(Online) ISSN 2744-1741
*Original Research*

**Defense and Security Studies**
Vol. 7, No. 1, 2026, pp.174-188
https://doi.org/10.37868/dss.v7.id327

# Cyber-electronic warfare threats to UAS: comparative analysis and adaptive resilience framework

**Aleksandar Donev*[1], Dimitar Bogatinov**
[1] MSc Student, Military Academy, University "Goce Delcev", N. Macedonia

*Corresponding author E-mail: donevaleksandar1983@gmail.com

Received: Mar. 19, 2026
Revised: May 6, 2026
Accepted: May 9, 2026
Online: May 11, 2026

**Abstract**

Unmanned Aerial Systems (UAS) are increasingly deployed in defense, security, and critical infrastructure missions where reliable communications and navigation are essential for operational effectiveness. The purpose of this paper is to analyze the convergence of cyber threats and electronic warfare against UAS and to develop a comparative security framework for improving communication resilience in defense-relevant operating environments. The study makes three explicit contributions: it constructs a structured threat taxonomy aligned with the cyber-electromagnetic threat space; it introduces an operationalized comparative assessment procedure using a five-criterion weighted scoring matrix; and it proposes a formalized state-based resilience framework with explicit indicator-driven transition thresholds. The research applies a theoretical-analytical and comparative method based on a synthesis of peer-reviewed literature, with primary applicability to small-to-medium tactical UAS relying on MAVLink-based communication in resource-constrained embedded environments. Key threats are categorized and examined, including man-in-the-middle attacks, command and code injection, denial-of-service operations, Global Navigation Satellite System (GNSS) spoofing, and radio-frequency (RF) jamming. Security postures are compared across five criteria using an explicit five-point scoring scale and criterion weights. The weighted composite scores indicate that adaptive and risk-informed approaches (3.65/5.00) show structurally stronger analytic alignment with hybrid threat conditions than layered defense models (2.90/5.00) or static architectures (2.20/5.00) within the defined framework. The major conclusion is that UAS communication security benefits from resilience-driven and adaptive design principles supported by structured comparative assessment and formalized state-transition logic, providing a practical basis for future implementation planning and policy development in contested electromagnetic and cyber environments.



*Keywords*: electronic warfare, command injection, man-in-the-middle, denial-of-service, layered defense, anomaly detection, ground control station, risk scoring, GNSS spoofing, adaptive resilience

## 1. Introduction

Unmanned aerial systems have become a critical capability across defense, border security, emergency response, and critical infrastructure protection due to their flexibility, reduced operational cost, and ability to

operate in complex environments. Their effectiveness, however, is strongly conditioned by the reliability and integrity of the communication and navigation subsystems that enable command-and-control, telemetry exchange, and mission execution. Recent survey literature emphasizes that UAS security is challenged by the combination of generic components, widely used communication protocols, and heterogeneous system integration, which collectively expand the attack surface and complicate end-to-end protection [1]. The security problem addressed in this paper is not limited to isolated techniques, but rather to the convergence of multiple threat vectors and the practical limitations of common protection approaches when facing dynamic, hybrid scenarios. Comprehensive reviews of UAS cybersecurity show recurring patterns of exploitation in communication links, software components, and system interfaces, where attacks may target confidentiality, integrity, and availability simultaneously [1], [2]. From an operational perspective, this convergence becomes more critical when cyber actions are coordinated with electromagnetic interference, producing compounded effects on decision-making, mission continuity, and platform survivability.

A persistent concentration of vulnerabilities is observed around the command-and-control link, navigation integrity, and the interface between the aerial platform and the ground control ecosystem. For example, Global Navigation Satellite System (GNSS) spoofing has been widely analyzed as a threat capable of misleading or redirecting UAVs by manipulating positioning information, including stealthy or staged attack strategies [3], while GNSS spoofing detection and characterization is treated as a mature research problem with defense relevance [4]. Similarly, jamming remains a dominant risk to communications and navigation availability, and research has examined how adversarial interference can shape mission outcomes and disrupt essential functions [5]. In parallel, cyber-focused studies highlight that UAS networks can be exposed to interception, manipulation, and disruption attacks, including man-in-the-middle and denial-of-service actions, particularly when security controls remain static or are only partially integrated across system layers [2].

These challenges motivate a resilience-oriented analytical approach that goes beyond siloed treatment of cyber threats and electromagnetic threats. A complementary driver is the growing emphasis on airworthiness and operational security processes that integrate security risk assessment and assurance activities throughout the lifecycle. Aviation security guidance recognizes formal processes and methods for airworthiness security (including threat modeling and verification considerations), which are increasingly referenced by authorities as acceptable means of compliance [6]. At the protocol level, widely deployed UAV ecosystems have also introduced mechanisms such as message signing to support authentication and mitigate unauthorized command injection and manipulation risks, but practical adoption and system-level integration remain nontrivial in heterogeneous deployments [7].

Accordingly, the objective of this paper is threefold, and its contributions are explicitly differentiated from existing survey and review literature [1], [2], [11]. First, whereas prior surveys provide broad coverage of attack classes and defense concepts, this paper constructs a five-dimensional threat taxonomy structured around operational consequence and attacker access model, extended to treat hybrid cyber-electromagnetic combinations as a distinct high-priority threat class warranting integrated assessment. Second, the paper introduces a formalized five-criterion weighted scoring procedure for comparing security postures - a reproducible analytic tool absent from survey-level treatments that rely on qualitative prose comparison. Third, the proposed state-based resilience framework advances beyond conceptual resilience models by formalizing indicator-driven transition thresholds between security states, providing a specification directly usable for implementation planning. The scope remains theoretical and analytical, without empirical validation, but the structured methodology provides a traceable and reproducible basis for reasoning that goes beyond narrative synthesis [1], [6].

The remainder of the paper is organized as follows. Section 2 describes the research method and comparative design. Section 3 presents a threat taxonomy relevant to unmanned system communications and navigation. Section 4 provides a comparative analysis of existing security approaches and identifies recurring limitations under hybrid conditions. Section 5 outlines the proposed conceptual framework and the rationale behind its

design. Section 6 presents the results and discussion through a scenario-based analytical assessment. Section 7 concludes the paper and summarizes conclusions, limitations, and directions for future work.

## 2. Research method

This paper applies a theoretical-analytical and comparative research method to examine cyber and electronic warfare threats to unmanned aerial systems (UAS) and to assess how different security approaches address these threats. Because experimental validation is outside scope, the study relies on structured synthesis of high-quality literature and a transparent comparison framework.

First, sources were identified through structured search of IEEE Xplore, Web of Science, and Scopus, using search strings combining terms such as 'UAS cybersecurity', 'UAV electronic warfare', 'GNSS spoofing detection', 'GNSS jamming UAV', 'MAVLink security', 'UAV intrusion detection', and 'unmanned systems communication resilience'. The search covered publications from 2016 to 2026, with primary emphasis on works from 2020 onwards. Inclusion criteria required that sources address at least one of the following: (a) empirical or experimental analysis of UAS attack or defense mechanisms; (b) survey or review coverage of UAS security spanning multiple attack classes; or (c) primary protocol or standards documentation directly relevant to UAS communication security (e.g., MAVLink specification, EASA airworthiness guidance). Sources were excluded if they addressed security of generic ground-based or fixed network systems without UAS-specific relevance, or if they predated the MAVLink 2 specification without historical relevance to the analysis. Coverage was expanded using a structured snowballing approach from seed papers to relevant primary sources [10].

Second, a comparative assessment is conducted across three recurring security postures: static protection, layered defense, and adaptive/risk-informed approaches [1], [2]. Each posture is evaluated against five predefined criteria with assigned weights reflecting their relative importance to hybrid threat readiness in defense-relevant UAS environments: (1) threat coverage [weight 0.25], (2) responsiveness under hybrid cyber-electromagnetic conditions [weight 0.30], (3) operational suitability for defense contexts [weight 0.20], (4) resource awareness under constrained onboard compute and energy budgets [weight 0.15], and (5) feasibility of integration and assurance across heterogeneous UAS stacks [weight 0.10]. Each criterion is scored on a five-point scale: 1 = Very Low, 2 = Low, 3 = Moderate, 4 = High, 5 = Very High. Scores are assigned based on evidence synthesized from the reviewed literature for each criterion (Section 4), and a weighted total is computed as the criterion-weighted sum of scores. The resulting decision matrix (Table 1) provides a structured and reproducible comparative baseline. It is important to note that these scores represent structured qualitative assessments grounded in literature synthesis, not empirical measurements; their purpose is analytic ordering rather than absolute performance quantification. The findings are then interpreted through scenario-based analytical assessment - covering navigation deception, availability denial, and hybrid combinations - to illustrate expected effects and response limitations under contested conditions [4], [8].

## 3. Threat taxonomy relevant to unmanned system communications and navigation

This section defines a threat taxonomy focused on the two most mission-critical dependency chains in unmanned aerial systems (UAS): (1) communications and command-and-control (C2) and (2) navigation (GNSS-based positioning and timing). The taxonomy is derived from widely used UAS security classifications in the literature and is aligned with the security objectives of availability, integrity, confidentiality, and control authority in UAS operations [11], [2].

### 3.1. Taxonomy dimensions and classification logic

To ensure that threats are comparable across different UAS architectures, each threat in this taxonomy is classified along five dimensions: (1) target surface (C2/telemetry link, payload/video link, ground control station (GCS) interface, onboard software/firmware, or navigation receiver chain) [11], [2]; (2) attack effect

(disruption, deception, or takeover) [11], [3]; (3) security property impacted (availability, integrity, confidentiality, authenticity, and control authority) [11]; (4) attacker access assumption (proximity-based RF access, network-path access, or local/system access) [11], [12]; and (5) operational consequence (loss of C2, degraded mission performance, unsafe flight behavior, or forced mission termination). This structure supports consistent mapping of cyber threats and electronic warfare (EW) effects into one analytical frame, which is essential for later comparative assessment.

Frequency band context. The attack surface is shaped in part by the frequency bands on which UAS operate. Common UAS spectrum segments include UHF telemetry and C2 links at 433 MHz and 900 MHz, ISM bands at 2.4 GHz and 5.8 GHz for control and video, GPS L1 at 1575.42 MHz (shared by Galileo E1), GLONASS around 1602 MHz, BeiDou B1 at 1561.098 MHz, and increasingly 4G LTE (700-2600 MHz) and 5G Sub-6 GHz (3.3-5.0 GHz) for BVLOS operations [11], [21]. Each band presents specific vulnerability profiles: low-power civil GNSS signals carry no cryptographic authentication and are susceptible to intentional interference and spoofing, while ISM bands used for C2 and telemetry are accessible with commercially available RF equipment. The transition to IP-based 4G/5G connectivity introduces additional threat surfaces familiar from mobile network security, including protocol-level attacks and rogue base station scenarios [20], [21].

### 3.2. Threats to communications and command links

**A. Man-in-the-middle (MITM) and interception attacks.**
MITM threats include interception and manipulation of UAV-GCS traffic, potentially enabling command tampering, telemetry falsification, or replay of stale data. Surveys consistently identify MITM/interception as a major risk in UAS communication chains, especially when encryption and authentication are absent or inconsistently deployed across links and relays [11], [2].

**B. Unauthorized access and credential/protocol compromise.**
Unauthorized access may occur through weak authentication, misconfigured services, exposed management interfaces, or credential compromise of the GCS/operator device. This category is often coupled with protocol weaknesses and insufficient access control in heterogeneous UAS ecosystems [11], [2].

**C. Command injection and false message insertion.**
Command injection targets the integrity of mission commands by inserting unauthorized control messages into the C2 channel. This risk is particularly relevant to widely used UAV control protocols where messages can be forged if cryptographic authentication is not enforced end-to-end. Empirical work on MAVLink demonstrates how message properties and deployment patterns can enable practical packet injection and mission disruption [12]. Network-level detection research further supports the feasibility of false MAVLink injection under realistic assumptions [13].

**D. Denial of Service / Distributed Denial of Service (DoS/DDoS).**
DoS attacks degrade availability by exhausting bandwidth, processing capacity, or protocol resources on the UAV, relay nodes, or GCS. UAS surveys report DoS as a high-impact class due to the tight coupling between link availability and safe flight control [11], [2], [12].

**E. Protocol and implementation exploitation.**
Beyond conceptual attack classes, protocol parsing issues, fuzzing-discovered faults, and implementation vulnerabilities can cause autopilot or ground software instability, potentially resulting in mission aborts or unsafe behavior. Empirical studies and follow-on analyses highlight that protocol-level weaknesses can translate into operational disruptions even without full system compromise [12], [13].

### 3.3. Threats to navigation and positioning integrity

**A. GNSS spoofing (navigation deception).**
GNSS spoofing aims to mislead the Unmanned Aerial Vehicle (UAV)'s position/velocity/time estimates by broadcasting counterfeit satellite-like signals, enabling trajectory manipulation or unsafe navigation decisions.

A dedicated UAV-focused review provides a detailed spoofing taxonomy and emphasizes that spoofing can be engineered to be stealthy and operationally effective against civil GNSS-dependent platforms [3]. More general spoofing literature explains how detection and mitigation are central to maintaining navigation integrity under adversarial conditions [4].

**B. RF jamming (availability denial).**

Jamming disrupts availability by raising the noise floor or saturating the receiver front-end, leading to degraded or lost GNSS fixes and/or disrupted RF communications. In UAS contexts, jamming is frequently treated as a primary EW risk because even short disruptions can cascade into control instability or failsafe activation [11], [2], [4]. Systematic reviews focused on UAV navigation consolidate common jamming and spoofing approaches and defenses [8].

### 3.4. Hybrid (cyber-electromagnetic) threat combinations

A key operational concern is that adversaries may combine deception and disruption across domains to amplify effects - for example, spoofing to manipulate navigation while jamming or DoS suppresses recovery channels, or command injection timed with RF interference to reduce operator ability to validate telemetry. The literature increasingly treats such combinations as a practical reality in contested environments, motivating integrated resilience-oriented assessment rather than isolated threat treatment [11], [3], [8]. Real-world incidents corroborate this concern: the 2011 compromise of a high-value ISR UAV reportedly exploited excessive trust in civil GNSS signals without cryptographic validation, and systematic electronic warfare operations in the 2014-2022 Ukrainian conflict demonstrated that GPS jamming combined with C2 link interference can substantially degrade tactical UAS effectiveness [20].

## 4. Comparative analysis of existing security approaches and recurring limitations under hybrid conditions

This section compares three dominant security postures discussed in the UAS security literature - static protection, layered defense, and adaptive/risk-informed approaches - against the threat taxonomy in Section 3, with emphasis on hybrid cyber-electromagnetic conditions. The comparison follows the criteria and scoring procedure defined in Section 2 and aligns with how surveys map defenses to attack surfaces in UAS ecosystems [1], [2], [11].

### 4.1. Static security architectures

Static protection refers to security measures configured at design time or deployment time and typically maintained with limited or no runtime adaptation. Common examples include fixed cryptographic settings, baseline access control, predefined protocol checks, and static operational procedures for link usage. Surveys observe that such controls can improve baseline confidentiality and integrity, but their effectiveness depends strongly on consistent end-to-end deployment and correct operational configuration across UAV, GCS, relays, and payload subsystems [1], [2], [11].

Protocol mechanisms such as message authentication and signing are frequently referenced as practical controls that can reduce unauthorized command injection when properly enabled and managed [7], [9]. However, static configurations do not inherently address dynamic adversary behavior such as time-varying interference patterns, stealthy navigation deception, or coordinated multi-vector attacks [4], [8].

Applying the scoring procedure from Section 2: threat coverage scores 2 (Low) as static controls address a subset of attack classes but leave interference-driven and navigation-deception threats largely unaddressed; responsiveness under hybrid conditions scores 1 (Very Low) as there is no mechanism for runtime adaptation; operational suitability scores 2 (Low) because predictable failsafe behaviors can be anticipated and exploited in contested environments; resource awareness scores 4 (High) as static configurations typically impose minimal

runtime overhead; and integration/assurance feasibility scores 4 (High) as deployment and verification of fixed controls is well understood.

### 4.2. Layered defense models

Layered defense (defense-in-depth) combines multiple controls across system layers - communication security (e.g., encryption and authentication), monitoring (e.g., anomaly detection and IDS), platform hardening, and operational procedures - to reduce single points of failure. This posture is widely recommended in UAS security surveys because attacks can occur at the protocol, network, application, and physical/RF layers, and no single control covers all threat types [1], [2], [11].

Nevertheless, layered architectures often face limitations in integration consistency, added overhead, and coordination delays between detection and response, especially under fast hybrid escalation and constrained resources [1], [2], [16], [17].

Applying the scoring procedure: threat coverage scores 3 (Moderate) as multiple layers extend coverage but with gaps at the cyber-EW interface; responsiveness under hybrid conditions scores 3 (Moderate) as detection capabilities improve but response coordination may lag under simultaneous multi-vector alerts; operational suitability scores 3 (Moderate) as defense-in-depth is broadly appropriate but effectiveness is sensitive to integration maturity; resource awareness scores 3 (Moderate) as additional monitoring and control layers increase overhead; and integration/assurance feasibility scores 2 (Low) as achieving consistent enforcement across UAV-GCS-relay interfaces is operationally demanding.

### 4.3. Adaptive and risk-informed approaches

Adaptive/risk-informed approaches aim to adjust protection strength and response actions in relation to observed conditions (e.g., threat indicators, environmental interference, mission phase, and resource availability). This posture is motivated by the observation that UAS operate in dynamic environments and may require responses that balance mission continuity against performance and energy constraints [1], [2].

In hybrid cyber-electromagnetic settings, adaptive approaches are better positioned to coordinate integrity-oriented controls with resilience actions addressing interference and navigation trust management [4], [8], [18]. However, such approaches depend on reliable indicators, well-defined decision logic, and feasible integration across heterogeneous UAS stacks - factors repeatedly highlighted as practical challenges [1], [2], [17].

Applying the scoring procedure: threat coverage scores 4 (High) as the approach addresses both cyber and EW threat classes in an integrated manner; responsiveness under hybrid conditions scores 4 (High) as state-based coordination of detection and response is explicitly designed for combined threats; operational suitability scores 4 (High) as proportional escalation and mission-aware response align with contested environment requirements; resource awareness scores 3 (Moderate) as risk-based activation can optimize overhead but reliable indicators add processing demands - a consideration empirically grounded in cryptographic overhead measurements on embedded UAV platforms, where even modest security additions impose measurable CPU and energy costs [20]; and integration/assurance feasibility scores 2 (Low) as assurance of adaptive decision logic and reliable indicator pipelines across heterogeneous stacks remains a significant implementation challenge.

### 4.4. Comparative summary and recurring limitations under hybrid conditions

Table 1 presents the weighted decision matrix derived from the scoring procedure in Section 2, providing a structured and reproducible basis for comparing the three security postures. Weighted totals are computed as the sum of criterion scores multiplied by criterion weights.

In Table 1, scoring key: 1 = Very Low, 2 = Low, 3 = Moderate, 4 = High, 5 = Very High. Scores represent structured qualitative assessments based on literature synthesis; weighted totals are analytic ordering indicators, not empirical performance measurements.

Table 1 Weighted decision matrix for UAS security posture comparison

| Criterion | Weight | Static Score | Static Weighted | Layered Score | Layered Weighted | Adaptive Score | Adaptive Weighted |
|---|---|---|---|---|---|---|---|
| Threat coverage | 0.25 | 2 | 0.50 | 3 | 0.75 | 4 | 1.00 |
| Responsiveness under hybrid conditions | 0.30 | 1 | 0.30 | 3 | 0.90 | 4 | 1.20 |
| Operational suitability for defense | 0.20 | 2 | 0.40 | 3 | 0.60 | 4 | 0.80 |
| Resource awareness | 0.15 | 4 | 0.60 | 3 | 0.45 | 3 | 0.45 |
| Integration/assurance feasibility | 0.10 | 4 | 0.40 | 2 | 0.20 | 2 | 0.20 |
| Weighted Total (max 5.00) | 1.00 | - | 2.20 | - | 2.90 | - | 3.65 |

Table 2 shows qualitative comparative summary of security postures under hybrid conditions.

Table 2 Qualitative comparative summary of security postures under hybrid conditions

| Approach | Adaptability | EW Resistance | Strategic Suitability |
|---|---|---|---|
| Static security architectures [Weighted score: 2.20/5.00] | Low (score 1-2): relies on fixed configurations; limited ability to react to escalation or combined threats | Low-Medium (score 1-2): can protect message integrity if properly configured, but does not address interference-driven degradation or navigation deception | Medium (score 2): suitable for low-to-moderate threat contexts; vulnerable in contested environments due to limited responsiveness |
| Layered defense models [Weighted score: 2.90/5.00] | Medium (score 3): multiple controls improve detection and coverage, but response coordination may lag under fast hybrid escalation | Medium (score 3): broader resilience than static models, yet often lacks unified cyber-EW alignment and may not sustain function under strong interference | High-Medium (score 3): appropriate for defense settings when integration is mature, but effectiveness depends on consistent enforcement across UAV-GCS-relay interfaces |
| Adaptive/risk-informed approaches [Weighted score: 3.65/5.00] | High (score 4): supports proportional escalation and de-escalation and state-based response under hybrid conditions | High-Medium (score 4): better positioned to handle combined deception and disruption by linking indicators to coordinated responses, including navigation trust management | High (score 4): aligns with contested environments and mission continuity needs, but assurance and implementation complexity remain challenges |
| Recurring hybrid limitations (cross-cutting) | Even advanced approaches face ambiguity in distinguishing interference from deception and require robust detection-response coupling | Hybrid attacks can suppress recovery channels (e.g., spoofing + jamming/DoS), exposing gaps where cyber-only or EW-only measures are insufficient | End-to-end consistency and interoperability across UAV-GCS ecosystems remain decisive; gaps at interfaces often determine real-world resilience |

(Based on comparative evidence from [1], [2], [4], [11], [17])

Table 1 reveals a clear trade-off pattern. Static architectures achieve the highest resource-efficiency scores (4) and the best integration/assurance scores (4) due to their deployment simplicity, but this advantage is offset by critically low responsiveness to hybrid conditions (1) and limited threat coverage (2), yielding the lowest weighted total of 2.20/5.00. Layered defense improves substantially on threat coverage and responsiveness, reaching 2.90/5.00, but suffers on integration/assurance feasibility (2) because consistent enforcement across UAV-GCS-relay interfaces is operationally demanding. The adaptive and risk-informed approach achieves the highest weighted total of 3.65/5.00, driven by its advantage on the two highest-weighted criteria - responsiveness under hybrid conditions (weight 0.30) and threat coverage (weight 0.25) - but faces the same integration/assurance challenge as layered defense, and its moderate resource-awareness score reflects the measurable CPU and energy overhead associated with active monitoring and decision logic on constrained embedded processors.

## 5. Proposed coneptual framework and rationale

Building on the trade-offs summarized in Tables 1 and 2, the proposed framework aims to preserve baseline efficiency while enabling proportional escalation under hybrid cyber-electromagnetic conditions. This section outlines a conceptual security framework designed to address the recurring limitations identified in Section 4 when UAS operate in contested environments. The framework is not presented as an implementation blueprint; rather, it serves as a structured analytical model that links (1) the threat classes in Section 3, (2) operational constraints, and (3) response options that can be reasoned about consistently in defense-relevant settings. The design rationale is grounded in UAS cybersecurity survey findings on attack surfaces and defense gaps [1], [2], and in established literature on GNSS spoofing and jamming behavior and detection families [4], [8], [18].

### 5.1. Design objectives and platform scope

The framework is primarily intended for small-to-medium tactical UAS with a maximum take-off weight below 25 kg, employing MAVLink-based communication protocols over resource-constrained embedded processors - such as ARM Cortex-M class autopilot controllers (e.g., STM32H7-based platforms). This class encompasses widely used research and tactical platforms relying on software-defined security layers without dedicated hardware security modules. Applicability to MALE/HALE class systems or platforms employing military-grade COMSEC hardware may require additional assurance considerations beyond the scope of this framework.

The framework is guided by five objectives aligned with hybrid-threat realities. Hybrid threat alignment treats cyber intrusions and electromagnetic interference as potentially coordinated, considering combined effects on control authority, availability, and navigation integrity [4], [8], [18]. Resilience orientation prioritizes continuity of essential functions under degradation rather than assuming full prevention is always feasible [1], [2]. Risk-informed proportionality scales protective actions to observed risk and mission phase to avoid unnecessary overhead while preserving safety and control authority [1], [2]. Resource awareness remains compatible with constrained onboard compute and energy conditions [1], [2]. Traceability and assurance support clear reasoning about why a response is triggered, which is important for operational acceptability and lifecycle security planning [1], [2].

### 5.2. Framework overview

The proposed framework consists of four conceptual layers. The sensing/indicators layer collects evidence of abnormal conditions affecting C2 integrity and availability (e.g., suspicious command patterns, authentication failures) and navigation integrity and availability (e.g., GNSS consistency anomalies, loss of fix, interference indicators). GNSS-focused literature emphasizes that detection and mitigation must be driven by observable correlates of spoofing and jamming rather than assumptions about attacker capability [4], [18]. The threat interpretation layer maps observed indicators to the threat taxonomy (Section 3), distinguishing disruption-oriented, deception-oriented, or takeover-oriented patterns at the communication and navigation dependency chains [1], [2], [8]. The risk assessment layer estimates an operational risk level based on threat severity,

exposure, mission criticality, and resource margin, enabling proportional response selection rather than fixed escalation [1], [2]. The response orchestration layer activates a state-based response (Section 5.4) that coordinates cyber controls with EW-relevant resilience actions (e.g., navigation trust management, fallback modes, controlled mission degradation).

### 5.3. Risk-informed adaptation logic

To avoid purely static security behavior, the framework uses a risk-informed logic to guide response selection. Conceptually, risk is treated as a function of four factors: threat severity (expected impact if the threat succeeds), exposure and likelihood (plausibility given the operational context and current indicators), mission criticality (dependence on the affected function during the current phase), and resource margin (available compute, energy, and time budget for additional controls without compromising safe flight).

This logic is designed to address a recurring limitation identified in Section 4: under hybrid conditions, uniformly high protection can be operationally costly, while uniformly low protection can be unsafe. The framework therefore supports proportional escalation and de-escalation of measures according to observed conditions and mission needs.

### 5.4. State-based response mechanism with indicator thresholds

To make adaptation interpretable and auditable, the framework expresses response behavior as discrete security states with explicit transition triggers and threshold conditions. The following indicator thresholds provide a reference baseline for state transitions, subject to platform-specific calibration:

**State S0 (baseline).** Normal operation with standard authentication and monitoring is applied when indicators do not suggest active hybrid threats. The platform operates with standard MAVLink authentication policies and routine telemetry health monitoring.

**S0 to S1 transition (baseline to elevated).** The Elevated state is triggered when any of the following conditions persists for more than 5 seconds: (a) GNSS signal-to-noise ratio drops more than 10 dB below the established operational baseline, or the positional consistency between GNSS output and IMU-based dead reckoning diverges beyond 30 meters; (b) MAVLink authentication failures exceed 2 events per minute; (c) C2 link received signal strength indicator (RSSI) degrades by more than 15 dB from the operational baseline; or (d) anomalous packet injection patterns are detected on the C2 channel. In S1, additional command validation and interface monitoring are enabled, and non-essential interfaces may be restricted.

**S1 to S2 transition (elevated to defensive/resilient).** The Defensive/Resilient state is triggered when any of the following conditions holds: (a) GNSS-IMU positional inconsistency exceeds 50 meters or persists for more than 10 consecutive seconds while in S1; (b) authentication failures sustain at more than 10 events per minute; (c) C2 link loss exceeds 3 continuous seconds; or (d) two or more independent S1-level indicators are simultaneously active, suggesting coordinated multi-vector action. In S2, priority shifts to maintaining safe control authority and bounded mission behavior via strict command acceptance policies, navigation trust management (e.g., fallback to IMU-only or last-known-safe position logic), and controlled mission degradation.

**Return transitions.** To prevent rapid state oscillation under intermittent interference, return transitions follow a hysteresis logic. S2 returns to S1 only when all active S2-trigger conditions have cleared for at least 30 consecutive seconds. S1 returns to S0 only when all indicator readings have been nominal for at least 60 consecutive seconds.

This abstraction is quite consistent with practical UAV ecosystems that implement hardening controls such as authenticated command acceptance (e.g., MAVLink message signing [7], [9]), which explicitly separates acceptable from unacceptable command traffic as a function of trust configuration. It also aligns with GNSS security literature emphasizing that once spoofing or jamming is suspected, systems should shift from naive trust in navigation outputs to validated or fallback behaviors to preserve navigation integrity and safety [4], [18].

### 5.5. Rationale and traceability to Section 4 limitations

The framework is intentionally matched to the recurring hybrid limitations identified in Section 4. The joint treatment of disruption and deception indicators addresses the misalignment between controls and attacker objectives, ensuring responses are selected based on whether the dominant risk is availability loss (e.g., jamming or DoS) or integrity loss (e.g., injection or spoofing) [4], [8]. Coordinated actions across UAV-GCS boundaries address incomplete end-to-end enforcement, consistent with survey findings on interface gaps [1], [2]. Explicit state transitions formalize how detection signals lead to concrete operational actions, resolving detection-response coupling challenges [1], [2]. Risk-informed proportionality reduces unnecessary overhead and supports mission-aware security scaling [1], [2]. Finally, the intermediate Elevated state (S1) supports uncertainty management by increasing validation before committing to more disruptive defensive actions, reducing the risk of inappropriate responses under ambiguous RF conditions [4], [18].

## 6. Results and discussion: scenario-based analytical assessment and defense resilience implications

This section presents scenario-based analytical results derived from the threat taxonomy (Section 3), the comparative criteria and weighted scores (Section 4), and the framework transition thresholds (Section 5.4). The scenarios reflect widely discussed disruption and deception patterns affecting UAS communications and navigation. Figure 1 provides a compact visual summary of the structured qualitative comparison across the three scenarios; the values represent relative ordering within the scoring framework described in Section 2 and are not empirical performance measurements.

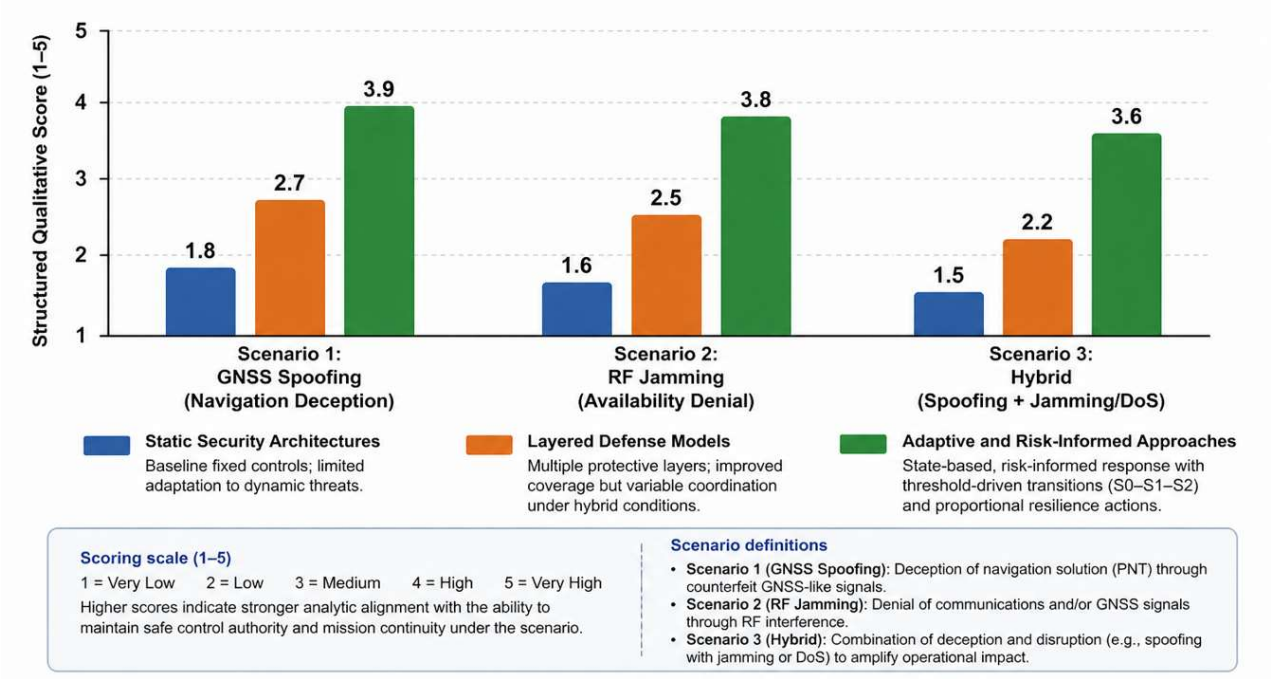


Figure 1. Scenario-based analytical comparison of security postures across GNSS spoofing, RF jamming, and hybrid (spoofing + jamming/DoS) conditions.

### 6.1. Results

#### 6.1.1. Scenario 1: GNSS spoofing (navigation deception)

**Scenario description.** The attacker broadcasts counterfeit GNSS-like signals to mislead the UAS navigation solution, aiming to induce trajectory deviation, geofence violation, unsafe routing, or loss of mission integrity. Spoofing may be engineered to appear plausible and can be staged to reduce detectability, making it a high-consequence deception threat for GNSS-dependent platforms.

**Static architectures.** Static controls (e.g., baseline authentication for C2) do not directly validate navigation truthfulness. The platform may continue to trust corrupted GNSS outputs unless independent integrity checks or fallback navigation logic are already configured. This produces a vulnerability gap where C2 integrity may remain intact while navigation integrity degrades silently, enabling mission manipulation without classic cyber compromise.

**Layered defense models.** Layered approaches can improve detection likelihood if they include navigation consistency checks, sensor fusion sanity tests, or monitoring that flags abnormal navigation behavior. However, the response may remain operationally unclear or delayed if detection and response are not tightly coupled, particularly when spoofing is subtle and confidence thresholds are conservative.

**Adaptive/risk-informed approaches (proposed framework).** According to the structured assessment criteria, the proposed framework shows stronger analytic alignment with this scenario. Spoofing is treated as an integrity-deception condition, supporting risk-informed escalation through state-based actions (S1/S2) with explicit thresholds. Under emerging inconsistencies exceeding the 30-meter GNSS-IMU divergence threshold, the Elevated state (S1) increases validation; under stronger indicators (>50 m divergence or sustained >10 s), the Defensive/Resilient state (S2) prioritizes navigation trust management while maintaining safe control authority. This advantage is conceptual, not demonstrated empirically, and reflects the analytic ordering produced by the scoring procedure.

#### 6.1.2. Scenario 2: RF jamming (availability denial)

**Scenario description.** The attacker raises the RF noise floor or saturates receiver front-ends to degrade or deny GNSS reception and/or C2/telemetry communications. The objective is loss of availability, forced failsafe activation, reduced situational awareness, or mission termination. Even short disruptions can cascade into safety or control instability depending on mission phase and system configuration.

**Static architectures.** Static configurations typically cannot adapt to time-varying interference. If jamming affects GNSS, the platform may lose fix and enter failsafe logic; if C2 is affected, control link loss may trigger mission abort or return-to-home behaviors. While these responses may be safety-oriented, they may not be resilient - they can be predictable, exploitable, or operationally suboptimal under adversarial intent.

**Layered defense models.** Layering improves observability (link-quality monitoring, anomaly alarms) and can incorporate operational mitigations (procedural fallback, redundancy). However, under strong jamming, many cyber controls become irrelevant because the dominant failure mode is availability loss. The practical limitation is that layered cyber security does not substitute for communications resilience under electromagnetic denial, and response effectiveness depends on whether resilience mechanisms are coordinated and mission-aware.

**Adaptive/risk-informed approaches (proposed framework).** The framework treats jamming as a disruption-dominant condition and supports escalation to response states prioritizing continuity of essential control. In S1 (triggered when RSSI degrades more than 15 dB from baseline), the system increases monitoring and validation; in S2 (triggered by C2 link loss exceeding 3 seconds), it shifts to resilience actions with proportionality driven by mission phase and resource margin. This approach is structurally better aligned with contested environments, focusing on sustaining safe behavior rather than assuming connectivity can be preserved.

#### 6.1.3. Scenario 3: hybrid combination (spoofing + jamming or spoofing + DoS)

**Scenario description.** The attacker combines deception and disruption to amplify effects. A representative pattern is GNSS spoofing to misdirect the UAS while jamming or DoS suppresses recovery channels, operator verification, or corrective updates. This hybrid approach increases uncertainty, delays diagnosis, and can push the system into unsafe or mission-compromising states.

**Static architectures.** Static controls are particularly limited under hybrid conditions because they typically address a subset of properties (e.g., C2 authenticity) without coordinating availability and navigation-integrity

management. Hybrid attacks can bypass protected elements by shifting the effective attack surface to what remains unprotected or non-adaptive.

**Layered defense models.** Layered controls improve coverage and may detect elements of the hybrid pattern. The recurring limitation is coordination: multiple alerts can occur simultaneously (navigation anomalies combined with link degradation), while response actions may conflict (e.g., reliance on GNSS-based return-to-home during GNSS deception). Without an explicit state-based orchestration logic, layered defenses risk delayed or inconsistent operational responses.

**Adaptive/risk-informed approaches (proposed framework).** The proposed framework is explicitly designed for hybrid alignment (Section 5.1). Its analytic advantage is not simply more controls, but coherent response selection: disruption and deception signals are jointly interpreted through explicit thresholds, risk is assessed proportionally, and state transitions provide a traceable mechanism for prioritizing safe control authority when trust is degraded. Under hybrid escalation, two or more simultaneous S1-level indicators trigger S2, supporting conservative acceptance policies and resilience actions that avoid unsafe reliance on untrusted navigation while preserving mission survivability where feasible. This advantage is assessed within the defined scoring framework and has not been experimentally validated.

### 6.2. Discussion: implications for defense resilience

The structured assessment indicates that hybrid cyber-electromagnetic threat readiness is primarily determined by whether a security posture can coordinate integrity and availability management rather than optimizing only one dimension. In defense-relevant environments, resilience depends on maintaining essential control functions even when navigation trust is degraded or communications are intermittently denied. This suggests that security should be treated as a mission-continuity capability, not only a preventive control layer.

A second implication is that layered defense, while necessary for broad coverage, does not automatically translate into operational resilience unless there is an explicit mechanism converting detection into timely and mission-compatible response. Under hybrid escalation, multiple alerts and degraded signals can increase ambiguity and delay decisions; therefore, pre-defined state-based response logic with explicit thresholds (Section 5.4) becomes a practical requirement for controllability and accountability.

Finally, the adaptive/risk-informed framework provides analytic value because it introduces proportional escalation and a clear operational posture under uncertainty (Elevated state S1) and under strong evidence of disruption or deception (Defensive/Resilient state S2). This improves interpretability and supports defense planning by enabling consistent reasoning about when to restrict autonomy, when to prioritize survivability over mission goals, and how to avoid unsafe reliance on untrusted navigation during contested operations. It should be emphasized that these advantages are inferred from the structured assessment procedure and require experimental or simulation-based validation before claims of empirical superiority can be supported. These implications directly motivate the conclusions, limitations, and future work in Section 7.

## 7. Conclusions, limitations and future work

### 7.1. Conclusions

This paper examined cyber and electronic warfare threats to unmanned aerial systems (UAS) through a theoretical-analytical and comparative approach, with emphasis on communications, command-and-control, and GNSS-based navigation dependencies, and with primary applicability to small-to-medium tactical UAS relying on MAVLink-based communication. The analysis indicates that hybrid cyber-electromagnetic conditions amplify risk by combining disruption and deception, often targeting the weakest dependency link rather than a single subsystem.

The paper makes three explicit contributions. First, a structured five-dimensional threat taxonomy was constructed and extended to cover hybrid cyber-electromagnetic combinations as a distinct high-priority threat

class. Second, a formalized five-criterion weighted scoring procedure was introduced to compare security postures in a reproducible manner; the weighted decision matrix (Table 1) shows that static architectures (2.20/5.00) offer high resource efficiency but very low responsiveness to hybrid conditions, layered defenses (2.90/5.00) improve coverage at the cost of integration sensitivity, and adaptive/risk-informed approaches (3.65/5.00) show the strongest analytic alignment with contested environments, driven by their advantage on the two highest-weighted criteria. Third, a state-based resilience framework with explicit indicator-driven transition thresholds was formalized, providing a specification directly usable for implementation planning.

Overall, the study argues that resilience-driven and adaptive principles show stronger conceptual alignment with hybrid threat realities than fixed protection strategies, particularly where communication availability and navigation trust cannot be assumed. This conclusion is grounded in structured analytic assessment rather than empirical evidence, which is the primary limitation of the present work.

### 7.2. Limitations

The study is limited by its non-empirical nature. The comparative claims are derived from structured synthesis of existing literature and analytical reasoning rather than experimental measurements or operational datasets. The five-point scoring scale is based on qualitative assessment of the literature; while it provides a reproducible and transparent framework, the assigned scores represent structured judgment rather than measured data, and different weighting schemes could alter the comparative ordering of approaches. Scenario-based assessment, while useful for consistent reasoning about hybrid effects, cannot quantify detection performance, false-alarm rates, or resource overhead under specific platform constraints. The indicator thresholds proposed in Section 5.4 are reference baselines for conceptual illustration; their calibration for specific platforms would require empirical testing. Additionally, the analysis abstracts across heterogeneous UAS architectures within the defined small-to-medium tactical class; implementation feasibility and assurance effort may vary significantly across platforms, mission profiles, and integration ecosystems.

### 7.3. Future work

Future research should validate the proposed framework using simulation and/or controlled testbed studies that combine GNSS spoofing, RF jamming, and cyber intrusion patterns under realistic operational constraints. A priority direction is to evaluate the indicator thresholds proposed in Section 5.4 against real platform data, refine the scoring procedure using expert elicitation or Delphi-style methodology, and assess how uncertainty and ambiguous signals affect response timing and safety. Further work is needed on interoperability and assurance, including how state-based response policies can be integrated across UAV-GCS ecosystems, standardized for broader adoption, and aligned with lifecycle security and certification practices such as EASA AMC 20-42 [6]. Extending the framework to MALE/HALE class systems and to platforms with hardware security modules would also be a valuable direction.

### Funding information

No funding was received from any financial organization to conduct this research.

### Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

### References

[1] N. Bai, X. Hu, and S. Wang, "A survey on unmanned aerial systems cybersecurity," Journal of Systems Architecture, vol. 156, p. 103282, Nov. 2024, https://doi.org/10.1016/j.sysarc.2024.103282.

[2] Z. Wang, Y. Li, S. Wu, Y. Zhou, L. Yang, Y. Xu, T. Zhang, and Q. Pan, "A survey on cybersecurity attacks and defenses for unmanned aerial systems," Journal of Systems Architecture, vol. 138, p. 102870, May 2023, https://doi.org/10.1016/j.sysarc.2023.102870.

[3] S. Z. Khan, M. Mohsin, and W. Iqbal, "On GPS spoofing of aerial platforms: A review of threats, challenges, methodologies, and future research directions," PeerJ Computer Science, vol. 7, Art. no. e507, 2021, https://doi.org/10.7717/peerj-cs.507.

[4] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," Proceedings of the IEEE, vol. 104, no. 6, pp. 1258–1270, Jun. 2016, https://doi.org/10.1109/JPROC.2016.2526658.

[5] P. Tedeschi, G. Oligeri, and R. Di Pietro, "Leveraging jamming to help drones complete their mission," IEEE Access, vol. 8, pp. 5049–5064, 2020, https://doi.org/10.1109/ACCESS.2019.2963105.

[6] European Union Aviation Safety Agency (EASA), "AMC 20-42 Airworthiness information security risk assessment," 2023. [Online]. Available: https://www.easa.europa.eu/. [Accessed: 23-Feb-2026].

[7] MAVLink Developer Guide, "Message signing (authentication)," [Online]. Available: https://mavlink.io/en/guide/message_signing.html. [Accessed: 24-Feb-2026].

[8] S. E. Meheretu, E. Nigussie, G. B. Gebremeskel, and S. Y. Hailesilassie, "A systematic literature review on spoofing and jamming approaches in unmanned aerial vehicles navigation," Journal of Aerospace Technology and Management, vol. 17, Art. no. e3425, 2025, https://doi.org/10.1590/jatm.v17.1396.

[9] ArduPilot Copter Documentation, "MAVLink2 signing," [Online]. Available: https://ardupilot.org/copter/docs/common-MAVLink2-signing.html. [Accessed: 24-Feb-2026].

[10] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in Proc. 18th Int. Conf. Evaluation and Assessment in Software Engineering (EASE), London, U.K., May 2014, https://doi.org/10.1145/2601248.2601268.

[11] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks," Ad Hoc Networks, vol. 133, Art. no. 102894, Aug. 2022, https://doi.org/10.1016/j.adhoc.2022.102894.

[12] Y.-M. Kwon, J. Yu, B.-M. Cho, Y. Eun, and K.-J. Park, "Empirical analysis of MAVLink protocol vulnerability for attacking unmanned aerial vehicles," IEEE Access, vol. 6, pp. 43203–43212, Aug. 2018, https://doi.org/10.1109/ACCESS.2018.2863237.

[13] S. Jeong, E. Park, K. U. Seo, J. D. Yoo, and H. K. Kim, "MUVIDS: False MAVLink injection attack detection in communication for unmanned vehicles," in Proc. NDSS Workshop on Automotive and Autonomous Vehicle Security (AutoSec), 2021, https://doi.org/10.14722/autosec.2021.23036.

[14] H. Xi, L. Ru, J. Tian, B. Lü, S. Hu, W. Wang, H. Wang, and X. Luan, "Enhanced cybersecurity framework for unmanned aerial systems: A comprehensive STRIDE-model analysis and emerging defense strategies," IET Information Security, Art. no. 9637334, Aug. 2025, https://doi.org/10.1049/ise2/9637334.

[15] R. Mustafovski, A. Risteski, and T. Shuminoski, "Designing a secure communication framework for UAV-to-TOC operations in military and emergency environments," ETIMA, vol. 3, no. 1, pp. 349–357, 2025, https://doi.org/10.46763/ETIMA2531349m.

[16] T. Wisanwanichthan and M. Thammawichai, "A lightweight intrusion detection system for IoT and UAV using deep neural networks with knowledge distillation," Computers, vol. 14, no. 7, p. 291, 2025, https://doi.org/10.3390/computers14070291.

[17] A. Khanfor, R. Hamadi, N. Lasla, and H. Ghazzai, "AI-driven intrusion detection for UAV in smart urban ecosystems: A comprehensive survey," arXiv preprint arXiv:2601.19345, Jan. 2026, [Online]. Available: https://arxiv.org/abs/2601.19345. [Accessed: 25-Feb-2026].

[18] K. Rados, M. Brkic, and D. Begusic, "Recent advances on jamming and spoofing detection in GNSS," Sensors, vol. 24, no. 13, p. 4210, 2024, https://doi.org/10.3390/s24134210.

[19] A. Montaruli, R. Patriarca, and D. Taurino, "How cyber-resilient are unmanned aircraft systems? A systematic meta-review," Aerospace, vol. 13, no. 2, p. 150, 2026, https://doi.org/10.3390/aerospace13020150.

[20] A. Allouch, O. Cheikhrouhou, A. Koubaa, M. Khalgui, and T. Abbes, "MAVSec: Securing the MAVLink protocol for Ardupilot/PX4 unmanned aerial systems," in Proc. 15th IEEE Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), Tangier, Morocco, Jun. 2019, pp. 621–628, https://doi.org/10.1109/IWCMC.2019.8766667.

[21] J. A. Betancourt, R. Romero-Alvarez, D. Krishnamurthy, K. Heimerl, and E. Zheleva, "A survey of security challenges and solutions for UAS traffic management (UTM) and small unmanned aerial systems (sUAS)," arXiv preprint arXiv:2601.08229, Jan. 2026. [Online]. Available: https://arxiv.org/abs/2601.08229. [Accessed: 02-May-2026].