Architectural Patterns and Performance Implications of AI-Integrated Optoelectronic Systems for Defense Applications

Alexandru-Dragoş Adam, Nirvana Popescu

Faculty of Automatic Control and Computer Science, National University of Science and Technology POLITEHNICA Bucharest, Bucharest 060042, Romania (email: alexandru.adam2610@stud.acs.upb.ro, nirvana.popescu@upb.ro)

Abstract: Artificial intelligence (AI) is increasingly embedded into optoelectronic (EO) and EO/IR defense systems to enable faster perception, autonomous or human-assisted decision-making, and resilient operation in contested environments. This paper presents an adapted PRISMA-like review and critical synthesis of AI-integrated EO systems for defense applications, with emphasis on system architectures and their performance implications across surveillance, recognition, safety-critical and mission-critical use cases. From an initial pool of approximately 3,700 records screened across major scientific databases, 32 primary studies were selected for in-depth analysis and categorized by sensing modality (EO, IR, hyperspectral, multi-sensor fusion), task type (detection, classification, tracking, anomaly detection), and deployment constraints (edge vs. centralized processing, latency, power, and reliability requirements). Rather than ranking methods by reported accuracy—which is often non-comparable due to heterogeneous datasets and evaluation protocols—this study highlights how architectural choices and operational conditions shape real-world performance, including common failure modes such as weather degradation, occlusion, sensor drift, domain shift, and adversarial interference. The synthesis identifies recurring design patterns (hybrid edge–cloud pipelines, safety-isolated compute domains, and human-autonomy teaming loops) and summarizes research gaps in standardization, certification/verification, robustness, and explainability needed for deployable defense systems.

Keywords: artificial intelligence; optoelectronic systems; EO/IR; defense; surveillance; recognition; safety-critical systems; mission-critical systems; PRISMA-like review; operational robustness.

1. INTRODUCTION

The increasing complexity and technological intensity of modern warfare have driven the defense industry to adopt advanced sensing and intelligent processing capabilities, integrating traditional platforms with artificial intelligence (AI). Among the key technological advances reshaping defense systems is the integration of AI with optoelectronic (EO) technologies. Optoelectronic systems, which involve the interaction of light with electronic devices, have long played a crucial role in defense applications such as surveillance, reconnaissance, targeting, and communications. With the rapid evolution of AI methods, these systems have become increasingly adaptive and data-driven, enabling new operational paradigms centered on real-time perception and decision support.

AI-integrated optoelectronic systems offer enhanced capabilities including automated detection, real-time data processing, and improved situational awareness. Such integration is especially relevant in environments where human intervention is constrained, including unmanned aerial vehicles (UAVs) (Kaleem et al., 2024; Matthew et al., 2021), missile defense infrastructures, and distributed surveillance networks. The fusion of AI and EO sensing contributes to reduced reaction times, faster threat identification, and improved mission effectiveness under dynamic and uncertain operational conditions.

Beyond automation, AI plays a growing role in safety-critical and mission-critical defense infrastructures, supporting predictive maintenance, anomaly detection, and intelligent decision-making pipelines. Machine learning models are increasingly applied to large volumes of visual and sensor data to detect patterns, classify objects, and assist operators in complex environments. Recognition systems based on deep learning architectures, including facial and object recognition frameworks, have demonstrated significant progress in controlled scenarios (Fola-Rose et al., 2024). However, translating these capabilities into real-world operational settings remains an ongoing challenge.

Despite the growing body of literature on AI-enabled defense technologies, many existing studies focus on isolated algorithms or application-specific implementations rather than system-level architectural considerations. Furthermore, performance metrics reported across studies are often derived from heterogeneous datasets and evaluation protocols, limiting direct comparison between methods. As a result, there is a need for a structured synthesis that examines how architectural design choices, sensing modalities, and deployment constraints influence the operational performance of AI-integrated optoelectronic systems.

Recent advancements in artificial intelligence and optoelectronic sensing have significantly impacted defense technologies requiring high precision, low latency, and robust data processing (Oran et al., 2023; Shimoni et al., 2019; Ruban et al., 2018). EO systems, including infrared, hyperspectral, and multi-sensor fusion platforms, form the backbone of modern ISR architectures by enabling advanced imaging and environmental perception (Lan et al., 2022; Maung et al., 2020; Liu et al., 2020). The integration of AI into these systems supports scalable decision-making frameworks and enhances resilience in complex operational environments.

Key intersections between AI and optoelectronic systems include surveillance, recognition, safety-critical infrastructures, and mission-critical decision pipelines. AI-driven surveillance solutions can analyze large-scale video streams in real time, while recognition systems provide rapid identification capabilities essential for secure defense operations. In safety-critical and mission-critical contexts, AI contributes to improved reliability through intelligent monitoring and adaptive control mechanisms (Margulies, 2016; Rawat et al., 2021; Khlaaf et al., 2024; Sebastião, 2023).

Rather than providing a purely descriptive overview, this paper focuses on the architectural patterns and performance implications of AI-integrated optoelectronic defense systems. To support this analysis, an adapted PRISMA-like literature review strategy was employed to identify representative studies across surveillance, recognition, safety-critical, and mission-critical domains.

The main contributions of this work are:

• proposing an architectural perspective on AI-integrated optoelectronic systems in defense applications;
• synthesizing representative studies using an adapted PRISMA-like selection methodology;
• analyzing performance implications beyond reported accuracy metrics, with emphasis on deployment constraints;
• identifying operational gaps, common failure modes, and research directions relevant to real-world defense environments.

2. RELATED WORK AND CONTEXT

AI integration in defense-oriented optoelectronic (EO) and EO/IR systems has been addressed in prior surveys and domain reports, typically emphasizing algorithmic performance (e.g., detection/classification accuracy) or focusing on a single application domain (e.g., surveillance, recognition, or cybersecurity). However, defense deployments frequently operate under constraints that are not captured by algorithm-centric reviews: limited onboard compute and power (SWaP), latency bounds for time-critical actions, degraded or intermittent communications, and adversarial pressure affecting both sensing and networking.

Related work can be broadly grouped into: (i) computer-vision–centric surveys (object detection, tracking, facial recognition), (ii) sensing-modality–centric studies (EO/IR and hyperspectral imaging for ISR), (iii) safety/mission-critical AI and certification-focused literature, and (iv) resilience/cybersecurity perspectives addressing adversarial manipulation and infrastructure threats. While these directions provide valuable building blocks, they often do not offer a unified synthesis of system-level architectural patterns—such as edge–cloud partitioning, safety-isolated compute domains, hybrid human–autonomy loops, and resilience mechanisms—and how these patterns shape deployable performance in operational settings.

This paper positions its contribution at the intersection of these streams by synthesizing representative studies through an architectural and performance-implications lens. Rather than treating reported accuracy as a comparable benchmark across heterogeneous datasets, the review emphasizes how sensing modality, inference location, and assurance constraints determine real-world outcomes and failure behavior.

3. RESEARCH METHODOLOGY

To provide a rigorous examination of AI-integrated optoelectronic systems in defense applications, this study employed an adapted PRISMA-like review methodology designed to support architectural and performance-oriented synthesis rather than direct quantitative comparison of algorithms. The objective of this approach was not to rank individual methods by reported accuracy, but to identify recurring architectural patterns, operational constraints, and deployment implications across representative studies.

The literature search was conducted using major academic and technical databases, including IEEE Xplore, Google Scholar, ScienceDirect, SpringerLink, and specialized defense-related journals. Articles published between 2018 and 2024 were considered to capture recent developments in AI-enabled optoelectronic systems.

The initial identification phase yielded 3,700 records (IEEE Xplore: 2,455; defense-related journals: 122; Google Scholar: 1,123). After duplicate removal, 2,965 unique records remained. Title and abstract screening excluded 2,513 records, leaving 452 articles for full-text eligibility assessment. At this stage, 323 articles were excluded because they lacked sufficient technical detail, did not address defense-oriented optoelectronic sensing, or did not provide enough deployment-relevant context. The remaining 129 articles were examined in detail, of which 32 primary studies were retained for the final qualitative synthesis because they most directly supported the architectural and operational analysis developed in this review.

Rather than functioning as strict filtering criteria, a set of research questions guided the analytical framework of the review:

RQ1: What image processing and AI architectures are used in defense-oriented optoelectronic systems?
RQ2: Which architectural design choices support robustness and operational deployment?
RQ3: How is optoelectronic sensor data integrated into AI-driven decision pipelines?
RQ4: Which AI paradigms appear most frequently across surveillance and recognition tasks?

3.1 Search Strategy and Article Selection

The article selection process combined database querying with staged screening aligned with PRISMA-inspired practices. Queries were constructed using three conceptual blocks:

- Sensing domain: “optoelectronic”, “electro-optical”, “EO/IR”, “infrared”, “hyperspectral”, “ISR”, “multi-sensor fusion”

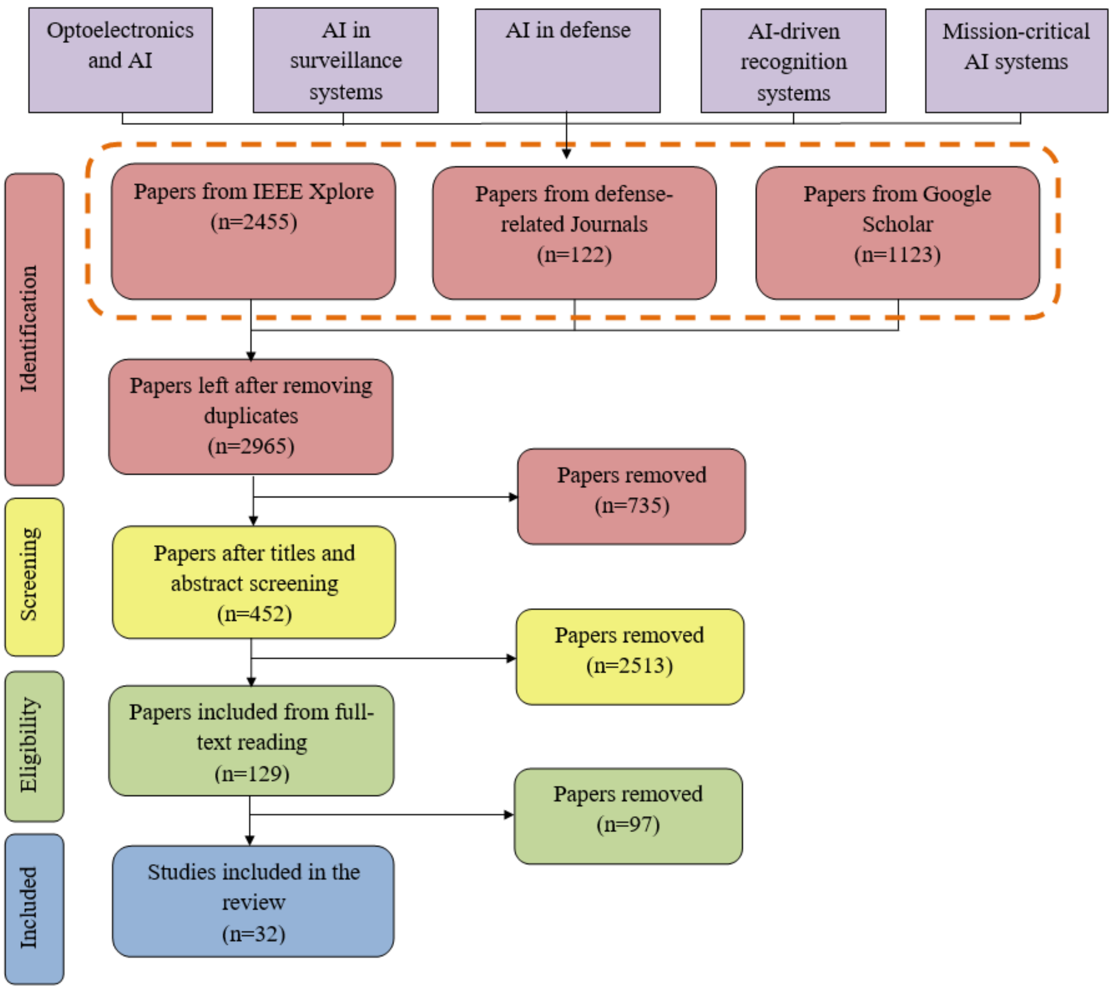

Fig. 1. Adapted PRISMA-like workflow illustrating the identification, screening, eligibility, and inclusion stages for selecting studies on AI-integrated optoelectronic systems in defense applications.

- AI methods/tasks: "machine learning", "deep learning", "computer vision", "object detection", "tracking", "recognition", "anomaly detection"
- Operational context: "defense", "military", "surveillance", "reconnaissance", "border security"

To provide transparency and traceability of the literature selection process, Figure 1 illustrates the adapted PRISMA-like workflow used in this study. The diagram summarizes the main stages of article identification, screening, eligibility assessment, and inclusion, reflecting the structured methodology described in this section.

The process begins with the identification of records from multiple sources, including IEEE Xplore, Google Scholar, and defense-related journals. After duplicate removal, the screening stage filters studies based on titles and abstracts, excluding works that do not align with the scope of AI-integrated optoelectronic systems in defense. The eligibility phase consists of full-text analysis, where articles are assessed according to their technical relevance and their contribution to architectural and operational understanding. Finally, the inclusion stage retains a subset of representative studies used for qualitative synthesis.

The numerical values associated with each stage indicate the number of records remaining after each filtering step, providing a quantitative overview of the selection process and ensuring methodological consistency across the review.

Records were excluded during screening when they focused exclusively on civilian scenarios, lacked technical or methodological content, or did not involve optoelectronic sensing pipelines. Full-text eligibility assessment further removed studies that provided algorithmic descriptions without deployment context or lacked sufficient evaluation detail to support architectural interpretation.

Inclusion criteria prioritized peer-reviewed studies describing AI integration within optoelectronic or multi-sensor defense systems, particularly those discussing deployment constraints, system architectures, or operational performance implications.

3.2 Research Scope

The scope of the review defines the thematic boundaries of the analysis rather than the methodological procedure itself. The selected studies span five interconnected domains relevant to AI-integrated optoelectronic defense technologies:

- surveillance architectures and distributed sensing pipelines;

- recognition systems and biometric or object-detection frameworks;
- optoelectronic sensing and EO/IR data processing;
- safety-critical infrastructures requiring reliability and certification;
- mission-critical decision-support and human–autonomy collaboration.

Particular emphasis is placed on architectural configurations, deployment contexts, and system-level trade-offs rather than isolated algorithmic benchmarking.

3.3 Analysis Framework

The selected studies were analyzed using a qualitative synthesis framework focused on architectural and operational interpretation. Instead of comparing reported accuracy values across heterogeneous datasets, the analysis employed consistent evaluation dimensions derived from the research questions.

Each study was examined with respect to:

- sensing modality (EO, IR, hyperspectral, or multi-sensor fusion);
- inference location and architecture (edge, centralized, or hybrid pipelines);
- deployment constraints such as latency, power consumption, and communication limitations;
- evaluation context (controlled laboratory settings versus operational environments);
- robustness considerations, including environmental degradation, occlusion, domain shift, or adversarial threats.

This framework enables cross-domain synthesis by emphasizing system-level behavior and design trade-offs rather than numerical performance rankings, supporting the architectural analysis presented in Section 4.

4. ARCHITECTURAL PATTERNS AND PERFORMANCE IMPLICATIONS OF AI-INTEGRATED OPTOELECTRONIC DEFENSE SYSTEMS

Following the systematic methodology described in Section 3, the selected studies were analyzed through a comparative framework rather than a purely descriptive narrative. Each work was examined across multiple analytical dimensions, including sensing modality, inference location (edge vs centralized), operational constraints, safety- or mission-critical requirements, and robustness considerations. Unlike taxonomy-oriented review papers that organize literature strictly by algorithmic stages, this section synthesizes the analyzed studies according to architectural deployment patterns and operational constraints relevant to defense environments.

Therefore, this section does not aim to compare absolute performance values between studies. The reviewed works rely on heterogeneous datasets, sensing platforms, and evaluation protocols, which limits direct quantitative comparison. Instead, the analysis focuses on architectural characteristics, deployment constraints, and operational implications.

To support the architectural synthesis presented in this section, Tables 1–6 summarize representative studies across surveillance, recognition, optoelectronic sensing, safety-critical, and mission-critical domains. The tables are not intended to provide a direct quantitative comparison between methods, but rather to highlight how different approaches contribute to architectural design choices and operational deployment considerations.

4.1 Architectural Characteristics of AI-Enabled Surveillance Systems

Across surveillance applications, the literature shows a clear transition from isolated detection models toward integrated AI pipelines composed of acquisition, preprocessing, detection, tracking, behavior interpretation, and automated alert mechanisms. In operational environments, overall system performance depends less on marginal differences between neural network architectures and more on latency, computational constraints, sensor quality, and communication reliability.

Edge-deployed platforms validated on resource-constrained unmanned ground vehicles illustrate how architectural efficiency and hardware-aware model selection become critical design factors [1]. A representative example is the land-warfare UGV surveillance system in [1], where multiple detectors (SSD, CenterNet, Faster R-CNN) are compared under embedded constraints; the reported results (including mAP and IoU-based inference performance) underline the practical relevance of selecting architectures that preserve real-time throughput on limited compute.

Hybrid spatial–temporal approaches combining convolutional and recurrent neural networks extend surveillance capabilities from object detection toward behavioral analysis and anomaly detection, although they introduce increased computational load and sensitivity to latency [2–4]. This is reflected in works that explicitly combine CNN-based spatial perception with RNN-based temporal modeling for anomaly detection in video streams and dynamic perimeters [2–4], where authors repeatedly note trade-offs between detection performance and end-to-end latency as model complexity grows.

A recurring observation across surveillance studies is the performance gap between controlled experimental conditions and operational deployments. Environmental variability, occlusions, illumination changes, and bandwidth limitations frequently degrade performance once systems leave laboratory conditions. Consequently, recent work increasingly emphasizes distributed processing, edge optimization, and cybersecurity integration as key components of surveillance architectures [5,6]. Beyond physical sensing, [6] extends the surveillance stack to the protection of the surveillance infrastructure itself, discussing AI-based detection and mitigation of cyber threats (e.g., zero-day and ransomware patterns) as part of an end-to-end resilient surveillance architecture. Table 1 summarizes representative studies on AI-enabled surveillance systems and their relevance to architectural and operational considerations.

Table 1. Representative studies on AI-enabled surveillance systems in defense applications, categorized by focus area, AI method, and architectural relevance.

Article Reference	Focus Area	AI Method	Relevance
Shahnoor, Shaikh F., et al. [1]	AI in real-time surveillance	Deep Learning Algorithms	High
Iqbal, Muhammad Javed, et al.[2]	Object detection and tracking	Convolutional Neural Networks	High
Vashishth, Tarun Kumar, et al. [3]	Predictive analytics in surveillance	Recurrent Neural Networks	Medium
Shabbir, Aiman, et al. [4]	Accuracy in automated surveillance	CNNs and RNNs	High
Abba, Sani, et al. [5]	Security monitoring with AI	Multi-layer Perceptrons	Medium
Huyen, Nguyen Thi Minh, and Tran Quoc Bao. [6]	AI in enhancing cybersecurity	Reinforcement AI	Medium

4.2 Recognition Systems in Defense: Operational and Security Perspectives

Recognition technologies in defense have evolved from standalone classifiers into interconnected security infrastructures integrating biometric identification, object recognition, and multi-sensor intelligence. While deep learning architectures continue to improve identification accuracy [7,10], the literature indicates that technical performance alone is insufficient once recognition systems become operational assets.

Several studies emphasize adversarial risks and the vulnerability of biometric systems to manipulation or malicious exploitation [9], motivating the integration of cybersecurity mechanisms and anomaly detection frameworks [6,12]. In particular, [9] frames biometric recognition not merely as an ML task but as an attack surface, motivating layered mitigation strategies (robust models, encryption, and multi-layer security controls) suitable for high-impact deployments.

Ethical considerations such as bias, transparency, and governance also emerge as important design constraints in high-impact security applications [7,11]. For example, [7] explicitly situates facial recognition advances within a governance and ethics context (privacy, bias, and accountability), which becomes relevant in defense where high-stakes decisions amplify societal and operational consequences.

Another emerging trend is the fusion of recognition algorithms with broader situational awareness platforms [8], where AI contributes to decision support rather than functioning as an isolated classification component. A representative implementation direction is seen in [10], which proposes a computationally efficient recognition structure deployed in a cloud setting (tree-structured deep learning), illustrating the increasing role of system architecture (edge/cloud split, service deployment) in achieving scalable recognition.

Because recognition studies rely on diverse datasets, sensing modalities, and operational contexts, reported accuracy values must be interpreted within their experimental scope rather than compared directly. Table 2 summarizes representative studies on recognition systems and highlights their role within broader security and decision-support architectures.

Table 2. Representative studies on AI-based recognition systems in defense applications, categorized by focus area, AI method, and architectural relevance.

Article Reference	Focus Area	AI Method	Relevance
Fola-Rose, Asante, et al. [7]	Facial recognition for defense	CNNs	High
Mahajan, Nitish, et al. [8]	Deep Learning-based Object Recognition	Deep Learning	High
Jalaluddin, Arooj Zafar [9]	Countermeasures to AI Malware	Biometric AI	Medium
Rahim, Asif, Yanru Zhong, and Tariq Ahmad [10]	Intelligent Face Recognition	Deep Learning	High
Rashid, Adib Bin, et al. [11]	AI in Military	Advanced Neural Networks	Medium
Zhang, Xianni, et al. [12]	Cybersecurity Enhancement	Multi-Modal AI	High

4.3 AI Integration within Advanced Optoelectronic Sensing Architectures

In optoelectronic defense applications, improvements arise not only from algorithmic innovation but also from advances in sensing modalities. Hyperspectral imaging and specialized optical platforms expand the analytical space from object detection toward material discrimination and environmental interpretation [14]. As highlighted in [14], HSI supports tasks such as subpixel target detection and material identification across wide spectral ranges (including visible to LWIR), enabling the detection of concealed or camouflaged elements that are difficult to resolve with RGB imagery alone.

Research addressing atmospheric effects and image formation demonstrates how real-world conditions fundamentally alter model behavior, motivating the use of adaptive segmentation and optimization techniques [15]. A representative example is [15], where classical segmentation limitations under noise and illumination variability motivate an AI-based optimization strategy (artificial bee colony), emphasizing robustness rather than solely improving a single benchmark score.

Strategic analyses of future warfare architectures position AI-enabled sensing as a central component of networked ISR ecosystems [13]. However, many proposed solutions remain validated primarily under controlled experimental conditions, highlighting the need for deployment-oriented evaluation frameworks that account for sensor drift, atmospheric interference, and onboard computational limitations. Table 3 presents representative works addressing AI integration within advanced optoelectronic sensing architectures.

Table 3. Representative studies on AI-integrated optoelectronic sensing architectures in defense applications.

Article Reference	Focus Area	AI Method	Relevance
Oran, Ibrahim Bora, et al. [13]	AI and Robotics in Future Wars	Robotics, AI	High
Shimoni, Michal, et al. [14]	Hyperspectral Imaging for Security	Image Processing, AI	Medium
Ruban, Igor, et al. [15]	Optoelectronic Surveillance	AI and swarm techniques	High

4.4 Performance Evaluation under Operational Constraints

Across surveillance, recognition, and optoelectronic applications, a consistent discrepancy exists between controlled experimental evaluations and operational deployment environments. Controlled studies typically rely on curated datasets and stable acquisition conditions that simplify evaluation compared to real-world deployments. Operational contexts introduce variability related to weather conditions, vibration, communication latency, domain shift, and adversarial interference.

ISR platforms and mission-oriented architectures demonstrate that performance degradation should be considered an expected characteristic of real deployments rather than an exception [23–25,30,31]. For instance, the architectures discussed in mission-network and ISR contexts frequently assume degraded connectivity or stressed infrastructure, motivating designs that explicitly address resilience (e.g., UAV-assisted mission networks [23]) and data distribution between operational real-time layers and command-and-control infrastructures [31].

Consequently, modern system design increasingly incorporates redundancy, sensor fusion, fallback strategies, and continuous monitoring mechanisms to maintain reliability under uncertain conditions. This distinction explains why numerical performance values presented in Tables 1–6 should not be interpreted as directly comparable outcomes, but rather as indicators of methodological maturity within specific operational contexts. Table 4 summarizes studies focused on performance evaluation and safety-critical aspects of AI-based defense systems.

Table 4. Representative studies on performance evaluation and safety-critical AI systems in defense applications.

Article Reference	Focus Area	AI Method	Relevance
Wang, Yue, and Sai Ho Chung [16]	AI in Safety-Critical Systems	AI, Safety-Critical Systems	High
Raquel, Delgado-Aguilera J., et al. [17]	Certification for AI Safety	AI Safety Models	High
Michel, Andy [18]	AI Explainability in Safety Systems	AI, Explainability Models	Medium
Andreoni, Martin, et al. [19]	Generative AI for Security	Generative AI	High
Esfandabadi, Mohammad Hossein, et al. [20]	Performance Optimization	Performance AI Models	Medium
Mattioli, Juliette, et al. [21]	Knowledge-Based AI Systems	Data-Driven AI	High

4.5 Reliability Challenges and Failure Mechanisms in AI-Driven Defense Systems

The literature consistently identifies three major categories of failure mechanisms affecting AI-integrated defense technologies. Environmental degradation remains a dominant challenge for optoelectronic sensing, as atmospheric distortion, occlusion, and reduced visibility significantly influence signal quality. Advanced sensing modalities such as hyperspectral imaging partially mitigate these issues but introduce increased processing complexity [14,15].

Adversarial manipulation and cyber threats emerge as systemic risks once AI becomes embedded within operational decision chains. Defensive strategies include filtering-based model hardening, explainability frameworks, and secure architecture design aimed at improving trustworthiness and resilience [6,9,12,18,28]. A representative robustness direction is [28], which hardens image classifiers using a filtering-based defense (including Gaussian filtering layers) and noise-injection during training, reflecting a practical class of mitigations that can be integrated into embedded pipelines. Complementary to model hardening, [18] targets trust and verification by proposing confidence and explainability constructs (e.g., NAC and concept-based interpretability) that are particularly relevant when systems must justify decisions under adversarial conditions.

In safety-critical and mission-critical contexts, verification and certification requirements extend beyond algorithmic performance. Research on certification frameworks and hybrid architectures shows that reliable deployment often requires functional separation between high-performance AI components and safety-critical control systems [17,21,26,27]. A concrete architectural pattern is demonstrated in [26], where a hypervisor-based separation isolates a high-performance deep learning domain (Linux) from a safety-critical control domain (FreeRTOS) on MPSoCs, illustrating how assurance can be pursued at system level even when AI components are complex. Table 5 presents representative works addressing reliability, resilience, and mission-critical AI deployment.

Table 5. Representative studies on reliability, resilience, and mission-critical AI systems in defense applications.

Article Reference	Focus Area	AI Method	Relevance
Thames, Chris, and Yifan Sun [22]	AI Approaches for Mission-Critical Systems	AI in Mission-Critical Systems	High
Kaleem, Zeeshan, et al. [23]	UAVs in Mission Networks	Generative AI	High
Van Bossuyt, Douglas L., et al. [24]	Resilience Engineering for AI Systems	AI, Resilience Engineering	Medium
Hagos, Desta Haileselassie, et al. [25]	Human-Autonomy Teaming	Hybrid AI	High
Cittadini, Edoardo, et al. [26]	Cyber-Physical Systems in Missions	Cyber-Physical AI	Medium
Linkov, Igor, et al. [27]	Interpretable Mission-Critical AI	Interpretable AI	High

4.6 System-Level Design Trade-Offs in AI-Integrated Defense Platforms

Taken together, the analyzed studies suggest that the primary impact of AI in optoelectronic defense systems lies in transforming sensing platforms into active decision-support components capable of prioritizing, filtering, and interpreting complex operational environments. However, this transformation increases system complexity and expands the potential attack surface.

In defense applications, performance cannot be reduced to a single evaluation metric. Effective solutions emerge from architectural trade-offs between latency, energy consumption, robustness to environmental variability, resilience against adversarial manipulation, and compliance with safety- or mission-critical assurance requirements [16–18,21,26,27]. The reviewed works repeatedly converge on the need for architectures that combine (i) efficient edge inference for time-critical actions, (ii) resilient networking and system-of-systems design for mission contexts [23–25], and (iii) assurance mechanisms such as certification pathways and functional isolation for safety/mission-critical integration [17,21,26,27].

By organizing the literature around architectural patterns and operational constraints, this review provides a synthesis that moves beyond model-level comparison toward a system-level understanding of AI integration in modern defense technologies. Table 6 summarizes studies highlighting system-level trade-offs and architectural design considerations in AI-integrated defense platforms.

Table 6. Representative studies supporting system-level design trade-offs in AI-integrated defense platforms.

Article Reference	Focus Area	AI Method	Relevance
Wang & Liu [28]	Robust image recognition under adversarial attacks	Multilayer filter defense + Gaussian filtering	High
Patil et al. [29]	AI-enabled defense technologies	Multi-domain AI models	High
Arya et al. [30]	UAV-based aerial sensing for border security & ISR	Multi-sensor AI fusion (IR, RGB, IoT)	Medium
Dalkıran et al. [31]	Integration of real-time image/sensor systems with C4I	DDS–JMS hybrid architecture	High
Chang et al. [32]	Optical–electronic CNN acceleration for embedded defense systems	Diffractive optical CNN layer	Medium

5. CROSS-DOMAIN GAPS AND FUTURE RESEARCH DIRECTIONS

Building upon the architectural patterns and operational limitations identified in Section 4, this section synthesizes the main cross-domain gaps emerging from the reviewed literature and outlines the most relevant future research directions for deployable AI-enabled defense systems. While AI demonstrates substantial benefits across surveillance, recognition, optoelectronic sensing, safety-critical, and mission-critical systems, the reviewed studies collectively reveal recurring challenges related to integration, operational deployment, ethical governance, and technological maturity. These gaps highlight not only technical limitations but also architectural constraints shaping future research directions in AI-driven defense systems.

5.1 Integration Challenges Across Heterogeneous Defense Architectures

The reviewed studies indicate that integrating AI into optoelectronic and multi-platform defense environments remains a complex engineering challenge. Optoelectronic systems often require precise calibration procedures to maintain performance under varying environmental conditions, which complicates seamless interaction with adaptive AI models. Differences in hardware architectures, communication protocols, and software ecosystems introduce compatibility issues that limit scalability and interoperability across platforms.

Rather than isolated algorithmic limitations, the literature suggests that integration challenges emerge primarily from system-level design constraints. Multi-domain deployments combining UAVs, ground vehicles, and distributed sensing infrastructures require unified data pipelines and standardized interfaces to enable efficient collaboration between AI modules and legacy defense technologies. The analyzed works implicitly highlight the need for interoperable middleware solutions and modular AI architectures capable of adapting to heterogeneous operational environments without extensive reconfiguration.

Across surveillance and recognition domains, convolutional neural networks remain the dominant image-processing paradigm, supporting object detection, facial recognition, and anomaly analysis. Predictive analytics and behavior modeling further extend AI functionality from passive monitoring toward proactive threat anticipation. However, the effectiveness of these solutions is often constrained by the absence of standardized integration frameworks, suggesting that future research should focus on architectural interoperability rather than solely on model performance improvements.

5.2 Ethical, Security, and Governance Constraints in Operational AI Deployment

Across the safety-critical and mission-critical literature discussed in Section 4.4 and 4.5, ethical and security considerations emerge not as abstract philosophical concerns but as practical design constraints influencing system architecture. Autonomous decision-making introduces questions of accountability, transparency, and trust, particularly in high-stakes environments where AI outputs may directly impact human safety.

The reviewed studies emphasize that AI-enabled recognition and surveillance systems increasingly become targets of adversarial manipulation and cyber intrusion. Vulnerabilities range from adversarial attacks on machine learning models to broader threats against AI-controlled infrastructure. Consequently, ethical deployment is closely linked to cybersecurity resilience, explainability, and governance frameworks rather than isolated policy discussions.

Robust solutions identified in the literature include deep learning-based recognition pipelines combined with cybersecurity safeguards and reliability mechanisms designed for high-security environments. Techniques such as anomaly detection, explainable AI models, and multi-layered security architectures demonstrate how ethical considerations translate into concrete technical requirements. These findings suggest that future research must prioritize trustworthy AI frameworks that integrate transparency, fairness, and operational resilience as core system properties rather than optional add-ons.

5.3 Real-World Validation and Operational Performance Gaps

A consistent observation across the analyzed studies is the discrepancy between controlled experimental validation and real-world deployment conditions. While many AI-driven defense solutions achieve high performance under curated datasets and laboratory settings, operational environments introduce unpredictable variables such as extreme weather, sensor degradation, communication latency, and domain shift.

The literature highlights that most AI-enabled surveillance, recognition, and optoelectronic systems remain primarily validated in simulated or controlled contexts. This gap limits the ability to assess long-term robustness and scalability in realistic defense scenarios. Instead of viewing real-world testing as a final validation stage, the reviewed works suggest that operational feedback loops should become an integral component of system development cycles.

Within optoelectronic systems specifically, AI-driven signal enhancement and automated target tracking emerge as recurrent approaches that transform raw sensor data into actionable intelligence. Techniques involving noise reduction, adaptive filtering, and AI-assisted tracking demonstrate how advanced image-processing pipelines enhance situational awareness. However, their effectiveness depends heavily on environmental variability, emphasizing the need for field trials and deployment-oriented evaluation frameworks capable of capturing operational complexity.

5.4 Emerging AI Methodologies and Technological Evolution

The analyzed studies indicate that emerging AI methodologies, particularly reinforcement learning and generative models, represent a transition from static perception toward adaptive decision-making architectures. Reinforcement learning enables autonomous systems to optimize actions based on dynamic environmental feedback, supporting mission-critical applications that require continuous adaptation.

Generative adversarial networks and synthetic data generation techniques offer promising approaches for addressing data scarcity and improving robustness in recognition and surveillance tasks. By augmenting training datasets and simulating complex operational scenarios, these techniques may enhance the generalization capabilities of AI models deployed in defense environments.

Despite their potential, the integration of advanced AI methods remains largely experimental within defense applications. Current research emphasizes hybrid architectures combining traditional deep learning with adaptive or generative components to balance performance with reliability. Across the literature, convolutional neural networks continue to dominate image-processing workflows, but emerging techniques suggest a gradual shift toward more flexible and context-aware AI systems capable of operating under uncertain and adversarial conditions.

5.5 Synthesis of Cross-Domain Research Insights

A synthesis of the analyzed literature reveals several recurring technological patterns shaping AI-driven defense systems. Deep learning architectures, particularly CNN-based models, remain the most widely adopted solutions for image processing, object detection, and recognition across surveillance and optoelectronic applications. Their dominance reflects both technological maturity and adaptability to diverse sensing modalities.

In parallel, predictive analytics and anomaly detection frameworks extend AI functionality beyond perception, enabling systems to anticipate potential threats and enhance situational awareness. Within optoelectronic sensing, AI-driven signal processing techniques improve data clarity, target tracking, and decision-making speed, demonstrating how sensor intelligence evolves from passive observation toward active interpretation.

Across safety-critical and mission-critical domains, hybrid architectures integrating reliability mechanisms, redundancy strategies, and explainable AI components emerge as key enablers of trustworthy deployment. These cross-domain findings reinforce the notion that effective AI integration in defense systems depends less on individual algorithmic breakthroughs and more on the architectural design of resilient, interoperable, and operationally validated systems.

6. DISCUSSION

The integration of artificial intelligence (AI) into defense technologies has accelerated the evolution of surveillance, recognition, optoelectronic sensing, and safety- and mission-critical infrastructures. Building upon the architectural patterns and operational limitations identified in Sections 4 and 5, this review highlights several cross-domain trends that extend beyond individual algorithmic improvements. Rather than representing isolated technological advances, AI adoption in defense reflects a systemic shift toward distributed sensing, adaptive decision-support architectures, and resilience-oriented system design. These findings indicate that the impact of AI lies not only in improving performance metrics but also in reshaping how defense platforms process, prioritize, and interpret operational data.

Across surveillance applications, the analyzed literature demonstrates a transition from standalone detection algorithms toward integrated pipelines that combine real-time perception, behavioral analysis, and automated alert generation. AI-enabled surveillance systems increasingly operate at the edge, enabling faster response times and improved situational awareness under operational constraints. Studies such as those by (Iqbal et al., 2021; Shahnoor et al., 2022) illustrate how deep learning models support autonomous threat recognition, but the broader insight emerging from this review is that system performance depends more on architectural integration, communication reliability, and hardware optimization than on marginal differences between neural network models. This shift reflects a movement toward scalable surveillance ecosystems capable of operating in complex and resource-constrained environments.

Recognition systems show a similar evolution. While deep learning has significantly improved facial and object recognition accuracy, the reviewed studies suggest that performance alone is insufficient in operational defense contexts. Research by (Fola-Rose et al., 2024; Mahajan et al., 2024) highlights the growing role of AI in rapid identification and decision support, yet the synthesis presented in this review reveals a broader trend toward integrating recognition modules within multi-sensor intelligence frameworks. As adversarial strategies evolve, recognition systems increasingly require resilience against manipulation, domain shifts, and adversarial interference. Consequently, future progress depends not only on improving classification accuracy but also on enhancing robustness, transparency, and cybersecurity integration.

The integration of AI within optoelectronic systems further illustrates the importance of sensor-driven innovation. Studies by (Ruban et al., 2018; Oran et al., 2023) demonstrate how AI-assisted signal processing enhances performance in low-light and high-noise environments, supporting surveillance and reconnaissance missions that rely on precise imaging and targeting. However, a cross-domain observation emerging from this review is that improvements in sensing modalities often redefine the analytical problem itself, shifting the focus from simple object detection toward material discrimination, environmental interpretation, and adaptive data filtering. These developments highlight the growing role of optoelectronic intelligence as an active component within AI-driven defense architectures.

In safety-critical and mission-critical systems, AI introduces both opportunities and structural challenges. Research by (Wang et al., 2022; Andreoni et al., 2024) illustrates how anomaly detection, redundancy mechanisms, and adaptive learning strategies enhance system resilience in high-stakes environments. Nevertheless, the analyzed literature consistently emphasizes that reliability in defense applications depends on hybrid architectures that combine data-driven AI with deterministic control mechanisms. The need for certification frameworks, explainable AI methods, and rigorous testing protocols emerges as a recurring theme, reflecting the tension between innovation and operational assurance in safety-critical deployments.

Image recognition remains a foundational capability across modern defense systems, enabling autonomous targeting, threat detection, and battlefield awareness. Studies such as (Thames and Sun, 2024; Kaleem et al., 2024) demonstrate the increasing speed and scalability of AI-driven visual processing pipelines. However, the broader synthesis presented here indicates that performance improvements must be evaluated within operational contexts characterized by environmental variability, sensor noise, and evolving adversarial tactics. As a result, future research must focus on adaptive architectures capable of maintaining reliability under uncertain and dynamic conditions rather than solely pursuing incremental gains in accuracy.

Despite the substantial progress highlighted across these domains, this review identifies several persistent gaps shaping future research directions. Integration challenges remain a dominant barrier, particularly in multi-platform defense ecosystems where interoperability and standardized protocols are limited. Ethical and security considerations increasingly function as architectural constraints, influencing system design through requirements related to transparency, accountability, and cyber resilience. Furthermore, the lack of real-world testing continues to restrict the operational maturity of many AI-driven defense technologies, emphasizing the importance of deployment-oriented validation frameworks capable of capturing environmental variability and long-term system behavior.

Looking ahead, emerging AI methodologies—including reinforcement learning, generative adversarial networks, and adaptive multi-modal architectures—are expected to drive the next phase of technological evolution. These approaches enable autonomous systems to learn from dynamic environments and generate synthetic training data, improving robustness in data-scarce scenarios. However, as highlighted by recent strategic analyses (Patil et al., 2024; De Spiegeleire et al., 2017; Ahn et al., 2020; Choi, 2021), advances in AI capabilities are likely to be accompanied by increasingly sophisticated adversarial countermeasures. Consequently, future research must prioritize resilience, adaptability, and secure system design to ensure that AI remains a reliable asset within defense applications.

7. CONCLUSIONS

This review has several limitations. First, the study is qualitative and synthesis-oriented rather than meta-analytic, which means that reported performance metrics were not statistically aggregated across papers. Second, the included studies are heterogeneous in terms of sensing modalities, datasets, experimental protocols, and deployment scenarios, which limits direct cross-study comparability. Third, although the review followed an adapted PRISMA-like selection logic, the final corpus of 32 primary studies reflects relevance to architectural and operational interpretation rather than exhaustive coverage of all AI-related defense literature. Finally, some included sources represent broader system-level perspectives that support the understanding of deployment constraints even when they are not focused exclusively on EO/IR sensing.

In conclusion, this state-of-the-art review demonstrates that AI's transformative impact across surveillance, recognition, optoelectronic, safety-critical, and image recognition systems extends beyond individual technological improvements toward a broader architectural evolution of defense platforms. While significant advancements have been achieved, challenges related to interoperability, ethical governance, operational validation, and system resilience continue to shape the trajectory of AI integration (Feldstein, 2019; Ulaşan, 2023). Addressing these issues will require coordinated collaboration among researchers, industry stakeholders, and policymakers to ensure responsible deployment and sustained innovation. The future of AI in defense lies not only in developing more powerful algorithms but in designing integrated, trustworthy systems capable of operating effectively within complex and unpredictable operational environments.

REFERENCES

Abba, S., et al., 2024. Real-time object detection, tracking, and monitoring framework for security surveillance systems. *Heliyon*, 10(15).

Ahn, J.-W., et al., 2020. An Empirical Study on Defense Future Technology in Artificial Intelligence. *Journal of the Korea Academia-Industrial Cooperation Society*, 21(5), pp.409-416.

Andreoni, M., et al., 2024. Enhancing autonomous system security and resilience with generative AI: A comprehensive survey. *IEEE Access*.

Arya, L., et al., 2023. Eyes in the Sky: Safeguarding Borders Security with AI-Powered Aerial Monitoring and IoT Integration. In: The International Conference on Recent Innovations in Computing. Singapore: *Springer Nature Singapore.*

Board, Defense Innovation, 2019. AI principles: recommendations on the ethical use of artificial intelligence by the department of defense: supporting document. *United States Department of Defense.*

Chang, J., et al., 2018. Hybrid optical-electronic convolutional neural networks with optimized diffractive optics for image classification. *Scientific Reports*, 8(1), pp.1-10.

Choi, J., 2021. Current and future considerations for the use of artificial intelligence by the United States' Department of Defense. *Robotics & AI Ethics*, 6(1), pp.1-6.

Cittadini, E., et al., 2023. Supporting AI-powered real-time cyber-physical systems on heterogeneous platforms via hypervisor technology. *Real-Time Systems*, 59(4), pp.609-635.

Dalkıran, E., et al., 2021. Automated integration of real-time and non-real-time defense systems. *Defence Technology,* 17(2), pp.657-670.

De Spiegeleire, S., Maas, M. and Sweijs, T., 2017. Artificial intelligence and the future of defense: Strategic implications for small-and medium-sized force providers. *The Hague Centre for Strategic Studies*.

Esfandabadi, M.H.M., Esmaeili, A. and Karbasishargh, K., 2024. Optimizing performance through retrofitting: strategies for effectiveness, defence, and resiliency to enhance safety and reliability. *International Journal of Reliability, Risk and Safety: Theory and Application*, 7(1), pp.83-92.

Feldstein, S., 2019. The global expansion of AI surveillance. *Washington, DC: Carnegie Endowment for International Peace*, 17(9).

Fola-Rose, A., et al., 2024. A Systematic Review of Facial Recognition Methods: Advancements, Applications, and Ethical Dilemmas. *2024 IEEE International Conference on Information Reuse and Integration for Data Science* (IRI). IEEE.

Hagos, D.H., El Alami, H. and Rawat, D.B., 2024. AI-Driven Human-Autonomy Teaming in Tactical Operations: Proposed Framework, *Challenges, and Future Directions.* arXiv preprint arXiv:2411.09788.

Huyen, N.T.M. and Bao, T.Q., 2024. Advancements in AI-Driven Cybersecurity and Comprehensive Threat Detection and Response. *Journal of Intelligent Connectivity and Emerging Technologies*, 9(1), pp.1-12.

Iqbal, M.J., et al., 2021. Real-Time Surveillance Using Deep Learning. *Security and Communication Networks*, 2021(1), p.6184756.

Jalaluddin, A.Z., 2020. An Exploration of Countermeasures to Defend Against Weaponized AI Malware Exploiting Facial Recognition. *Capitol Technology University*.

Kaleem, Z., et al., 2024. Emerging trends in UAVs: From placement, semantic communications to generative AI for mission-critical networks. *IEEE Transactions on Consumer Electronics*.

Khlaaf, H., West, S.M. and Whittaker, M., 2024. Mind the Gap: Foundation Models and the Covert Proliferation of Military Intelligence, *Surveillance, and Targeting*. arXiv preprint arXiv:2410.14831.

Lan, J., et al., 2022. Adversarial attacks and defenses in speaker recognition systems: A survey. *Journal of Systems Architecture*, 127, p.102526.

Linkov, I., et al., 2023. Toward Mission-Critical AI: Interpretable, Actionable, and Resilient AI. 2023 15th *International Conference on Cyber Conflict: Meeting Reality* (CyCon). IEEE.

Liu, Z.-Y., et al., 2020. Defense against n-pixel attacks based on image reconstruction. *Proceedings of the 8th International Workshop on Security in Blockchain and Cloud Computing.*

Mahajan, N., Chauhan, A. and Kajal, M., 2024. An Introduction to Deep Learning-Based Object Recognition and Tracking for Enabling Defense Applications. *Advances in Aerial Sensing and Imaging*, pp.109-127.

Margulies, P., 2016. Surveillance by algorithm: The NSA, computerized intelligence collection, and human rights. *Florida Law Review*, 68, pp.1045.

Matthew, U.O., et al., 2021. Artificial intelligence autonomous unmanned aerial vehicle (UAV) system for remote sensing in security surveillance. 2020 *IEEE 2nd International Conference on Cyberspace* (CYBER NIGERIA). IEEE.

Mattioli, J., et al., 2022. Combining Data-Driven and Knowledge-Based AI Paradigms for Engineering AI-Based Safety-Critical Systems. *Workshop on Artificial Intelligence Safety* (SafeAI).

Maung, M., Pyone, A. and Kiya, H., 2020. Encryption inspired adversarial defense for visual classification. 2020 *IEEE International Conference on Image Processing* (ICIP). IEEE.

Michel, A., 2021. Towards Enabling Explanation in Safety-Critical Artificial Intelligence Systems.

Nyakundi, N.B.N. and Reza, H., 2024. Development of an effective safety assessment capable of measuring the safety of AI-based systems. *2024 IEEE International Conference on Electro Information Technology (eIT)*. IEEE.

Oran, I.B., et al., 2023. Technology, artificial intelligence, and robotics in future wars. *Journal of Organizational Behavior Research.*

Patil, A.T., Vidhale, B. and Titarmare, A., 2024. Strategic innovations in defense systems: a comprehensive analysis of emerging technologies and future trends. 2024 *International Conference on Intelligent Systems for Cybersecurity* (ISCS). IEEE.

Rahim, A., Zhong, Y. and Ahmad, T., 2022. A deep learning-based intelligent face recognition method in the Internet of Home things for security applications. *Journal of Hunan University Natural Sciences*, 49(10).

Raquel, D.-A.J., et al., 2024. Establishing rigorous Certification Standards: A systematic methodology for AI safety-critical systems in military aviation. *IEEE Access.*

Rashid, A.B., et al., 2023. Artificial intelligence in the military: An overview of the capabilities, applications, and challenges. *International Journal of Intelligent Systems,* 2023(1), p.8676366.

Rawat, R., et al., 2021. Surveillance robot in cyber intelligence for vulnerability detection. *In: Machine Learning for Robotics Applications,* pp.107-123.

Ruban, I., et al., 2018. A swarm method for segmentation of images obtained from on-board optoelectronic surveillance systems. 2018 *International Scientific-Practical Conference Problems of Infocommunications. Science and Technology* (PIC S&T). IEEE.

Sebastião, F.P., 2023. The Role of a Microservice Architecture on Cybersecurity and Operational Resilience in Critical Systems. *Dissertation*.

Shabbir, A., et al., 2024. Analyzing surveillance videos in real-time using AI-powered deep learning techniques. *International Journal on Recent and Innovation Trends in Computing and Communication*, 12(2), pp.950-960.

Shahnoor, S.F., et al., 2022. AI-driven Real-time System for Land Surveillance and Reconnaissance. *Proceedings of the 2022 Fourteenth International Conference on Contemporary Computing.*

Shimoni, M., Haelterman, R. and Perneel, C., 2019. Hyperspectral imaging for military and security applications: Combining myriad processing and sensing techniques. *IEEE Geoscience and Remote Sensing Magazine,* 7(2), pp.101-117.

Silva, H., Vieira, M. and Neto, A., 2023. Are safety-critical systems really survivable to attacks?. *2023 IEEE International Systems Conference (SysCon)*. IEEE.

Thames, C. and Sun, Y., 2024. A Survey of Artificial Intelligence Approaches to Safety and Mission-Critical Systems. 2024 *Integrated Communications, Navigation and Surveillance Conference* (ICNS). IEEE.

Tyugu, E., 2011. Artificial intelligence in cyber defense. 2011 *3rd International Conference on Cyber Conflict*. IEEE.

Ulaşan, F., 2023. The use of artificial intelligence in the defense system within the framework of the policy making cycle: The case of the United States. *Uluslararası Toplumsal Bilimler Dergisi,* 7(3), pp.517-535.

Van Bossuyt, D.L., et al., 2022. Model based resilience engineering for design and assessment of mission critical systems containing artificial intelligence components. In: *Artificial Intelligence and Cybersecurity: Theory and Applications. Cham: Springer International Publishing*, pp.47-66.

Vashishth, T.K., et al., 2024. Enhancing Surveillance Systems through Mathematical Models and Artificial Intelligence: An Image Processing Approach. *Mathematical Models Using Artificial Intelligence for Surveillance Systems*, pp.91-120.

Vegesna, V.V., 2023. Comprehensive analysis of AI-enhanced defense systems in cyberspace. International Numeric *Journal of Machine Learning and Robots*, 7(7).

Wang, M. and Liu, Z., 2024. Defense against Adversarial Attacks in Image Recognition Based on Multilayer Filters. *Applied Sciences*, 14(18), p.8119.

Wang, Y. and Chung, S.H., 2022. Artificial intelligence in safety-critical systems: a systematic review. *Industrial Management & Data Systems*, 122(2), pp.442-470.

Wiesenthal, M., 2022. The ethical implications of AI-based mass surveillance tools. *MS thesis*.

Zhang, X., et al., 2024. AI-Powered Cybersecurity: Enhancing Threat Detection and Defense in the Digital Age. 2024 *IEEE 7th International Conference on Electronic Information and Communication Technology* (ICEICT). IEEE.