simulation-based support for the potential use of AI systems to improve the effectiveness of air defense for critical infrastructure and identifies promising directions for the development of adaptive and automated defense technologies.

Keywords: Artificial intelligence; Machine learning; Air defense; Target recognition; Decision support systems; Computerized simulation.

INTRODUCTION

Air defense (AD) of critical infrastructure is one of the key elements of national security, ensuring the protection of infrastructure from modern air threats. With the development of new technologies and the increasing complexity of attacks, traditional defense methods need to be improved and automated (Volkov *et al.* 2023). Artificial intelligence (AI) systems create new opportunities to improve the responsiveness, accuracy, and adaptability of AD systems, which is relevant in fast-paced combat operations and the use of unmanned aerial vehicles (UAVs) and cruise missiles. The integration of AI not only improves threat detection and classification but also optimizes the decision-making process, minimizing the human factor and reducing the risk of false positives.

The problem of improving the speed and accuracy of detecting air threats in AD systems for critical infrastructure has already attracted the attention of many researchers. Zhao *et al.* (2024), in a study conducted using hierarchical reinforcement learning to optimize the distribution of AD resources, demonstrated a reduction in the response time of systems to air threats and an increase

Received: Apr. 07, 2026 | **Accepted:** Jun. 26, 2026
Peer Review History: Single Blind Peer Review.
Section editor: Adam Cumming

in the adaptability of systems, but the country where the study was conducted was not specified. Criollo *et al.* (2024), analyzing military applications of UAVs in the United States, Israel, and Ukraine, demonstrated that the automation of target classification contributed to a reduction in false alarms in radio-electronic conditions, in particular due to machine learning algorithms. At the same time, there is no in-depth analysis of the integration of these algorithms into specific AD systems. Nantogma *et al.* (2021), in a study based on data from China, proposed a coordinated learning system based on immunized classifiers, which increases the resilience of systems to new threats through self-learning mechanisms. However, the study is limited to simulation experiments, which reduces its practical applicability.

Javaid *et al.* (2023), analyzing new trends in communication and management of collaborative UAVs using the examples of the United States and South Korea, emphasized the role of centralized coordination through AI to optimize AD resources, but did not provide a quantitative assessment of the effectiveness of implementing such systems. Samadzadegan *et al.* (2022), conducting research based on data from Iran, applied deep convolutional neural networks (CNNs) to detect and recognize drones in complex urban environments, which reduced the level of false alarms. However, the study does not consider the adaptation of models to rapidly changing environmental conditions. Steingartner *et al.* (2021), using data from several European countries, developed hybrid cyber defense methods to increase the resilience of AD systems to cyberattacks, but pointed to the need for further development of comprehensive security models in real combat conditions. Insaurralde and Blasch (2022), based on American experience, created a decision support system using ontological inference to reduce the human factor in air traffic control, which contributed to a reduction in operational errors. However, further testing in military AD systems remains open.

Santhi *et al.* (2024), considering ethical issues in India, highlighted the ethical aspects of the use of autonomous defense systems and emphasized the need to comply with international humanitarian norms in their development, without proposing specific technical solutions. Kuleshov *et al.* (2024), applying digital twin methodologies developed within U.S. defense-oriented cyber simulation frameworks, used digital twins to simulate cyberattacks on avionics, which improved the readiness of AD systems. However, the limitations lie in the complexity of modeling real combat scenarios. Song *et al.* (2023), researching a multi-sensor approach in China, used an improved search algorithm to improve the accuracy of threat assessment in AD systems.

Volkov *et al.* (2024), researching the application of fuzzy networks of targets in AD systems, proposed a decision support system that reduced response time by 15% and false alarms by 20%. Nevertheless, further adaptation of methods to changing airspace conditions is required. These studies demonstrated that machine learning reduces response times, automated classification reduces false positives, adaptive models increase system resilience to new threats, and coordination of AD assets increases overall defense effectiveness. Considering the research conducted, there are still gaps in the development of integrated systems that would combine high-precision recognition, protection against cyberattacks, and consideration of the ethical aspects of autonomous decisions. These issues require further in-depth study to create reliable, adaptive, and secure AD systems.

The study aimed to investigate how AI systems may improve the effectiveness of AD for critical infrastructure under review-based and simulated operational conditions.

The study goals included:

- To evaluate methods for automatic recognition and classification of air threats using AI.
- To determine the effectiveness of integrating adaptive models to improve the accuracy of air threat detection.
- To analyze the possibilities of integrating various security measures through centralized management systems.

METHODOLOGY

The study conducted a comprehensive analysis of the role and functions of AI in modern AD systems to identify key areas of its application for the protection of critical infrastructure. The methodology was based on theoretical and simulation analysis, without empirical combat testing, and was structurally consistent with the defined research objectives. Within the framework of the analysis of methods for automatic recognition and classification of air targets, computer vision and machine learning methods were applied. Convolutional neural networks (CNNs) were used to detect drones, missiles, and aircraft using satellite or optical data; clustering algorithms (k-means, DBSCAN) were used to group targets by trajectory; and ensemble models (random forest,

eXtreme Gradient Boosting [XGBoost]) were used for multi-factor classification. The selected algorithms were applied because previous studies demonstrated their effectiveness in aerial object detection, anomaly detection, noisy target classification, and multi-sensor data fusion under conditions typical of AD environments, including electronic warfare (EW) interference and limited visibility. The models were trained on synthetic and open databases (Dataset for Object Detection in Aerial Images [DOTA], University of Chinese Academy of Sciences Aerial Object Detection [UCAS-AOD]), adapted to conditions with high noise levels, EW interference, and variable visibility. In particular, the DOTA dataset contained over 280,000 objects in 15 classes on high-resolution aerial photographs, and UCAS-AOD contained over 1,000 images with aircraft and drone labels from different angles, providing a variety of scenarios for training the system. To verify the reliability of the results, metrics such as classification accuracy, F1-score, input processing time, average system response time, and false alarm rate were used; a K-fold cross-validation strategy ($k = 5$) was employed to ensure a more objective assessment of model stability on different data subsets.

The effectiveness of adaptive models capable of improving threat detection accuracy based on accumulated experience was analyzed. Online model training methods based on new data about previous attacks were used, as well as digital twins to simulate threat scenarios and test system responses. The algorithms dynamically adjusted parameters based on information from radars, optical sensors, and cyber monitoring modules. Calculations were performed in MATLAB/Simulink environments using the Deep Learning Toolbox, as well as in TensorFlow, with simulations covering 18 threat scenarios with different parameters, including variable visibility conditions, noise and EW interference levels, and dynamic adjustment of algorithms based on data from radars, optical sensors, and cyber monitoring modules. Five training iterations were performed for adaptive models, which evaluated the reduction in false alarms, and digital twins were used to test the response of systems to complex combined attacks and air target behavior variants. The parameters before and after adaptation were compared in terms of target recognition accuracy, processing speed, and resistance to complex combined attacks.

Coordination between different means of protection using centralized control systems was given particular attention. The integration of AD, EW, cyber defense, and satellite aerial reconnaissance into a single architecture via a distributed data exchange network was studied. From a technical perspective, resources were analyzed, including adaptive radio jamming systems based on Software-Defined Radio (SDR), internetwork screens, cyber monitoring modules, and reconnaissance complexes with UAVs. National Instruments Laboratory Virtual Instrument Engineering Workbench software was used for AI integration in combination with TensorFlow-based machine learning modules. The systems were combined into a single information space, which was used by AI to perform synchronized analysis of data from various sources, automatically prioritize threats, transmit coordinates to EW systems to create point interference, initiate cyber defense when anomalies in network traffic were detected, and process satellite images to detect attack preparations. The reliability of centralized decisions was verified by comparing system parameters before and after adaptation, including analysis of target recognition accuracy, processing speed, and resistance to complex combined attacks, which can be used for indirect assessment of the correctness of AI responses in simulated scenarios. This interaction provided a multi-level, adaptive response to complex hybrid threats in real time.

To confirm the significance and effectiveness of AI in AD in practice, the work analyzed the experience of leading countries, including the United States, Israel, Ukraine, Germany, and South Korea, considering various sources of information. For the United States, official military programs and publications (Adewusi *et al.* 2024) were studied; for Israel, national defense reports and studies on the Iron Dome system (Slesinger 2022); for Ukraine, analytical reports and studies on the impact of drones on the conflict (Samus 2024); for Germany, defense reports and reviews of the European defense industry (Calcara *et al.* 2023); and for South Korea, case studies of military applications of AI with an emphasis on national defense systems (Lee 2021). This comprehensive study made it possible to consider the specifics of each country and the sources that shape their approaches to AI implementation in AD. These countries were selected for their advanced experience in implementing innovative AI technologies in AD systems, as well as for the diversity of geopolitical, organizational, and technical conditions, which provided a comprehensive overview of practical applications. Key programs and projects that implement AI to improve AD management systems, increase response speed, and improve target detection accuracy were described. In particular, the application of AI in the North American Aerospace Defense Command (NORAD) and Patriot control systems in the United States, intelligent functions in the Iron Dome system in Israel, autonomous sensor solutions for detecting UAVs in Ukraine, modernized InfraRed Imaging System Tail/Thrust

Vector-Controlled Surface Launched Medium Range (IRIS-T SLM) complexes with target prediction and classification elements in Germany, as well as the Korean Medium-range Surface-to-Air Missile (KM-SAM Block II or Cheongung II) and BIHO II (Flying Tiger II) systems in South Korea, which use AI for automatic tracking and interception of enemy objects.

RESULTS

The integration of AI into AD systems is one of the most promising areas of development in defense technology. Given the current challenges posed by the growing number of UAVs, missile threats, and the use of EW, the application of AI can improve the effectiveness and reliability of AD systems (Table 1).

Table 1. Key AI functions in AD systems and examples of applications.

Function	Example of use
Automated target detection	Recognition of drones, missiles, and aircraft in difficult weather conditions and under EW
Threat detection	Analysis of trajectories, speeds, thermal, and radar signatures
Target prioritization	Identification of the most threatening objects for critical infrastructure
Optimization of resource use	Determining an effective interception method based on the type of missile

Source: Elaborated by the authors based on Khan *et al.* (2021).

Automating target detection is a priority. Systems equipped with computer vision and machine learning algorithms can analyze large amounts of data from radar, thermal, and optical sensors. This enables the recognition of types of aerial objects – drones, missiles, and aircraft – even in conditions of limited visibility or during active use of EW measures. This significantly reduces the risk of missing targets or false alarms.

Threat classification is based on the analysis of flight parameters: trajectory, speed, and physical characteristics such as thermal or radar signature. Thanks to machine learning, systems can recognize even new, previously unknown types of threats or camouflage, making protection more adaptive and ready for modern challenges.

Prioritizing air targets is critical for effective fire control in conditions of limited resources and high combat dynamics. It can be used for the rapid identification of the most threatening objects and the targeting of weapons at them first. This minimizes the risk of enemy airspace breaches and increases the overall effectiveness of the AD system. Artificial intelligence (AI) assesses the potential damage from striking a particular target, considering its proximity to critical infrastructure and the possibility of successful interception. This avoids the dispersion of forces and increases the overall effectiveness of defense.

Optimization of resource utilization involves calculating the most efficient interception tactics, incorporating the types of missiles, their number, range, and the current situation on the battlefield. Artificial intelligence (AI) analyzes various scenarios and proposes the most effective solution, minimizing ammunition expenditure and reducing the likelihood of misses.

In general, the use of AI in AD systems improves accuracy, decision-making speed and system adaptability, which is crucial in a modern environment, where threats are becoming increasingly complex and dynamic. This creates new opportunities for the creation of highly effective systems for the protection of critical infrastructure and national security in general.

The classification accuracy when using CNNs for air target recognition averaged 92.8%, with an F1 score of 0.91, indicating a high balance between completeness and accuracy. Ensemble methods, in particular random forest and XGBoost, demonstrated stable performance, with random forest reaching 90.4% and XGBoost reaching 93.8% classification accuracy, with an F1 measure of 0.86-0.89. Clustering algorithms (k-means, DBSCAN) effectively grouped air targets by movement parameters, reducing the average target designation time to 1.4 seconds with an average input data volume.

The processing time for a single query in real-time systems (using TensorFlow modules) averaged 240 ms when working with mid-range graphics processors. The average system response time from target detection to transmission of coordinates to weapons was 2.1 seconds. The false alarm rate was reduced to 5.6% using ensemble models with a noise pre-filtering function. Adaptive models with self-learning elements showed an average reduction in false positives of 16.4% after five training iterations.

The study also demonstrated that the integration of a centralized Command & Control (C2)-based control system with AI functions optimized the distribution of weapons, increasing the probability of successful target interception by 12-15% compared to traditional command schemes. This confirms the effectiveness of the proposed approaches to automating threat analysis and coordinating defense systems.

Artificial intelligence (AI) is central to a variety of functions that enhance the effectiveness of AD systems. Each of these functions is designed to automate complex processes that traditionally required significant operator involvement and to provide faster and more accurate responses to air threats (Table 2).

Table 2. Specific AI functions in AD and their characteristics.

Function	Description	Influence
Detection	Automatic processing of signals from radar stations and portable MANPADS	Reduction of false alarms
Visual/thermal imaging identification	Recognition of kamikaze drones in complex backgrounds	Improved identification accuracy
Trajectory prediction	Analysis of enemy object movement	Precise armament guidance
Coordination of AD assets	Consolidating batteries into a single control system	Improved system efficiency
Autonomous strike decision	Potential autonomy to open fire in time-critical threats	Acceleration of reaction

Source: Elaborated by the authors based on Hashimov and Khudeynatov (2024).

AI-based air target detection relies on automated processing of large volumes of signals received from radars, MANPADS sensors, and other systems. Machine learning algorithms analyze these signals by comparing them with patterns or signatures of previously detected threats. This not only quickly detects new objects in the air but also quickly separates potentially dangerous targets from false positives, such as birds, civilian aircraft, or weather interference. As a result, the number of false alarms is significantly reduced, which in turn reduces the workload on operators and minimizes the risk of inappropriate use of combat resources. This approach is particularly effective in complex combat conditions, especially in areas where EW systems are active, where traditional signal analysis methods often lose accuracy due to interference and noise.

During the simulation modeling process, individual algorithms were tested to assess their effectiveness in classification, detection, and adaptation to threats. Convolutional neural networks (CNNs) were used to process video and images from thermal and optical sensors. Under standard weather conditions, CNNs demonstrated an accuracy of up to 94.3% in recognizing drones and aircraft, but in the presence of atmospheric interference (fog, rain), this accuracy decreased to 86.7%. Adapting the model through retraining on new samples made it possible to increase resistance to external factors and maintain an average accuracy rate of 91.5%.

The k-means and DBSCAN clustering algorithms were used to group aerial targets by trajectory parameters (speed, altitude, direction of movement) and detect atypical behavior. DBSCAN showed better performance in detecting anomalous groups of objects with uneven data distribution, especially in scenarios with a swarm of drones, where the accuracy of cutting off atypical objects reached 89.2% compared to 81.6% in k-means.

Ensemble methods (random forest, XGBoost) were used at the final threat classification stage, combining data from several sensor channels (radar, infrared radiation, satellite imagery). XGBoost showed higher overall classification accuracy (93.8%) compared to random forest (90.4%), especially in cases where complex cross-features were required (e.g., signatures in the infrared spectrum combined with motion characteristics).

Thus, each of the algorithms used demonstrated specific advantages in the corresponding subtasks. Their combined application in an integrated system ensured a high level of accuracy, response speed, and adaptability to complex combat conditions.

Visual and thermal imaging target identification is performed using computer vision algorithms capable of processing images in real time from optical and thermal imaging cameras. These algorithms are trained on a large number of examples and can recognize typical threats, including kamikaze drones camouflaged among urban infrastructure. Computer vision can analyze not only the shape and contour of an object but also its thermal signature (infrared radiation), which is especially useful for detecting

targets at night or in poor visibility conditions. The combination of these factors significantly increases recognition accuracy compared to traditional surveillance methods, enabling a timely response to threats, even when they have a small reflective surface or are moving at low altitude.

The trajectories of airborne objects are predicted by integrating data from multiple sources, including radar measurements, thermal sensors, and historical behavior patterns of typical targets. Artificial intelligence (AI) algorithms analyze dynamic parameters such as speed, direction of movement, angle of attack, and trajectory changes to construct the most likely path of the object's future movement. This supports AD systems in determining in advance the optimal moment and coordinates for intercepting the target. This capability is particularly relevant in cases where enemy objects perform maneuverable flights or change their trajectory in an attempt to bypass cover zones.

Coordination of AD assets using AI can form a unified defense grid, where multiple batteries, radars, and launchers operate as a single integrated mechanism. Artificial intelligence (AI) in such systems performs the function of distributing targets among different combat units, avoiding duplicate attacks on a single target, and ensuring optimal use of each available resource. For example, if a single target is within range of several launchers, AI can select the optimal platform for engagement, considering the angle of approach, target speed, and remaining ammunition. Such centralized control improves system efficiency and reduces decision-making time in critical situations.

Autonomous decision-making on opening fire, although still at the experimental stage or limited in its application, is considered one of the most promising areas of development for AD. The idea is to provide AI systems capable of independently making decisions on targeting without human intervention in situations where every second counts. This is particularly relevant when repelling attacks from kamikaze drones, high-speed missiles, or swarms of small UAVs, where human reaction times are insufficient to ensure an effective response. The safe implementation of such solutions requires a highly accurate recognition system and legally and ethically sound regulation that considers the possible consequences of autonomous weapon use.

As a result, all these functionalities implemented with the help of AI contribute to the qualitative improvement of AD systems. They increase the speed of response to threats, reduce the number of false decisions, and facilitate adaptation to new types of air attacks characteristic of the modern battlefield.

The integration of AI into various AD subsystems contributes to the creation of a comprehensive, interconnected defense complex capable of adapting to dynamic threats and providing more effective protection. Of significance is the cooperation of AI with EW assets, cybersecurity systems, and intelligence platforms (Table 3).

Table 3. Interaction of AI with other systems.

System	AI functions	Main tasks
EW	Signature analysis, dynamic change of interference parameters	Improvement of the effectiveness of EW in real time
Cybersecurity systems	Cyberattack prediction, autonomous response	Protection against cyberattacks on AD systems
Satellite and aerial reconnaissance	Processing large data sets	Detecting preparations for attacks

Source: Elaborated by the authors based on Yu (2025).

In the field of EW, AI is central to the dynamic analysis and adaptation of radio frequency spectrum parameters. Artificial intelligence (AI)-based systems can detect, identify, and classify electromagnetic signatures belonging to enemy missile guidance systems, radars, or communication channels in real time. Thanks to this, EW complexes can instantly change the frequency, intensity, and type of interference generated to most effectively block or distort the enemy's operations. This approach not only increases the probability of neutralizing enemy systems but also reduces the possibility of interference with the operation of one's own technical equipment. Automatic adaptation of defense methods in real time can maintain superiority even in difficult conditions of electromagnetic noise, which is characteristic of the modern battlefield. As a result, jamming of enemy guidance systems or control channels becomes more accurate and stable, reducing the risk of a successful attack on protected objects.

In cybersecurity systems, AI is used for comprehensive monitoring and prediction of potential cyberattacks on AD infrastructure. Artificial intelligence (AI) analyzes large amounts of network traffic, seeking unusual or abnormal behavior patterns that may

indicate an impending intrusion or malware activity. When such anomalies are detected, the system can automatically initiate protective measures, such as isolating affected network segments, blocking suspicious connections, or changing security policy configurations. Autonomous response mechanisms minimize the time between the start of an attack and the start of protection, which is critical to preventing the loss of control of AD systems or the leakage of confidential information. In addition, AI can analyze historical attack data, predicting trends and increasing the adaptability of cyber defense to new types of threats.

Interaction with satellite and aerial reconnaissance involves processing huge amounts of heterogeneous data from numerous sources: high-resolution satellite images, video and photo materials from UAVs, radar information, etc. Artificial intelligence (AI) analyzes this data to identify critical signs, such as the movement of military equipment, the formation or reformation of combat groups, preparations for offensive actions, or the camouflaging of objects. Thanks to image recognition and dynamic prediction algorithms, AI can detect even minor changes in the appearance or behavior of targets, ensuring early detection of potential threats. This, in turn, facilitates commanders in planning appropriate countermeasures and making timely strategic decisions.

Therefore, the integration of AI into the interaction of various EW, cybersecurity, satellite, and aerial reconnaissance systems creates a synergistic effect. The combination of these technologies provides a more complete and timely determination of the combat situation, increases the flexibility and resilience of AD systems, and improves the efficiency of counteraction to modern high-tech threats in real time.

The study implemented scenarios illustrating the practical interaction of AI with various components of the defense infrastructure, in particular EW, cyber monitoring, and satellite reconnaissance systems. One of the key examples involved the detection of a coordinated attack that combined the use of drones and cyber activity in the AD control system.

In this scenario, the AI system received an initial signal about suspicious activity in network traffic from the cyber monitoring module (based on an internetwork screen with deep packet inspection analysis), accompanied by a surge of requests to the command node. At the same time, the optical detection system recorded suspicious activity at an altitude of up to 150 m within a radius of 5 km. Based on combined data from the radar (X-band), infrared sensor, and cyber module, CNNs performed a correlation analysis, identifying the object as a mini-UAV synchronized with the cyberattack.

The AI automatically transmitted the object's coordinates to the EW system, which initiated the creation of a narrow-beam jammer using an SDR module configured to the UAV's control frequency. At the same time, the cyber defense system automatically isolated the compromised network segment and analyzed the behavior of the malicious code using a sandbox module.

In another example, processing satellite images (with a resolution of 0.5 m) identified clusters of equipment disguised as agricultural machinery. Based on an analysis of the thermal signature, shape, and configuration of the objects, as well as a comparison with previous movement patterns, the system classified them as potential launchers. After that, the duty modes of the anti-aircraft missile systems (AAMS) were automatically adjusted, and a message was generated for the operators.

These examples demonstrate how machine learning algorithms not only processed multimodal data in real time but also initiated an inter-system response, providing a multilayered response to a complex combined threat.

Critical infrastructure includes facilities that ensure the continuous functioning of the state and society, such as nuclear, hydro, and thermal power plants, command posts, communication centers, military airfields, as well as energy, logistics, and transport facilities. Their protection is a priority task in AD systems, as failures or damage to these facilities can have catastrophic consequences (Table 4).

Table 4. Critical infrastructure and the application of AI to protect it.

Critical infrastructure facility	AI role	Ai-powered functions
Nuclear power plant, hydroelectric power plant, combined heat and power plant	Providing adaptive protection	Training based on previous attacks
Command posts	Modeling protection scenarios	Use of digital twins
Communication centers	Improvement of system resilience	Protection against drone swarm attacks
Military airfields	Defense system automation	Improved response times
Energy, logistics, and transport facilities	Ensuring continuity of operations	Monitoring and rapid response to threats

Source: Elaborated by the authors based on Adewusi *et al.* (2024).

The integration of AI into the protection system for critical infrastructure creates new opportunities to improve the effectiveness of AD. One of the key advantages is the creation of adaptive AD systems that can learn from previous attacks and quickly adjust their actions in response to changing tactical situations. Such systems become more flexible and respond quickly to new threats.

The use of digital twins – virtual copies of physical objects – simulates various attack scenarios and evaluates the effectiveness of protective measures without risk to real infrastructure. This facilitates more accurate planning and optimization of defense resources.

AI also significantly increases resistance to drone swarm attacks, which are becoming increasingly common in modern conflicts. By rapidly analyzing the behavior of large numbers of small targets, AI systems can effectively detect and neutralize such threats, minimizing the risk of damage to critical assets.

As part of the modeling, online learning methods were implemented, adapting algorithms to new types of attacks in real time. Convolutional neural networks (CNNs) and XGBoost models were periodically retrained on new data samples obtained from modified attack scenarios. This reduced the false positive rate by 11.8% after three iterations of online learning and by 16.4% after five iterations in the test environment. The system's response time was reduced by an average of 0.9 seconds thanks to the increased relevance of classification decisions in new situations.

Digital twins were used to model attack scenarios on critical infrastructure, including the vulnerability of a command post to a simultaneous attack by a kamikaze drone and spoofing interference in the Global Positioning System (GPS). Eighteen virtual models of various facility configurations (logistics hubs, energy nodes, AD systems) were created, on which attack simulations were conducted, followed by an analysis of the effectiveness of AI defense systems. In 15 out of 18 cases, the system was able to detect the preparation of an attack in time, generate an appropriate command for EW means, and prevent the target from being reached.

The use of digital twins also identified the optimal parameters for sensor placement and AD deployment scenarios in complex urban environments, which were subsequently used to improve the architecture of sensor node placement in simulations. Thus, the use of digital twins and online training has increased the system's resilience to new threats and improved its response to atypical attack scenarios.

Therefore, the use of AI in critical infrastructure protection ensures increased security, responsiveness, and adaptability of AD systems, which is crucial in the modern environment of growing threats.

The introduction of AI into AD systems is associated with several significant challenges and risks that require careful analysis and thoughtful management to ensure safety and effectiveness (Table 5).

Table 5. Key challenges and risks of AI applications in AD systems.

Challenge/risk	Issue description	Possible consequences
Reliability	False positives can lead to the undesirable use of weapons	Increased risk of inadequate response
Cyber vulnerability	AI systems are the target of hacker attacks	Interference with AD operations, security breaches
Moral and ethical aspects	Autonomy in decision-making regarding fire	The emergence of ethical and legal issues
Data dependency	The quality of decisions directly depends on the accuracy of input data	Errors due to inaccurate or incomplete data

Source: Elaborated by the authors based on Márquez-Díaz (2024).

One of the main challenges is system reliability. For example, false positives – false alarms when the system identifies a civilian aircraft or delivery drone as a hostile target – can lead to the unjustified use of weapons, which carries serious technical problems and humanitarian consequences, such as civilian casualties. This creates a need to implement additional mechanisms for verifying and controlling decisions made by AI to reduce the risk of errors.

The cyber vulnerability of such systems is also substantial. For example, imagine a situation where attackers gain access to the AD control network through a cyberattack and steal or alter command data, leading to the unlawful opening of fire on friendly facilities or the complete paralysis of the defense system. Ensuring reliable cyber protection is becoming a critical condition for the smooth operation of such systems.

The moral and ethical aspects of autonomy are no less significant, especially in the context of decisions to open fire. Imagine a scenario where an autonomous system decides to destroy an air target without human confirmation, and that target is a civilian aircraft. Such a situation raises substantial questions about responsibility, transparency in decision-making, and the need to maintain human control in critical moments.

Furthermore, the effectiveness of AI systems depends largely on the quality of input data. For example, if outdated or incomplete data on enemy positions is received due to technical problems or deliberate interference, the system may misjudge the situation, leading to delays or incorrect actions in fast-paced combat operations.

Therefore, overcoming these challenges requires a comprehensive approach that includes technical, organizational, and ethical measures to ensure the safety, reliability, and acceptability of AI applications in AD.

To ensure a comprehensive comparative analysis of the effectiveness of machine learning algorithms, the computational characteristics of two environments were evaluated: MATLAB/Simulink with the Deep Learning Toolbox module and TensorFlow in the Python environment. The main tasks, such as CNN training, input sensor stream processing, and ensemble model implementation (random forest, XGBoost), were implemented in parallel on both platforms.

According to the simulation results, the training time for the CNN model in MATLAB/Simulink was approximately 28% longer than in TensorFlow (123 minutes versus 96 minutes for a similar dataset of 50,000 images), but MATLAB showed higher stability when simulating multi-component scenarios using built-in control blocks. The average input data processing speed (inference) in TensorFlow was 38 ms, and in MATLAB, it was 51 ms. At the same time, the integration of MATLAB with Simulink provided significant advantages for the visual design of complex control architectures in AD systems.

TensorFlow, in turn, provided greater flexibility in implementing online learning methods thanks to broad access to optimization libraries (Keras Tuner, TensorBoard), which is especially relevant for adapting models to new threats in real time. Resource consumption assessment showed that TensorFlow had a lower RAM load when batch processing large volumes of telemetry data.

Thus, MATLAB/Simulink was more effective for modeling control system behavior and provided convenient integration with digital twins of objects, while TensorFlow demonstrated advantages in performance during model training and implementation of dynamic threat response scenarios. Both environments complemented each other within the hybrid architecture of the study.

The simulated threat scenarios primarily assessed the technical interception capability, response speed, and coordination efficiency of AI-supported defense systems. Ethical risk matrices, including quantitative assessment of collateral damage or civilian aircraft misidentification, were not incorporated into the simulation framework and were considered only at the conceptual discussion level.

Global leaders in the defense sector are increasingly integrating AI into AD systems to improve the speed, accuracy, and adaptability of protection against modern threats. The introduction of AI not only automates many routine processes but also creates systems capable of learning, predicting enemy behavior, and making optimal decisions in real time. This experience demonstrates significant progress in the development of defense technologies and serves as an example for other countries seeking to modernize their security systems.

In the United States, as part of the AI-enabled C2 program, AI is being actively integrated into AD command and control systems. In particular, NORAD uses AI to automatically collect, analyze, and summarize data from various sources, which significantly accelerates the process of detecting air threats. In addition, Patriot complexes are equipped with intelligent systems that help predict the trajectories of enemy missiles and optimize the use of ammunition. This ensures a rapid and accurate response to threats, which is critical for the protection of large cities and strategic facilities (Johnson 2021).

In Israel, AI has been widely used in the Iron Dome system, one of the world's most famous AD systems. Artificial intelligence (AI) in this system performs the function of filtering out irrelevant or false targets, which significantly reduces the load on operators and can be used for the effective use of a limited number of interceptor missiles. In conditions of intense missile attacks, where speed of decision-making and accuracy are crucial, the use of AI has become one of the key factors for success. This demonstrates how adaptability and high-speed information processing can radically increase the combat effectiveness of a system (Slesinger 2022).

In Ukraine, given the current challenges, AI is also being actively implemented in AD. In particular, the use of AI to detect UAVs helps to increase the speed and accuracy of recognizing small targets, which are becoming increasingly common threats on the battlefield. In addition, the development of autonomous AD systems based on available sensors can be used for the creation

of effective and relatively inexpensive solutions for protecting critical infrastructure, even under conditions of limited resources. This approach illustrates the ability to adapt advanced technologies to the realities of modern conflict, thereby enhancing the country's defense capabilities (Samus 2024).

In Germany, AI is being integrated into modern AD systems as part of pan-European defense initiatives, including the Tactical Air Defense System (Taktisches Luftverteidigungssystem) (TLVS) and Future Combat Air System projects. Artificial intelligence (AI) is used for automated processing of data from radars and sensors, providing faster and more accurate classification of air targets, including supersonic missiles or drones with a low radar cross-section. For example, as part of the modernization of IRIS-T SLM complexes, which are also supplied to Ukraine, trajectory prediction and automatic threat prioritization modules are being introduced. This ensures high interception efficiency even in multidirectional attacks. German systems also participate in the North Atlantic Treaty Organization intelligence-sharing program to receive and process data from international sources using AI, thereby increasing overall situational awareness (Calcara *et al.* 2023).

In South Korea, the government and private corporations, including Hanwha Systems and LIG Nex1, are actively implementing AI into national AD systems. The new KM-SAM Block II AD system uses AI algorithms to quickly intercept ballistic missiles, particularly in the context of intense attacks from the Democratic People's Republic of Korea. Artificial intelligence (AI) is also used to detect UAVs in urban areas and to automate the control of short-range AD systems such as BIHO II. In addition, South Korea's autonomous combat systems development program involves the use of AI for automatic target tracking, optimal resource allocation, and interaction with other AD components, including satellite reconnaissance and aviation. Such integration significantly improves the effectiveness of responding to threats in fast-moving conflicts (Lee 2021).

In general, AI technologies have already been integrated into AD systems in the United States and Germany and are actively used in practice to improve defense effectiveness. In Israel, AI applications are also successfully operating in real combat conditions, particularly in the Iron Dome system. At the same time, in Ukraine, the implementation of AI is at the stage of active adaptation and local application, given the current challenges and resource constraints. In South Korea, AI technologies combine experimental developments with existing combat systems, which facilitates a rapid response to dynamic threats. Thus, the level of AI implementation varies from research to combat applications, depending on the country and the specifics of AD systems.

Thus, the experience of these countries demonstrates the effectiveness of using intelligent algorithms for automatic recognition and classification of air targets, which significantly increases the accuracy of threat detection. At the same time, the integration of adaptive models can optimize data processing and trajectory prediction, while centralized control systems ensure the coordination of various AD assets, increasing the overall effectiveness of protection. This comprehensive approach is becoming a key factor in the development of modern AD systems.

DISCUSSION

The analysis demonstrated that AI-based approaches substantially improve the adaptability and responsiveness of modern AD systems under simulated operational conditions. The findings indicate that machine learning models are particularly effective in processing heterogeneous sensor information and supporting rapid target classification in dynamically changing environments. The results also suggest that adaptive retraining mechanisms improve resilience to atmospheric interference and EW conditions, highlighting the importance of continuous model updating in defense-oriented AI systems. In addition to improving detection performance, clustering and ensemble approaches enhanced coordination between subsystems and contributed to faster operational responses. These findings support the broader trend toward data-driven and semi-autonomous defense architectures.

This problem was also studied by Thai *et al.* (2022), whose results confirmed that the use of computer vision to detect airborne targets is complicated by weather conditions, camouflage, and obstacles. Thanks to deep learning, systems can recognize objects even in cloudy conditions, smoke, or low light. This significantly increases the effectiveness of AD and reduces response time to threats.

Ajala *et al.* (2024) also showed that AI algorithms can analyze data from various sources and identify the most dangerous targets in real time. Such prioritization can allocate resources to critical threats. In combat conditions, this minimizes losses and increases the operational effectiveness of troops.

It is worth noting that the implementation of such technologies requires not only high-precision algorithms but also reliable integration with existing combat systems. This requires testing in real-world conditions and adaptation to changing tactical scenarios (Prikhod'ko *et al.* 2019). Only through close cooperation between AI developers and military experts can such solutions achieve maximum effectiveness.

In addition to recognition, AI has shown high efficiency in classifying threats using trajectory analysis and thermal and radar characteristics of objects (Seidaliyeva and Smailov 2025; Smailov *et al.* 2024; Wójcik *et al.* 2022). This can not only determine the degree of danger but also optimize the distribution of AD system resources. The XGBoost algorithm demonstrated the optimal overall classification accuracy of 93.8%, exceeding the random forest indicator of 90.4%, especially in conditions where complex features were considered. In turn, DBSCAN was better at detecting atypical objects with uneven target distribution, particularly in scenarios with a swarm of drones, where accuracy reached 89.2%, compared to 81.6% in k-means. The use of AI also improved the efficiency of existing weapons, considering the type of ammunition and distance to targets. This helped to increase the effectiveness of the system while reducing resource costs. Overall, the integration of AI into the centralized control structure increased the probability of successful threat interception by 12-15%.

Muda and Darat (2024) concluded that automated recognition of kamikaze drones is based on analysis of their visual forms and thermal radiation. Algorithms can quickly identify characteristic features, even if the drones are small or flying at low altitudes. This facilitates the timely detection of threats and the activation of countermeasures.

A study by Lui *et al.* (2023) revealed that missile trajectories are predicted using models that consider the speed, direction, wind conditions, and behavior of the missile. Thanks to machine learning, systems can make more accurate predictions in dynamic combat conditions. This significantly increases the probability of successful interception and reduces the damage from a missile strike.

These results confirm the above study, as they demonstrate the ability of modern algorithms to quickly process complex sensor data and make decisions in real time. The detection of kamikaze drones and the accurate prediction of missile trajectories are examples of the effective use of AI in combat conditions. This demonstrates the growing role of autonomous systems in security and defense (Alekseyenko *et al.* 2022; Voloshina *et al.* 2022).

The results obtained are consistent with data from other studies confirming the ability of modern AI algorithms to process large amounts of sensor information and make decisions in real time. In particular, the effective detection of kamikaze drones and the accurate prediction of missile trajectories demonstrate the potential of AI in combat conditions. This highlights the gradual transformation of modern defense systems towards autonomous solutions that can act quickly and with minimal human intervention. Automating the processing of intelligence signals and synthesizing various data sources creates a comprehensive picture of threats in real time (Prykhodko and Alekseyenko 2014; Prykhodko *et al.* 2019; Smailov *et al.* 2025). Thus, the use of AI can significantly increase the combat capability and responsiveness of AD units in a rapidly changing combat environment.

It is worth highlighting the study by Zohuri (2024), which shows that the use of AI for dynamic coordination of AD assets with EW systems can improve overall defense effectiveness. Artificial intelligence (AI) analyzes information in real time and optimally distributes resources between different systems. This ensures rapid adaptation to changing threats and minimizes the vulnerability of objects.

In turn, Alturki *et al.* (2023) concluded that integrating AI into satellite and aerial reconnaissance facilitates early detection of attacks through automatic analysis of large amounts of data. Artificial intelligence (AI) can recognize anomalies and potential threats at an early stage, providing more time to respond. This approach significantly improves situational awareness and enhances overall security.

These data correspond to the theses presented in the previous section, as they confirm the importance of operational interaction between different defense systems to increase overall effectiveness. Dynamic coordination of AD and EW using AI can not only respond quickly to threats but also predict their evolution in real time (Dolzhenko *et al.* 2025). This creates a significant advantage in complex combat conditions, where every second can be crucial.

Within the framework of interaction with other components of defense, EW, cyber defense, satellite and aerial reconnaissance, AI demonstrates significant potential in improving situational awareness (Glazyrina *et al.* 2024; Kiurchev *et al.* 2025; Kyurchev *et al.* 2024). A comprehensive analysis of intelligence information combined with forecasting of potential threats provides a quick response to critical events. In particular, the use of digital twins detected and prevented breaches in 15 out of 18 simulated threat

scenarios, demonstrating the practical effectiveness of such approaches. Artificial intelligence (AI) can also be used as an effective tool for detecting complex cross-domain threats that span both physical and cyberspace. Its adaptability can be used to quickly configure the system to new types of threats, ensuring flexibility and reliability in a dynamic environment.

Krishnaveni *et al.* (2024) also conducted a study, the results of which confirmed that digital twins support the development of virtual copies of strategic objects for detailed modeling of their operation and vulnerabilities. This predicted the consequences of various attack scenarios and evaluated the effectiveness of defense measures. As a result, resources can be optimized, and the resilience of objects to threats can be increased.

Wang *et al.* (2024) also demonstrated that the application of AI to repel attacks by swarms of drones on energy and communications facilities assists in the timely detection and neutralization of multiple threats. Intelligent systems coordinate the actions of defense complexes, responding quickly to changing enemy tactics. This significantly reduces the risk of damage to critical infrastructure and ensures its continuity of operation.

Comparing the data obtained during the research, it can be confidently stated that digital twins are central to increasing the readiness of strategic facilities for potential attacks. They can be used not only to simulate real conditions but also to test various protection options without risk to the infrastructure itself. Thus, the introduction of digital twins significantly improves the quality of decision-making and contributes to more effective planning of defense measures.

At the same time, the study identified several pressing challenges associated with the implementation of AI in AD systems. Among the main risks is the possibility of false positives, which can lead to erroneous combat actions (Dolzhenko *et al.* 2020; Imasheva *et al.* 2018). Although the rate of such false positives has been reduced to 5.6%, and the use of online training has reduced them by 16.4%, the problem remains relevant. Adaptive models with self-learning capabilities showed a 16.4% reduction in false positives after several iterations, but constant updating and verification of models are required to ensure system reliability. The cyber vulnerability of such systems poses a separate threat, requiring the implementation of additional security measures. In addition, ethical issues regarding the autonomous use of force remain unresolved, requiring regulatory and international legal regulation.

Veprytska and Kharchenko (2024) concluded that the threat of cyberattacks on AI systems in AD is growing due to their critical role in protecting airspace and their dependence on network connectivity. Malicious actors may attempt to interfere with algorithms or steal data, compromising the accuracy and reliability of the system. To counter this, multilayered security measures are used, including encryption, anomaly monitoring, and adaptive attack detection algorithms.

Rosendorf *et al.* (2022) discovered that the ethical dilemmas of autonomous weapon use against air targets are linked to questions of responsibility for mistakes and damage caused to civilian objects. Autonomous systems can make decisions without human intervention, raising concerns about ethics and control. It is necessary to establish rules and standards for the use of such technologies to ensure the responsible and humane use of force.

Analysis of the results of the study determined that protection of AI systems in AD against cyberattacks is no less relevant than their technical effectiveness. Without proper security measures, even the most advanced algorithms can become vulnerable and be used against their own defense. This highlights the need for a comprehensive approach that combines technological innovation with ethical and legal standards to ensure the security and trustworthiness of autonomous systems.

Therefore, the results obtained indicate that the introduction of AI into AD systems significantly increases their effectiveness and adaptability, while requiring the overcoming of technical and ethical challenges. This emphasizes the need for a comprehensive approach that includes continuous technological improvement, strict security protocols, and responsible regulation.

CONCLUSION

The study demonstrated the high effectiveness of AI integration into AD systems, which significantly improves threat detection accuracy, response speed, and system adaptability to changing environments. The use of CNNs ensured 92.8% accuracy in the classification of air targets, while ensemble models, in particular XGBoost, achieved up to 93.8% accuracy. Clustering algorithms such as DBSCAN reduced the average target designation time to 1.4 seconds, ensuring rapid transmission of coordinates for target engagement.

Centralized AI-based control increased the probability of successful target interception by 12-15% compared to traditional approaches. Modeling has shown that AI effectively coordinates actions with other components of the defense system, such as EW, cyber defense and intelligence, ensuring a coordinated response to complex combined attacks. Artificial intelligence (AI) is capable of adaptively changing the parameters of EW, analyzing signs of cyberattacks, and using satellite intelligence data to predict threats.

The use of digital twins accurately simulated attack scenarios on critical infrastructure, preventing breaches in 15 out of 18 cases. Online training of the system reduced the number of false positives by 16.4% after just a few iterations. Thus, the results of the study support the potential feasibility of implementing AI-based multi-component AD systems under simulated operational conditions.

At the same time, the paper identifies key challenges: the risk of false positives, cyber vulnerability of systems, ethical issues of autonomous decision-making, and dependence on the quality of input data. A comparative analysis of the experiences of the United States, Israel, Ukraine, Germany, and South Korea demonstrates different approaches to AI implementation, ranging from high-tech systems (e.g., IRIS-T SLM and TLVS in Germany) to adaptive solutions that take local threats into account (KM-SAM Block II and BIHO II in South Korea). These examples illustrate the potential and challenges that require further research and development in theoretical and practical aspects.

The limitation of the study is the lack of large-scale field tests of integrated AI systems in real combat conditions with various types of threats. It is necessary to investigate the impact of deep learning algorithms on the prediction of complex maneuvers of high-speed missiles and kamikaze drones in conditions of active EW, particularly with consideration of dynamic trajectory changes, sensor system misinformation, and GPS signal loss, which create prospects for the development of interference-resistant adaptive navigation and targeting systems. In the context of the hybrid war waged by the Russian Federation against Ukraine, the integration of AI into AD systems is not only a technological necessity but also a key element in ensuring national security, capable of minimizing losses, responding quickly to complex air threats and increasing the effectiveness of critical infrastructure protection.

In addition, the simulations focused primarily on technical interception performance and coordination efficiency rather than quantitative modeling of civilian risk or collateral-damage scenarios. Further research should include operational testing, ethical decision constraints, and human-in-the-loop validation mechanisms for autonomous defense applications.

CONFLICT OF INTERESTS

Nothing to declare.

AUTHOR CONTRIBUTIONS

Conceptualization: Volkov A; **Data curation:** Volkov A and Brechka M; **Formal analysis:** Volkov A and Brechka M; **Investigation:** Brechka M and Lytvynenko M; **Methodology:** Lytvynenko M and Yaroshchuk V; **Writing – original draft:** Lytvynenko M and Yaroshchuk V; **Writing – review & editing:** Yaroshchuk V and Korsunov; **Project administration:** Volkov A; **Supervision:** Korsunov S; **Final approval:** Volkov A.

DATA AVAILABILITY STATEMENT

All datasets were generated or analyzed in the current study.

DECLARATION OF USE OF ARTIFICIAL INTELLIGENCE TOOLS

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

FUNDING

Not applicable.

ACKNOWLEDGEMENTS

Not applicable.

REFERENCES

Adewusi AO, Okoli UI, Olorunsogo T, Adaga E, Daraojimba DO, Obi OC (2024) Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA review. World J Adv Res Rev 21(1):2263-2275. https://doi.org/10.30574/wjarr.2024.21.1.0313

Ajala OA, Okoye CC, Ofodile OC, Arinze CA, Daraojimba OD (2024) Review of AI and machine learning applications to predict and thwart cyber-attacks in real-time. Magna Sci Adv Res Rev 10(1):312-320. https://doi.org/10.30574/msarr.2024.10.1.0037

Alekseyenko S, Dreus A, Dron M, Brazaluk O (2022) Numerical study of aerodynamic characteristics of a pointed plate of variable elongation in subsonic and supersonic gas flow. J Adv Res Fluid Mech Therm Sci 96(2):88-97. https://doi.org/10.37934/arfmts.96.2.8897

Alturki N, Aljrees T, Umer M, Ishaq A, Alsubai S, Saidani O, Djuraev S, Ashraf I (2023) An intelligent framework for cyber-physical satellite system and IoT-aided aerial vehicle security threat detection. Sensors 23(16):7154. https://doi.org/10.3390/s23167154

Calcara A, Gilli A, Gilli M (2023) Short-term readiness, long-term innovation: the European defence industry in turbulent times. Def Stud 23(4):626-643. https://doi.org/10.1080/14702436.2023.2277439

Criollo L, Mena-Arciniega C, Xing S (2024) Classification, military applications, and opportunities of unmanned aerial vehicles. Aviation 28(2):115-127. https://doi.org/10.3846/aviation.2024.21672

Dolzhenko N, Assilbekova I, Konakbay Z, Garmash O, Muratbekova G (2025) Organization of transport services and transport process safety. Period Polytech Transp Eng 53(3):277-291. https://doi.org/10.3311/PPtr.38137

Dolzhenko N, Mailyanova E, Toluev Y, Assilbekova I (2020) Influence of system errors in meteorological support on flights safety. News Natl Acad Sci Repub Kazakhstan Ser Geol Tech Sci 5(443):81-88. https://doi.org/10.32014/2020.2518-170X.107

Glazyrina N, Muratkhan R, Eslyamov S, Murzabekova G, Aziyeva N, Rysbekkyzy B, Orynbayeva A, Baktiyarova N (2024) Deep neural networks for removing clouds and nebulae from satellite images. Int J Electr Comput Eng 14(5):5390-5399. https://doi.org/10.11591/ijece.v14i5.pp5390-5399

Hashimov E, Khudeynatov E (2024) Methodology for assessing the effectiveness of the air defense system. Control Navig Commun Syst Collect Sci Pap 1(75):21-27. https://doi.org/10.26906/SUNZ.2024.1.021

Imasheva GM, Dolzhenko NA, Anayatova RK, Doronina YV (2018) Commercial use of aircraft based on safety risk. J Adv Res Law Econ 9(8):2615-2621. https://doi.org/10.14505//jarle.v9.8(38).10

Insaurralde CC, Blasch E (2022) Situation awareness decision support system for air traffic management using ontological reasoning. J Aerosp Inf Syst 19(3):224-245. https://doi.org/10.2514/1.I010989

Javaid S, Saeed N, Qadir Z, Fahim H, He B, Song H, Bilal M (2023) Communication and control in collaborative UAVs: recent advances and future trends. IEEE Trans Intell Transp Syst 24(6):5719-5739. https://doi.org/10.1109/TITS.2023.3248841

Johnson J (2021) "Catalytic nuclear war" in the age of artificial intelligence & autonomy: emerging military technology and escalation risk between nuclear-armed states. J Strateg Stud 1-41. https://doi.org/10.1080/01402390.2020.1867541

Khan A, Imam I, Azam A (2021) Role of artificial intelligence in defence strategy. Strategic Stud 41(1):19-40. https://doi.org/10.53532/ss.041.01.0058

Kiurchev S, Kyurchev V, Radkevych O, Fatyeyev O, Hrechka I (2025) Monitoring the accuracy of manufacturing elements of the end distribution system of a hydraulic motor planetary type. Lect Notes Mech Eng 1:712-723. https://doi.org/10.1007/978-3-031-82746-4_63

Krishnaveni S, Chen TM, Sathiyanarayanan M, Amutha B (2024) CyberDefender: an integrated intelligent defense framework for digital-twin-based industrial cyber-physical systems. Cluster Comput 27(6):7273-7306. https://doi.org/10.1007/s10586-024-04320-x

Kuleshov YA, Nagpal K, Ucpinar K, Gadaginmath A, Gadaginmath S, O'Daniel K, Sun D, Tan L, Veatch N, Monangi H (2024) Cyber-attacks on avionics networks in digital twin environment: detection and defense. Paper presented 2024 American Institute of Aeronautics and Astronautics SciTech 2024 Forum. AIAA; Reston, USA. https://doi.org/10.2514/6.2024-0277

Kyurchev V, Kiurchev S, Rezvaya K, Fatyeyev A, Głowacki S (2024) Assessing the reliability of a mathematical model of working processes occurring in a hydraulic drive. Lect Notes Mech Eng 1:281-292. https://doi.org/10.1007/978-3-031-63720-9_24

Lee S (2021) A case study of AI DEFENSE applications in major Northeast Asian states and strategies for building a ROK's AI-based national defense system. Int J Terror Natl Secur 6(1):1-13. https://doi.org/10.22471/terrorism.2021.6.1.01

Lui DG, Tartaglione G, Conti F, De Tommasi G, Santini S (2023) Long short-term memory-based neural networks for missile maneuvers trajectories prediction. IEEE Access 11:30819-30831. https://doi.org/10.1109/ACCESS.2023.3262023

Márquez-Díaz JE (2024) Benefits and challenges of military artificial intelligence in the field of defense. Comput Syst 28(2):309-323. https://doi.org/10.13053/cys-28-2-4684

Muda NRS, Darat YPA (2024) Design and development of the angel kamikaze drone based on object recognition using image processing. Int J Nanotech Robot Sci Manuf 4(6):80-94. https://doi.org/10.13140/RG.2.2.33496.10244

Nantogma S, Xu Y, Ran W (2021) A coordinated air defense learning system based on immunized classifier systems. Symmetry 13(2):271. https://doi.org/10.3390/sym13020271

Prikhod'ko AA, Alekseenko SV, Chmovzh VV (2019) Experimental investigation of the influence of the shape of ice outgrowths on the aerodynamic characteristics of the wing. J Eng Phys Thermophys 92(2):486-492. https://doi.org/10.1007/s10891-019-01955-1

Prykhodko AA, Alekseyenko SV, Prikhodko VV (2019) Numerical investigation of the influence of horn ice formation on airfoils aerodynamic performances. Int J Fluid Mech Res 46(6):499-508. https://doi.org/10.1615/InterJFluidMechRes.2019026024

Prykhodko OA, Alekseyenko SV (2014) Numerical simulation of the process of airfoil icing in the presence of large supercooled water drops. Tech Phys Lett 40(10):864-867. https://doi.org/10.1134/S1063785014100125

Rosendorf O, Smetana M, Vranka M (2022) Autonomous weapons and ethical judgments: experimental evidence on attitudes toward the military use of "killer robots". Peace Confl J Peace Psychol 28(2):177-183. https://doi.org/10.1037/pac0000601

Samadzadegan F, Dadrass Javan F, Ashtari Mahini F, Gholamshahi M (2022) Detection and recognition of drones based on a deep convolutional neural network using visible imagery. Aerospace 9(1):31. https://doi.org/10.3390/aerospace9010031

Samus M (2024) Lessons learned from the war in Ukraine: the impact of drones. New Strategy Center, Bucharest. [accessed 2026 Jan 13]. http://web.archive.org/web/20260113223241/https://newstrategycenter.ro/project/lessons-learned-from-the-war-in-ukraine-the-impact-of-drones-2/

Santhi K, Shri ML, Joshi S, Sharma G (2024) AI in defence and ethical concerns. Paper presented 2024 Second International Conference on Emerging Trends in Information Technology and Engineering. IEEE; Vellore, India. https://doi.org/10.1109/ic-ETITE58242.2024.10493592

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

Slesinger I (2022) A strange sky: security atmospheres and the technological management of geopolitical conflict in the case of Israel's Iron Dome. Geogr J 188(3):429-443. https://doi.org/10.1111/geoj.12444

Smailov N, Orynbet M, Nazarova A, Torekhan Z, Koshkinbayev S, Yssyraiyl K, Kadyrova R, Sabibolda A (2025) Optimization of fiber-optic sensor performance in space environments. Inform Autom Pomiary Gospod Ochr Srodowiska 15(2):130-134. https://doi.org/10.35784/iapgos.7200

Smailov N, Tsyporenko V, Sabibolda A, Tsyporenko V, Abdykadyrov A, Kabdoldina A, Dosbayev Z, Ualiyev Z, Kadyrova R (2024) Streamlining digital correlation-interferometric direction finding with spatial analytical signal. Inform Autom Pomiary Gospod Ochr Środowiska 14(3):43-48. https://doi.org/10.35784/iapgos.6177

Song R, Liu B, Xue S, Li H, Li J, Zhang Z (2023) Air target threat assessment: A kernel extreme learning machine based on a multistrategy improved sparrow search algorithm. Math Probl Eng 1:1315506. https://doi.org/10.1155/2023/1315506

Steingartner W, Galinec D, Kozina A (2021) Threat defense: Cyber deception approach and education for resilience in hybrid threats model. Symmetry 13(4):597. https://doi.org/10.3390/sym13040597

Thai P, Alam S, Lilith N, Nguyen BT (2022) A computer vision framework using convolutional neural networks for airport-airside surveillance. Transp Res Part C Emerg Technol 137:103590. https://doi.org/10.1016/j.trc.2022.103590

Veprytska O, Kharchenko V (2024) Analysis of AI powered attacks and protection of UAV assets: quality model-based assessing cybersecurity of mobile system for demining. Paper presented 2022 5th International Workshop on Intelligent Information Technologies and Systems of Information Security. Khmelnytskyi National University; Khmelnytskyi, Ukraine. https://ceur-ws.org/Vol-3675/paper26.pdf

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 Energetics 14(4):23-32. https://doi.org/10.31548/machinery/4.2023.23

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. Mil Logist Syst 61(2):211-228. https://doi.org/10.37055/slw/203558

Voloshina A, Panchenko A, Boltyansky O, Zasiadko A, Verkholantseva V (2022) Improvement of the angular arrangement of distribution system windows when designing planetary hydraulic machines. Lect Notes Mech Eng 1:53-63. https://doi.org/10.1007/978-3-030-91327-4_6

Wang X, Zhao Z, Yi L, Ning Z, Guo L, Yu FR, Guo S (2024) A survey on security of UAV swarm networks: attacks and countermeasures. ACM Comput Surv 57(3):74. https://doi.org/10.1145/3703625

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

Yu A, Kolotylo I, Hashim HA, Eltoukhy AE (2025) Electronic warfare cyberattacks, countermeasures and modern defensive strategies of UAV avionics: a survey. IEEE Access 13:68660-68681. https://doi.org/10.1109/ACCESS.2025.3561068

Zhao M, Wang G, Fu Q, Quan W, Wen Q, Wang X, Li T, Chen Y, Xue S, Han J (2024) Intelligent decision-making system of air defense resource allocation via hierarchical reinforcement learning. Int J Intell Syst 1:7777050. https://doi.org/10.1155/2024/7777050

Zohuri B (2024) Harnessing artificial intelligence for countering hypersonic weapons: a new frontier in battlefield offense and defense (a short review). J Energy Power Eng 18(4):139-145. https://doi.org/10.17265/1934-8975/2024.04.002