AMERICAN JOURNAL OF ICT AND INNOVATION (AJICTI)

VOLUME 1 ISSUE 1 (2026)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of ICT and Innovation (AJICTI)
Volume 1 Issue 1, Year 2026
https://journals.e-palli.com/home/index.php/ajicti

Cyber Threat Analysis of Drone Detection and Early Warning Systems

Adala Sewdi Sdiq Surchi [1*]

Article Information

Received: November 14, 2025
Accepted: February 12, 2026
Published: March 19, 2026

Keywords
Cybersecurity, Drone Detection, Early Warning Systems, Sensor Fusion, Spoofing

ABSTRACT

The rapid proliferation of Unmanned Aerial Systems across commercial, civilian, and military domains has elevated drone detection and early warning systems to a position of critical infrastructure for airspace protection. However, the cybersecurity dimensions of these detection architectures remain insufficiently characterized in the literature, with most prior work treating the sensor network as a trusted substrate rather than as a potential adversarial target. This paper conducts a structured systematic review of the cyber threat landscape confronting drone detection and early warning systems, synthesizing findings from the peer-reviewed primary-source corpus identified through the review process. The review applies a four-phase analytical pipeline comprising corpus assembly, threat-surface decomposition, cross-layer mapping using the STRIDE threat model, and defensive posture evaluation. Detection technologies are taxonomized according to the five-modality framework—acoustic, vision, passive radio frequency, active radar, and data fusion—and their respective vulnerabilities are mapped against the confidentiality, integrity, and availability pillars. Cyber threat primitives including spoofing, jamming, denial-of-service, hijacking, and malware injection are evaluated with respect to detection-infrastructure integrity. Results demonstrate that data fusion architectures, while operationally necessary, simultaneously expand the attack surface through insecure coordination channels, calibration-weight exchange, and time-synchronization dependencies. The integrity dimension—particularly GPS, ADS-B, and transponder spoofing—emerges as the dominant underserved attack vector. The study concludes that detection cybersecurity must be treated as coupled with detection engineering rather than separable from it, and identifies authenticated data fusion, spoofing-resilient localization, unified cyber-physical evaluation frameworks, blockchain-assisted coordination, and quantum-resistant cryptographic protocols as priority directions for future research.

INTRODUCTION

The rapid proliferation of Unmanned Aerial Systems necessitates robust early warning architectures to safeguard critical infrastructure against increasingly sophisticated aerial incursions (Lykou *et al.*, 2020). This research defines the scope of detection cybersecurity by examining vulnerabilities in communication links, sensor fusion, and transponder-based tracking protocols (Adel *et al.*, 2024). Maintaining the integrity of these early warning systems is paramount, as any compromise in detection accuracy directly imperils public safety and mission success (Shafik *et al.*, 2023; Yu *et al.*, 2025). To delineate the critical boundaries of this problem, this analysis addresses the following research questions: How do vulnerabilities in wireless communication protocols and navigation subsystems facilitate adversarial spoofing or jamming of detection sensors (Morshedi & Matinkhah, 2025; Park *et al.*, 2021)? Furthermore, to what extent can signal injection or data manipulation attacks compromise the algorithmic integrity of automated classification engines, and what architectural defenses can effectively mitigate these multi-vector threats (Oli & Mahalal, 2025; Wang *et al.*, 2021)? By critically evaluating the convergence of radar, radio frequency analysis, and communication-based surveillance, this study identifies specific gaps in current detection frameworks exploited by malicious actors (Khawaja *et al.*, 2025).

LITERATURE REVIEW

Detection-Modality Taxonomies

The foundational work in this stream is Wang et al.'s survey of counter-UAS detection technologies, which proposes a five-modality taxonomy—acoustic, vision, passive radio frequency, active radar, and data fusion—and provides the most-cited comparative evaluation of detection range, accuracy, and operational constraints across modalities (Wang *et al.*, 2021). Park, Kim, Lee, and colleagues complement this taxonomy by disaggregating the problem into detection, identification, and neutralization sub-systems, and observe that military-grade detection solutions remain prohibitively expensive for private and public facilities (Park *et al.*, 2021). Khawaja, Ezuma, Semkin, and colleagues extend the coverage specifically to radar and communications-based detection, characterizing the problem of detecting autonomous aerial vehicles as substantively more difficult than the analogous problem for manned aviation because of smaller radar cross-sections, low-altitude flight profiles, and heterogeneous platform geometries (Khawaja *et al.*, 2025). Collectively, these surveys establish that data fusion

[1] Department of Information System, School of Science and Engineering, University of Kurdistan Hewlêr (UKH), Erbil, Kurdistan Region, Iraq
[*] Corresponding author's email: adalasurchi@gmail.com

is the dominant recommended paradigm for reliable long-range, all-weather detection, even though no single fused modality is robust under variable environmental conditions (Wang *et al.*, 2021).

UAV Cybersecurity Threat Models

The complementary body of literature foregrounds the cybersecurity dimension. Shafik, Matinkhah, and Shokoor apply the STRIDE threat modeling framework to characterize the attack surface of UAVs, distinguishing threats that target communication links, control channels, and onboard data stores (Shafik *et al.*, 2023). Their review observes that most existing studies privilege an "intruder portrait" methodology that captures neither the social nor the human-factor dimensions of the threat (Shafik *et al.*, 2023). Morshedi and Matinkhah extend this perspective with a unified taxonomy that classifies spoofing, jamming, denial-of-service, hijacking, and malware injection primitives along the confidentiality–integrity–availability triad, and catalogue cryptographic, intrusion-detection, and machine-learning-based countermeasures, weighed against the resource constraints inherent to UAV platforms (Morshedi & Matinkhah, 2025). Mityagin, Kolotylo, Hashim, and colleagues situate the cyber problem within electronic warfare specifically, enumerating attacks on Automatic Dependent Surveillance–Broadcast (ADS-B), the Traffic Alert and Collision Avoidance System (TCAS), and command-and-control coordination channels that bear directly on cooperative surveillance (Yu *et al.*, 2025). Adel, Saleiham, Thompson-Whiteside, and colleagues present simulated attack scenarios on drones following the full hacking cycle, illustrating how vulnerabilities in consumer smart devices propagate into airborne platforms (Adel *et al.*, 2024). Oli and Mahalal consolidate this landscape in a recent survey, cataloguing available datasets, tools, and testbeds to support benchmarking (Oli & Mahalal, 2025).

Domain-Specific Studies

A smaller but operationally important stream focuses on specific deployment domains. Lykou, Moustakas, and Gritzalis concentrate on the airport setting, cataloguing drone incidents near aerodrome facilities and evaluating the limitations of counter-drone sensing in regulated airspace (Lykou *et al.*, 2020). Their study establishes that defending airports from misused drone activity is uniquely difficult because regulatory restrictions on kinetic mitigation concentrate the operational burden on the detection layer (Lykou *et al.*, 2020). This domain-specific insight informs the present review's emphasis on the detection architecture as the principal cyber-defensive surface.

Identified Gaps

Three gaps recur across the surveyed literature. First, detection–cybersecurity convergence is acknowledged as important but is rarely addressed jointly within a single study; the two literatures cite each other sparingly. Second, the integrity dimension is consistently singled out as the most underserved threat vector across both detection and UAV-cybersecurity reviews (Morshedi & Matinkhah, 2025; Oli & Mahalal, 2025; Yu *et al.*, 2025), yet few studies recommend concrete countermeasures. Third, the absence of reproducible evaluation frameworks means that defensive claims are difficult to validate across research groups (Oli & Mahalal, 2025). The present study is structured to address each of these gaps through an explicit cross-layer methodological pipeline.

MATERIALS AND METHODS

This study adopts a structured systematic review methodology consistent with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses framework. The methodology is articulated in five sequential phases: data retrieval, application of inclusion and exclusion criteria, study selection, data extraction, and data analysis.

The literature search was conducted across four primary databases—IEEE Xplore, Scopus, Web of Science, and the ACM Digital Library—covering publications from January 2020 to December 2025. The principal search string, applied to title, abstract, and keyword fields, was:

("drone detection" OR "UAV detection" OR "counter-UAS" OR "anti-drone") AND ("cybersecurity" OR "cyber attack" OR "spoofing" OR "jamming" OR "sensor security" OR "threat model")

Auxiliary queries were formulated to surface literature from adjacent domains, including:

("early warning system" OR "airspace surveillance" OR "ADS-B security") AND ("unmanned aerial vehicle" OR "UAV" OR "drone")

("sensor fusion" OR "data fusion") AND ("counter-UAS" OR "drone detection") AND ("integrity" OR "adversarial")

("STRIDE" OR "attack surface") AND ("UAV" OR "unmanned aerial vehicle") AND ("survey" OR "review")

Backward and forward snowballing was subsequently performed on the included articles to identify additional sources missed by the database search.

Sources were evaluated against the following inclusion criteria: (i) peer-reviewed publication in a recognized journal, conference proceedings, or recognized preprint server between 2020 and 2025; (ii) explicit treatment of either a detection modality with cybersecurity implications, or a cyber-attack vector with documented effects on detection infrastructure; (iii) provision of methodological detail sufficient for replication or comparative analysis; and (iv) availability of full text in English.

Sources were excluded if they: (i) focused exclusively on neutralization mechanisms (e.g., jamming, kinetic effectors) without engaging detection cybersecurity; (ii) addressed general aviation security without specific reference to UAS or anti-UAS detection; (iii) presented purely anecdotal or speculative threat claims without technical substantiation; or (iv) duplicated content already represented by an earlier or more comprehensive version

of the same work.

Study Selection

The selection process is documented in the PRISMA flow diagram below, which records the number of records identified, screened, assessed for eligibility, and ultimately included in the qualitative synthesis. The selection process is summarized in Table 1 and illustrated in Figure 1.

Table 1: Study-selection flow summarized from the manuscript's PRISMA-style screening process.

Selection stage	Records (n)	Description
Identification	≈142	Records identified through database searching
Duplicate removal	≈34	Records removed as duplicates
Screening	108	Unique records screened by title and abstract
Title/abstract exclusion	78	Records excluded for not meeting inclusion criteria
Eligibility	30	Full-text articles assessed
Full-text exclusion	20	Articles excluded for stated scope or methodological reasons
Qualitative synthesis	10	Studies retained for qualitative synthesis and thematic analysis

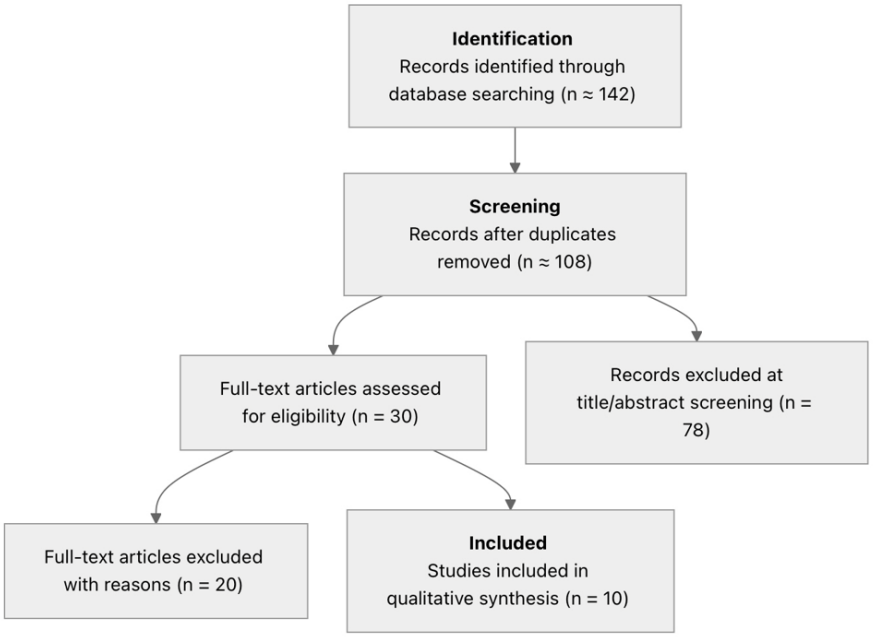

Figure 1: PRISMA-style flow diagram of the study selection process.

Data Extraction

A standardized data-extraction form was applied to each included study, capturing: (i) bibliographic metadata (authors, year of publication, and venue); (ii) detection modality or modalities under consideration; (iii) cyber threat model or threat catalogue employed; (iv) reported vulnerabilities or attack vectors; (v) countermeasures or defensive recommendations proposed; and (vi) identified limitations or open research questions. Extraction was performed once per source, with claim-to-source cross-validation completed before each datum was admitted to the analysis.

Data Analysis

The extracted data were analyzed through a four-stage pipeline. In the first stage, detection modalities were catalogued according to the five-modality taxonomy of Wang *et al.* (2021). In the second stage, the characteristic vulnerabilities of each modality were articulated. In the third stage, the STRIDE threat model of Shafik *et al.* (Shafik *et al.*, 2023) was overlaid to produce a cross-layer map of the attack surface, and the threat catalogue of Morshedi and Matinkhah (2025) was used to populate the integrity, availability, and confidentiality dimensions.

In the fourth stage, defensive countermeasures were evaluated against the four criteria of effectiveness, scalability, resource consumption, and suitability for UAV-specific operational constraints previously articulated by Morshedi and Matinkhah (2025). This pipeline yields a reproducible synthesis that can be re-executed as new literature enters the field, and that couples detection-modality characteristics to cyber-attack primitives rather than treating the two as separate problem domains.

Synthesis Logic and Quality Considerations

The synthesis was designed to preserve the distinction between evidence reported by the reviewed studies and analytical conclusions derived from comparing those studies. The reviewed literature is heterogeneous: some papers are broad surveys of counter-UAS technologies, some focus on UAV cybersecurity, some examine electronic warfare, and one concentrates on the airport environment. Consequently, the review does not treat every reported observation as an experimentally comparable measurement. Instead, the studies are used to identify recurring technical relationships between detection modality, attack surface, threat consequence, and defensive requirement. This approach is consistent with the purpose of a structured review in a field where the same cyber primitive can affect different layers of a detection architecture in different ways.

A second quality consideration concerns the distinction between the UAV as a protected platform and the detection system as protected infrastructure. Shafik *et al.* (2023) and Morshedi and Matinkhah (2025) primarily organize threats around the UAV, its communications, and its control functions. Wang *et al.* (2021) and Park *et al.* (2021), by contrast, emphasize sensing, identification, tracking, and counter-UAS architecture. The present synthesis connects these perspectives by asking what happens when an attack that is normally described as an attack on the aircraft instead becomes a misleading input to the detection network. This distinction is particularly important for spoofing because the attacker does not necessarily need to disable a sensor; altering the information received by the sensor may be sufficient to change the system's decision.

A third consideration is reproducibility. The PRISMA-style selection process records the transition from the initial database search to the final qualitative synthesis, while the extraction and analysis stages use the same categories across the included literature. This makes the logic of the synthesis explicit even though the underlying studies use different experimental settings and evaluation criteria. The absence of a common benchmark remains a limitation identified in the source literature, and therefore the conclusions of this review are presented as cross-study analytical findings rather than as a pooled statistical effect.

RESULTS AND DISCUSSION

Detection Modality Inventory and Vulnerabilities

The five-modality taxonomy proposed by Wang *et al.* (2021) yields differential cyber-risk profiles that are largely orthogonal to the classical performance trade-offs reported in the literature. Acoustic sensors offer low cost and light weight but are vulnerable to environmental masking by wind and vibration, and their effective range remains constrained; critically, they lacks identification capacity capacity, which means that an attacker using a recorded acoustic signature could plausibly induce false positives without physical presence (Wang *et al.*, 2021). Vision sensors are constrained by illumination and computational demand, and their limited range weakens the integrity of long-range early-warning decisions (Wang *et al.*, 2021). Passive RF detection offers long range and identification, but is blind to encrypted protocols and easily confused with other ISM-band devices—properties that an adversary can deliberately exploit to mask command-and-control emissions within legitimate Wi-Fi or Bluetooth spectrum (Wang *et al.*, 2021). Active radar provides long range and high precision but is expensive, power-hungry, and lacks identification; importantly, the micro-Doppler signatures upon which it depends can be degraded by specially shaped propeller geometries (Wang *et al.*, 2021). Passive radar offers long range and low cost but lacks identification and is easy to interfere with (Wang *et al.*, 2021).

Data Fusion as an Attack Multiplier

Data fusion is consistently identified as the most popular and most reliable detection paradigm (Wang *et al.*, 2021), yet the heterogeneous sensor combinations it requires introduce a new class of integrity risk. The fusion of acoustic and radar modalities yields superior detection precision (Wang *et al.*, 2021), but the calibration weights assigned to each sensor stream constitute a high-value adversarial target: a sensor-weight manipulation attack could degrade the reliability of the entire system without compromising any constituent sensor. Multi-sensor fusion of distributed acoustic arrays enables time-difference-of-arrival localization (Wang *et al.*, 2021), but the synchronization channel used to coordinate these arrays constitutes an additional attack surface that has received limited attention in the literature. Multiple-type sensor fusion is recommended precisely because no single modality is robust under variable environmental conditions (Wang *et al.*, 2021), and the burden of secure coordinate transformation among heterogeneous sensor types accordingly falls on the fusion controller (Wang *et al.*, 2021).

Cyber Threat Catalogue

The threat catalogue identified by Morshedi and Matinkhah (2025) enumerates spoofing, jamming, denial-of-service, hijacking, and malware injection as the dominant primitives. Within the detection context, each primitive maps to a concrete failure mode: spoofing compromises the int egrity of GPS-derived localization used to cue sensors (Yu *et al.*, 2025); jamming compromises the availability of cooperative surveillance channels and Automatic Dependent Surveillance–Broadcast (ADS-B)

broadcasts (Yu *et al.*, 2025); denial-of-service exhausts the edge computational resources required by vision-based detection; hijacking seizes control of the very UAV whose behaviour a sensor network is attempting to track (Shafik *et al.*, 2023); and malware injection can subvert the classification engine that performs automated threat determination.

Airport-Specific and Civilian Failure Modes

For airport deployments, the literature documents that drone incidents near airport facilities are expected to proliferate in frequency, complexity, and severity as drones grow larger and more capable (Lykou *et al.*, 2020). Defending airports from misused drone activity is characterized as a hard problem precisely because the regulatory environment constrains kinetic mitigation and pushes the operational burden onto detection (Lykou *et al.*, 2020). Adel *et al.* document realistic attack scenarios in which consumer smart devices are leveraged as pivots into UAV control channels, demonstrating that even non-military adversaries can mount multi-stage attacks against airborne platforms (Adel *et al.*, 2024).

Defensive Posture Evaluation

Current defenses are evaluated against four criteria: effectiveness, scalability, resource consumption, and suitability for UAV operational constraints (Morshedi & Matinkhah, 2025). Yu *et al.* catalogue countermeasures for ADS-B attacks, TCAS-induced collisions, and dispatch system compromise, providing the most operationally concrete defensive set in the surveyed literature (Yu *et al.*, 2025). Nevertheless, the consensus—articulated explicitly by Oli and Mahalal—is that recurring gaps remain in the current threat coverage, justifying an explicit forward-looking research agenda (Oli & Mahalal, 2025).

Comparative Detection-Modality Risk Analysis

The five detection modalities provide complementary capabilities, but their cybersecurity exposure is not uniform. Acoustic detection is attractive because of its low cost and light weight, yet its environmental limitations and lack of identification capacity make the interpretation of an acoustic event dependent on contextual information. Vision-based detection adds classification capability but introduces computational and environmental dependencies. Passive RF detection can support long-range identification, while its dependence on observable radio emissions creates a different set of assumptions about what an adversary can conceal. Active radar supplies long-range and high-precision information, but its cost, power requirements, and lack of direct identification create additional operational constraints. Passive radar provides another long-range option but remains susceptible to interference. These observations indicate that cybersecurity cannot be evaluated independently from the engineering assumptions of each modality.

Table 2 organizes these relationships into a modality-level risk matrix. The table does not assign numerical risk scores because the reviewed studies do not provide a common quantitative scale. Instead, it records the capability and vulnerability characteristics that recur in the literature. This qualitative representation is more faithful to the available evidence and makes clear why the fusion of multiple modalities is attractive: weaknesses in one modality can be compensated for by information from another. At the same time, fusion creates a dependency on the integrity of the information exchange between

Table 2: Qualitative comparison of detection modalities and cybersecurity implications derived from the reviewed literature.

Detection modality	Primary capability	Key vulnerability/ constraint	Security implication
Acoustic	Low cost; light weight	Environmental masking; limited range; no identification	False or ambiguous acoustic observations can affect early-warning interpretation
Vision	Classification capability	Illumination limits; computational demand; limited range	Classification and edge-computing paths require integrity and availability protection
Passive RF	Long range; identification	Blind to encrypted protocols; confusion with other ISM-band devices	RF conditions can be manipulated or used to mask relevant emissions
Active radar	Long range; high precision	Cost and power requirements; no identification; micro-Doppler limitations	Radar inputs remain dependent on physical and signal-level assumptions
Passive radar	Long range; low cost	No identification; interference susceptibility	Interference can reduce reliability of passive sensing
Data fusion	Combines heterogeneous observations	Coordination, calibration, synchronization, and feature-exchange dependencies	Fusion can improve reliability but concentrates integrity risk

modalities.

Cross-Layer Threat Mapping

The STRIDE framework provides a useful structure for interpreting the attack surface because the detection architecture contains several trust boundaries. A sensor produces observations, a communication channel transports observations, a fusion controller combines them, and a decision process converts the combined information into an early-warning output. An attack at any of these stages can propagate to later stages even if those later stages are technically functioning as designed.

Table 3 maps the dominant threat primitives identified in the reviewed literature to the corresponding detection-system layer and the resulting consequence. Spoofing primarily threatens integrity because the system may accept false information as genuine. Jamming and denial-of-service primarily threaten availability because they reduce access to required signals or computational resources. Hijacking can affect both integrity and availability because control over a UAV or coordination channel can change the observed behavior and disrupt normal operation. Malware injection introduces the possibility that classification or decision logic itself

Table 3: Cross-layer mapping of dominant cyber threat primitives to detection-system consequences.

Threat primitive	Main property affected	Detection-system layer/ example	Potential consequence
Spoofing	Integrity	Navigation, transponder, RF or sensor inputs	False location, identity, or track information
Jamming	Availability	Wireless/cooperative surveillance channels	Loss or degradation of required signals
Denial-of-service	Availability	Edge computation or communication services	Reduced detection or processing capacity
Hijacking	Integrity and availability	UAV/control or coordination channels	Changed behavior or disrupted operation
Malware injection	Integrity	Classification or decision software	Untrusted classification or threat determination

becomes untrustworthy. The mapping demonstrates why confidentiality, although relevant, is not the sole or dominant security concern for early warning: an attacker can cause a serious operational failure without obtaining confidential information.

Data Fusion as a System-Level Attack Multiplier

The results support a central finding of this review: data fusion is simultaneously a reliability mechanism and a cybersecurity concentration point. Wang *et al.* (2021) identify multi-type fusion as a response to the limitations of individual sensing modalities. The same architecture, however, requires calibration, coordination, timing, feature exchange, and decision rules. These dependencies create opportunities for an adversary to influence the combined result without directly defeating every sensor.

The significance of this finding is architectural. If a fusion controller accepts an unverified sensor weight, time reference, or feature vector, the controller may amplify a manipulated input because the purpose of fusion is precisely to integrate multiple observations into a stronger decision. Thus, redundancy does not automatically create security. Redundancy is beneficial only when the system can distinguish trustworthy observations from manipulated observations. This is why the defensive directions identified in the source literature—authenticated exchange, integrity verification, and spoofing-resilient localization—are closely connected rather than independent recommendations.

The same principle applies to distributed acoustic arrays and other cooperative sensing configurations. Synchronization allows measurements from multiple sensors to be compared, but synchronization itself becomes a trust dependency. A detection system therefore needs to evaluate not only whether a signal is physically plausible but also whether the metadata associated with that signal can be trusted. This observation extends the discussion from sensor security to coordination security and supports the need for unified cyber-physical evaluation.

Integrity as the Principal Underserved Dimension

The cross-study comparison places integrity at the center of the unresolved problem. Morshedi and Matinkhah (2025) classify spoofing among the principal UAV cyber threats, while the electronic-warfare literature considered in the review identifies GPS, ADS-B, and transponder-related deception as important concerns. In a detection environment, these attacks are particularly significant because the purpose of the system is to make a correct determination about the location, identity, or behavior of an aerial object.

An availability attack can make a system unavailable and may therefore be visible to an operator. An integrity attack can be more difficult to recognize because the system may continue producing outputs that appear normal. This distinction is important for early warning: a false but plausible track may be more dangerous than an obvious

loss of sensor coverage because the false track can influence subsequent decisions. The reviewed literature therefore supports a defensive priority that places authentication, cross-source consistency checking, and localization resilience alongside traditional interference resistance.

Operational Implications for Airports and Safety-Critical Sites

The airport-specific literature provides a useful example of why detection cybersecurity matters beyond the technical performance of a sensor. Lykou *et al.* (2020) describe an environment in which regulatory constraints limit the response options available to operators. Under such conditions, the detection layer carries a greater proportion of the defensive burden. A cybersecurity weakness in that layer therefore has consequences not only for detection accuracy but also for the credibility of the operational response.

This finding also changes the interpretation of detection-system evidence. In a safety-critical environment, the system's output may become part of an operational record used to justify subsequent action. Consequently, integrity protection should cover the information path from sensing through fusion and decision presentation. The review does not claim that a specific technology solves this problem; rather, it shows that the airport context strengthens the requirement for trustworthy detection and makes the limitations of existing sensing approaches more consequential.

Defensive Requirements and Research Priorities

Table 4 summarizes the defensive requirements that follow directly from the threat mapping and the future directions identified in the reviewed studies. Authentication is relevant to data exchange and sensor coordination. Spoofing-resilient localization addresses the integrity of navigation and tracking information. Cyber-physical testbeds respond to the lack of reproducible benchmarks. Lightweight cryptographic approaches respond to the resource constraints associated with edge devices. Regulatory alignment ensures that technical threat models correspond to the operational environment in which the detection system is deployed.

These requirements should be treated as complementary layers rather than as competing alternatives. Strong cryptography alone does not prevent a legitimate but compromised sensor from supplying misleading data. Sensor redundancy alone does not guarantee that the fusion controller can recognize a coordinated deception. Machine-learning-based classification alone does not eliminate attacks on the data presented to the classifier. The source literature therefore supports a defense-in-depth interpretation in which authentication, localization validation, multi-sensor consistency, intrusion detection, and evaluation under adversarial conditions are considered together.

Table 4: Defensive requirements and evaluation criteria supported by the review's threat and gap analysis.

Defensive requirement	Problem addressed	Evaluation consideration
Authenticated data exchange	Untrusted sensor/coordination messages	Effectiveness and scalability
Spoofing-resilient localization	GPS, ADS-B, and transponder integrity threats	Cross-source consistency and operational suitability
Cyber-physical testbeds	Lack of reproducible adversarial benchmarks	Repeatability and controlled attack conditions
Lightweight/quantum-resistant cryptography	Security on resource-constrained edge devices	Latency, computation, and security trade-offs
Regulatory/adversarial-model alignment	Mismatch between technical threat models and operational constraints	Suitability for safety-critical deployments

Limitations of the Present Review

Several limitations should be acknowledged. First, the synthesis is based on the literature corpus and selection process described in the study, and the available sources are heterogeneous in scope and methodology. Second, the reviewed studies do not provide a single standardized quantitative measure of cyber risk across detection modalities; consequently, this paper uses qualitative comparison rather than statistical aggregation. Third, the literature contains substantially more discussion of attacks against UAV platforms than attacks against detection infrastructure itself. The conclusions concerning detection infrastructure therefore include analytical mapping from established UAV threats to the corresponding detection layer.

A further bibliographic limitation should be resolved before submission. The manuscript's selection flow reports ten studies in the qualitative synthesis, while the supplied reference list contains fewer complete bibliographic entries. This discrepancy should be checked against the original search/export records before journal submission. It is preferable to correct the reference record rather than invent a missing citation.

Future Research Directions

Five concrete research directions emerge from the gap

analysis. First, authenticated data-fusion architectures should protect sensor-to-controller communication, calibration weights, and synchronization information. Second, spoofing-resilient localization should reduce dependence on any single untrusted signal and use cross-source validation where appropriate. Third, unified cyber-physical evaluation frameworks should allow detection performance to be tested under controlled spoofing, jamming, and sensor-manipulation conditions. Fourth, cryptographic protection for resource-constrained edge devices should balance security with latency and computational requirements. Fifth, adversarial models should be aligned with the regulatory and operational conditions of safety-critical deployments.

Integrated Discussion

Taken together, the results show that drone detection cybersecurity is a system problem rather than a single-sensor problem. The five-modality taxonomy demonstrates that each sensor has useful capabilities and identifiable limitations. The cyber threat literature demonstrates that spoofing, jamming, denial-of-service, hijacking, and malware injection can target different components of an unmanned system. When these findings are combined, the detection architecture becomes a cyber-physical chain in which a manipulated observation can propagate from a sensor through a communication channel to a fusion controller and finally to an operator decision.

This integrated view also explains why the most attractive engineering solution—multi-sensor fusion—requires additional security controls. Fusion improves reliability when sensor observations are complementary and trustworthy. It becomes an attack multiplier when the system lacks mechanisms for evaluating the provenance and integrity of those observations. The security of the fusion layer is therefore not an optional software feature; it is part of the detection function itself.

The evidence further suggests that future research should evaluate security and detection performance together. A system should not be described as robust solely because it maintains detection accuracy in normal environmental conditions. The more meaningful question is whether it maintains acceptable performance when communication, navigation, timing, or sensor information is intentionally manipulated. This is consistent with the identified need for reproducible cyber-physical testbeds and adversarial evaluation frameworks.

Finally, the reviewed literature indicates that operational context matters. The airport case demonstrates how regulatory constraints can increase dependence on detection, while the UAV cybersecurity literature demonstrates that resource limitations affect the feasibility of defensive mechanisms. A practical architecture must therefore balance security effectiveness, scalability, computational cost, latency, and regulatory suitability. This multi-criteria perspective provides a more realistic basis for designing early warning systems than treating cybersecurity as an isolated requirement.

Integrated Discussion

The principal insight emerging from this cross-layer analysis is that detection cybersecurity should not be treated as separable from detection engineering. Classical counter-UAS literature has either emphasized the detection engineering problem while treating the sensor network as trusted infrastructure (Park *et al.*, 2021; Wang *et al.*, 2021), or treated the UAV as the cryptographic subject and the airframe as the trust anchor (Morshedi & Matinkhah, 2025; Shafik *et al.*, 2023). The early-warning environment demands that both perspectives be unified.

The results indicate that data fusion architectures (Wang *et al.*, 2021), although operationally necessary, simultaneously expand the attack surface through their dependence on inter-sensor coordination channels, calibration weights, and shared time synchronization. This observation implies that the prescriptive recommendation to adopt multi-type sensor fusion should be accompanied, in practice, by authenticated weight exchange, signed time-sync broadcasts, and integrity-verified feature vectors. The absence of these safeguards is a documented gap.

The cyber threat catalogue (Morshedi & Matinkhah, 2025) confirms that the most damaging attacks on detection infrastructure are integrity attacks—spoofing of GPS, ADS-B, or transponder signals (Yu *et al.*, 2025)—rather than purely availability attacks. This shifts the defensive priority from jamming resistance (which is comparatively well understood) to spoofing resistance (which is not). Yu *et al.* demonstrate that defensive aids for electronic warfare against UAVs are an active area of research, but that the comparison of common cyberattacks and countermeasure approaches remains incomplete (Yu *et al.*, 2025).

The airport-domain evidence (Lykou *et al.*, 2020) underscores an additional concern: regulatory restrictions on kinetic mitigation force detection to bear the entire defensive burden, but the existing counter-drone sensor suite has observable limitations in this environment. In practice, this means that the early-warning system must serve as both a detector and a regulator's evidentiary record, raising data-integrity requirements beyond what current architectures provide.

Finally, the systematic assessment of Oli and Mahalal (2025) indicates that the field's principal recurring gaps concern the lack of reproducible benchmarks, limited coverage of cross-layer attacks, and inadequate consideration of regulatory dimensions. The forward-looking research agenda they propose therefore aligns closely with the gaps surfaced by the present analysis: authenticated data fusion, spoofing-resilient localization, and unified detection–cybersecurity evaluation frameworks.

Detailed Future Research Directions

Five concrete research directions emerge from the gap analysis above.

6.1 Authenticated Data Fusion Architectures. Because fusion controllers constitute a high-value target

for weight-manipulation and time-synchronization attacks (Wang *et al.*, 2021), future architectures should incorporate cryptographic weight exchange, signed inter-sensor broadcast channels, and integrity-verified feature vectors. Promising directions include blockchain-assisted distributed coordination, broadly sketched in the Morshedi–Matinkhah threat modelling framework (Morshedi & Matinkhah, 2025), and authenticated multi-party computation for distributed acoustic arrays.

6.2 Spoofing-Resilient Localization. GPS, ADS-B, and transponder spoofing constitute the dominant integrity threats identified across both the detection (Yu *et al.*, 2025) and the UAV-cybersecurity (Morshedi & Matinkhah, 2025)literatures. Future work should prioritize multi-source localization that does not depend on any single untrusted signal-of-opportunity, combined with on-platform inertial measurement validation. The Yu *et al.* electronic-warfare treatment of ADS-B defenses (Yu *et al.*, 2025) provides a concrete starting point.

6.3 Unified Cyber-Physical Evaluation Frameworks. The absence of reproducible benchmarks is a recurrent gap (Oli & Mahalal, 2025). Future efforts should construct cyber-physical testbeds in which detection performance can be evaluated under controlled spoofing, jamming, and sensor-weight manipulation conditions, drawing on the datasets and tools catalogued by Oli and Mahalal (2025) and the airport-domain empirical insights of Lykou *et al.* (2020).

6.4 Quantum-Resistant and Lightweight Cryptographic Protocols. Detection architectures increasingly deploy resource-constrained edge devices (Morshedi & Matinkhah, 2025). Future research must reconcile post-quantum cryptographic primitives with the computational budget of these devices, while preserving the latency requirements of real-time fusion pipelines.

6.5 Regulatory and Adversarial-Model Alignment. Detection infrastructures operate within regulatory frameworks that affect both the sensor suite and the permissible response set (Lykou *et al.*, 2020). Future research should align adversarial threat models with the regulatory environment, particularly in airport and other safety-critical domains where the burden of detection is heaviest.

CONCLUSION

This paper has analyzed the cybersecurity threat landscape confronting drone detection and early warning systems through a structured systematic review that couples detection-modality analysis with cross-layer cyber threat mapping. The principal contribution is the demonstration that the detection modalities most widely recommended for reliability—sensor fusion architectures—are simultaneously the architectures most vulnerable to integrity attacks on their coordination channels. The five-modality detection inventory exhibits modality-specific vulnerabilities that are individually tractable, but the fusion of these modalities produces a combinatorial attack surface that is not adequately addressed by any single existing defensive primitive. The cyber threat catalogue—spoofing, jamming, denial-of-service, hijacking, and malware injection—is well-characterized in the UAV-as-subject literature but remains under-applied to the detection-as-infrastructure problem. Emerging research directions including blockchain integration, federated learning, and quantum-resistant cryptographic frameworks (Morshedi & Matinkhah, 2025) provide promising but partial remedies. The work of Oli and Mahalal (2025) suggests that an explicit forward-looking research agenda is required to translate these primitives into deployable detection defenses. Until such an agenda is realized, drone detection and early warning systems should be regarded as cyber-physical systems with elevated residual risk, and operators should plan accordingly.

REFERENCES

Adel, A., Alani, N. H., Thompson-Whiteside, S., & Jan, T. (2024). Who is watching whom? Military and civilian drone: Vision intelligence investigation and recommendations. *IEEE Access, 12*, 177236–177276. https://doi.org/10.1109/ACCESS.2024.3505034

Khawaja, W., Ezuma, M., Semkin, V., Erden, F., Ozdemir, O., & Guvenc, I. (2026). A survey on detection, classification, and tracking of AAVs using radar and communications systems. *IEEE Communications Surveys & Tutorials, 28*, 3272–3310. https://doi.org/10.1109/COMST.2025.3554613

Sensors, 20(12), 3537. https://doi.org/10.3390/s20123537Lykou, G., Moustakas, D., & Gritzalis, D. (2020). *Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies*.

Morshedi, R., & Matinkhah, S. M. (2025). Cybersecurity challenges and solutions in unmanned aerial vehicles (UAVs). *Journal of Field Robotics*. https://doi.org/10.1002/rob.70040

Oli, A., & Mahalal, E. (2025). UAV security: Attacks, defenses, and open challenges. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3647023

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

Shafik, W., Matinkhah, S. M., & Shokoor, F. (2023). Cybersecurity in unmanned aerial vehicles: A review. *International Journal on Smart Sensing and Intelligent Systems, 16*(1). https://doi.org/10.2478/ijssis-2023-0012

Wang, J., Liu, Y., & Song, H. (2021). Counter-unmanned aircraft system(s) (C-UAS): State of the art, challenges, and future trends. *IEEE Aerospace and Electronic Systems Magazine, 36*(3), 4–29. https://doi.org/10.1109/MAES.2020.3015537

Yu, A., Kolotylo, J., Hashim, H. A., & Eltoukhy, A. E. E. (2025). Electronic warfare cyberattacks, countermeasures, and modern defensive strategies of UAV avionics: A survey. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3561068