SoK: The Cyber Attack Surface of Unmanned Vehicles (UxVs)

Alessandro Cantelli-Forti
RaSS National Laboratory, CNIT
Pisa, 56124, Italy
Email: alessandro.cantelli.forti@cnit.it

Hosam Alamleh
University of North Carolina Wilmington
Wilmington, NC 28403, USA
Email: alamlehh@uncw.edu

***Abstract*—Unmanned X-Vehicles (UxVs)—aerial, ground, surface, and underwater—share architectural patterns and a rapidly expanding cyberattack surface, yet the evidence base remains fragmented across platforms and operating environments. This Systematization of Knowledge (SoK) maps that surface using a two-axis lens: communication contexts (GCS-to-UxV, UxV-to-UxV, UxV-to-infrastructure, and UxV-to-satellite) and lifecycle phases (pre-deployment, operational, and post-deployment). We catalog concrete attack classes, including jamming, spoofing, replay/injection, machine-in-the-middle, and supply-chain or maintenance-stage compromise, and systematize their observable indicators. We identify cross-cutting patterns, highlight emerging themes, identify research gaps, and categorize detection signals associated with these attacks. We also release a reusable artifact—a taxonomy, coded corpus, and indicator catalog with detection-evaluation templates—to support reproducible, cross-modal assessment of UxV attack detection. This SoK excludes remediation and defense design and focuses on attacks, indicators, and detection.**

***Index Terms*—Unmanned Vehicles, Unmanned X-Vehicles (UxV); Cyber-Attack Surface; Communication Security; Lifecycle-Aware Security; Threat Indicators; Intrusion Detection; Security Taxonomy; Systematization of Knowledge**

1. Introduction and Scope

Unmanned systems — encompassing Unmanned Aerial (UAV), Surface (USV), Ground (UGV), and Underwater Vehicles (UUV) — collectively referred to as UxVs, are rapidly transforming modern defense, industrial, and civilian operations. These platforms rely on complex multi-domain communication architectures that integrate radio-frequency (RF), satellite, optical, acoustic, and tethered links to maintain command, control, and situational awareness across diverse environments. As autonomy and connectivity increase, so does the attack surface, exposing these systems to cyber, electronic warfare, and supply-chain threats across their entire lifecycle — from design and deployment to mission operation and post-mission data handling.

The research landscape remains fragmented: most work treats single platforms, channels, or lifecycle phases in isolation, so we lack a unified view of how attacks, observable indicators, and detection methods relate across UxV systems. There is currently no cross-domain, lifecycle-aware mapping that shows what is detectable on which communication surfaces, or where visibility gaps persist.

This Systematization of Knowledge (SoK) addresses that gap by jointly analyzing attacks, indicators, and detection techniques along two dimensions: (1) the communication interfaces linking UxVs to their environment, and (2) the lifecycle stages where those interfaces are exposed, trusted, or adversary-controlled. This communications-by-lifecycle view consolidates scattered results and highlights where detection capabilities are dense versus understudied. We do not survey defense designs as a primary target; when included studies report mitigations or countermeasures, we record them only as supporting context linked to the corresponding attack classes and observable indicators.

The core challenge is not the lack of individual detectors, but the lack of a comprehensive mapping from attack to indicator to detection over the UxV attack surface. By structuring evidence around communication surfaces and their changing trust assumptions, this SoK makes observability gaps explicit and points to the most impactful directions for improving monitoring and verification.

1.1. Motivation and Problem Statement

UxVs must maintain their communication links in challenging and often harsh environments. Control, sensing, and payload functions depend on links that may have low bandwidth, unstable coverage, or high noise. These limits make it hard to apply standard security mechanisms and force trade-offs between security, delay, autonomy, and mission safety.

A key challenge is that communication links are tied to decision logic, mission plans, and fail-safe modes across the whole lifecycle. A fault or attack on one link (for example, timing, synchronization, or signal quality) can push the system into an unexpected state or open a path to other interfaces. Security risks also appear before and after missions: setup, updates, repair, and data handling use different trust settings and tools, but are rarely analyzed in a consistent way.

The problem we address is the lack of a clear mapping from **lifecycle phase** (pre-deployment, operational, post-deployment) to **communication channel** (wired, wireless, tethered, optical, acoustic), to **attack type**, to **attack indicators**, and to **attack detection** methods. Without this mapping, it is hard to compare attack observability and detection evidence across platforms, or to know whether

reported indicators remain useful under poor link conditions, during handovers, or when attackers target non-operational phases.

This SoK builds such a mapping and uses it to: (i) organize known attacks, indicators, and detection methods by lifecycle phase and channel; (ii) extract common patterns and emerging themes; and (iii) identify research gaps.

2. Methodology

This SoK follows a structured and reproducible methodology to consolidate fragmented research on cybersecurity across Unmanned Systems (UxVs). The objective is to identify, classify, and analyse publications and documented incidents to reveal patterns, gaps, and trends characterising the security posture of UxV communication infrastructures throughout their lifecycle.

2.1. Search strategy

We adopted a two-stage collection strategy combining a structured database search (primary source) with cross-database validation and snowballing (secondary sources). Scopus served as the **primary corpus engine** due to its expressive Boolean syntax, consistent metadata model, and support for reproducible filters (`SUBJAREA`, `DOCTYPE`) required for a security-focused SoK.

Primary database (Scopus). We executed one core security query (Q1) and three recall boosters (RB1–RB3) targeting protocol-, communication-, and GNSS-level vulnerabilities. Queries were restricted to `SUBJAREA = ENGI, COMP` and `DOCTYPE = cp, ar, re`, thereby excluding non-technical domains and non–peer-reviewed items. Full query strings and filters are included in Annex A. Combined retrieval prior to deduplication yielded **3 390 records**, resulting in **2 935 unique studies** after DOI- and title-level deduplication.

Cross-database validation (IEEE Xplore, ACM DL, WoS). We queried additional scholarly databases to confirm that no major families of UxV–security studies were absent from Scopus. Missing structured filters, inconsistent metadata, and high-variance retrievals (often $>10\,000$ hits per query) dominated by robotics, perception, and control papers prevented reproducible filtering or export. These databases were therefore used exclusively for **coverage validation**. No security-relevant work identified in these checks was absent from the Scopus corpus.

Grey literature. Grey sources (e.g., NVD/CVE entries, CISA/ICS advisories, vendor documentation) were examined qualitatively to identify attack classes potentially absent from peer-reviewed work. These sources informed context and terminology but were not added numerically to preserve replicability. Additional details and pointers to key documents are provided in Annex D.

Snowballing. Backward and forward snowballing was applied to all studies retained after title/abstract screening. Forward snowballing (via Scopus) captured citing works potentially missed due to database-specific indexing. All studies identified through snowballing underwent the same eligibility assessment and met all inclusion criteria.
Full query strings, recall boosters, filters, merging logic, and replicability details are provided in Annex A.

2.2. Eligibility criteria

Studies were eligible if they: (i) focused on UxV cybersecurity or on security-relevant components of their compute, communication, or sensor stack; (ii) provided a clear threat model and/or empirical evidence through prototype, measurement, or evaluation; (iii) were published in peer-reviewed venues in security, robotics, or cyber-physical systems, or constituted authoritative technical reports; and (iv) examined technologies, protocols, or subsystems commonly deployed in UxV architectures.

We excluded studies limited to non-security perception or planning, purely social or ethical analyses, general automotive security without unmanned operation, and non-English or non–full-text items when adequate substitutes existed.

2.3. Screening and study selection

Screening followed a two-stage process. First, all $2\,935$ deduplicated records underwent title/abstract review, yielding $1\,035$ exclusions. Remaining records were labelled include, exclude, or *uncertain* when title/abstract information was insufficient for a decision.

Uncertain records (16) were retrieved and assessed in full text. Fifteen met all criteria and were retained; one was excluded at the eligibility stage. This process yielded $1\,899$ studies for final synthesis. Disagreements were resolved by discussion until consensus was reached; a third reviewer was available for arbitration but was not required.

A PRISMA-style summary of identification, screening, eligibility, and inclusion is provided in Table 1.

2.4. Deduplication and reviewer agreement (Cohen's κ)

We deduplicated records by normalising DOIs, titles (case folding and punctuation removal), venues, and publication years, and applied fuzzy matching (token–set ratio) to identify cross-index near-duplicates. When multiple versions existed (e.g., preprint versus camera-ready), we retained the most complete and citable version.

Two reviewers independently conducted title/abstract screening using a three-label scheme (include, exclude, uncertain). Cohen's κ was computed on the binary subset (include/exclude), excluding all records labelled uncertain. Agreement was high ($\kappa \approx 0.98$), and disagreements were resolved through discussion following PRISMA-aligned procedures; a third reviewer was available but not required. Full numerical details, confidence intervals, and the 2×2 contingency table are reported in Annex B.

2.5. Data extraction and synthesis

From each included study we extracted: vehicle domain (UAV/UGV/USV/UUV); system component (C2 link, GNSS, sensors/actuators, middleware—ROS/ROS 2, MAVLink, PX4/ArduPilot, in-vehicle networks, backhaul—SATCOM/4G/5G); attack vector and adversary goal (confidentiality, integrity, availability, safety impact); evaluation setup (simulation, laboratory, or field); and any

TABLE 1. PRISMA-STYLE SELECTION SUMMARY.

Identification	
Records identified (database search)	3390
Deduplication	
Records after deduplication	2935
Screening	
Records screened (title/abstract)	2935
Records excluded (title/abstract)	1035
Eligibility	
Reports sought for retrieval (full text)	16
Reports not retrieved	0
Reports assessed for eligibility (full text)	16
Reports excluded after full text	1
Included	
Studies included in the final synthesis	1899

mitigations or countermeasures reported alongside the attack. Extracted elements were mapped to our taxonomy (communication medium $\times$ lifecycle phase) and synthesised into cross-domain patterns, recurring attack classes, and research opportunities. Full extraction fields and the corresponding codebook are provided in Annex C.

2.6. SoK Framework and Research Design

This SoK integrates structured screening with qualitative synthesis, following PRISMA principles [1] and prior SoK methodology [2]. The analysis proceeds through corpus construction, taxonomy development, and synthesis of attack surfaces, detection signals, mitigations, and open challenges across UxV domains.

2.7. Two-Dimensional Taxonomy Development

To capture the breadth and evolution of attack surfaces, a two-dimensional taxonomy was developed. The first dimension represents **communication methods**, encompassing both physical and logical channels used by UxVs, including wired, fiber-tethered, optical, acoustic, radio-frequency (RF), cellular/5G, satellite, and peer-to-peer swarm links. The second dimension represents **lifecycle phases**, reflecting when these channels are most exposed to attack. These phases include the *pre-deployment phase*, which covers manufacturing, provisioning, and maintenance activities prior to mission use; the *operational phase*, encompassing real-time mission activities such as control, telemetry, and payload communication; and the *post-deployment phase*, which involves data retrieval, forensics, and decommissioning following mission completion.

Each cell within the two-dimensional matrix captures representative *threats, indicators, mitigations, and research gaps*, enabling both vertical (within-phase) and horizontal (across-channel) analysis. This structure allows systematic comparison of how similar attacks manifest differently across physical media and mission stages.

2.8. Data Synthesis and Analysis

Collected studies were analyzed to identify recurring patterns in attack types, observable indicators, detection approaches, and failure modes. Each identified vulnerability was mapped to one or more communication channels and lifecycle phases. Cross-channel dependencies (e.g., RF $\rightarrow$ SATCOM handovers, or GNSS $\rightarrow$ control logic dependencies) were explicitly traced to expose cascading effects not isolated to a single medium. Findings were iteratively validated by comparing multiple domains (UAV, UGV, USV, UUV) to ensure cross-domain consistency.

2.9. Novel Viewpoint: Communications $\times$ Lifecycle as the Primary Lens

Traditional UxV security taxonomies group evidence by subsystem (e.g., navigation, middleware) or by attack class (e.g., spoofing, jamming). We instead elevate *communication channels* and *lifecycle phases* to be first-class axes and use their Cartesian product as the organizing principle for all coding and synthesis.

Why this matters. (i) **Cross-link coupling:** security choices on one channel (e.g., C2) routinely influence exposure on others (e.g., telemetry, backhaul), which subsystem-first views obscure. (ii) **Redundancy paradox:** multi-link designs meant for resilience often enable *downgrade steering* into weaker links or unauthenticated modes. (iii) **Phase sensitivity:** pre-/operational-/post-deployment phases change which channels are active and which assumptions hold (e.g., "trusted" maintenance ports), altering risk in ways attack-type taxonomies miss.

How we operationalize it. Each included study is coded into cells of a matrix *(channel, phase)*; attacks/defenses/metrics are attached to those cells. We then derive: (a) *cross-cutting patterns* as frequent or high-salience motifs spanning many cells; (b) *emerging themes* via temporal signals over cell counts and indicator/detection categories; and (c) *gaps* as low-evidence cells weighted by operational salience and evaluation maturity. This lens changes prior conclusions by centering link interdependence and by making lifecycle-conditional risk explicit.

2.10. Deriving Cross-Cutting Patterns, Emerging Themes, and Gaps

Coded corpus. All included studies are normalized into a machine-readable corpus (the companion file) with one row per study and schema fields for domain (UAV/UGV/USV/UUV), communication channel (RF/FSO/acoustic/tethered/cellular/Wi-Fi/LPWAN/SATCOM/GNSS), lifecycle phase (pre-/operational/post-deployment), attack class (eavesdropping, jamming, spoofing, injection, MITM, supply chain, etc.), defenses (prevention/detection/mitigation), evaluation setting (sim/lab/field), metrics (e.g., FPR/FNR, SNR, PER, latency, time-to-regain-control), standards/frameworks referenced, and year. Free-text notes capture nuances (assumptions, hardware, datasets).

2.10.1. Cross-cutting patterns. We extract patterns that recur across vehicles, channels, and phases with a mixed quantitative–qualitative approach:

1) **Co-occurrence mapping.** We build a bipartite incidence matrix M whose rows are *attack classes* and columns are *(channel, phase)* cells; M_{ij} counts studies supporting the pairing. We compute normalized association scores to highlight

disproportionately strong pairings and rank the top-k cross-cutting patterns.

2) **Multi-factor motifs.** We extend to tripartite tensors $T(\text{attack}, \text{channel}, \text{phase})$ and apply nonnegative tensor factorization to expose higher-order motifs (e.g., {GNSS, spoofing, operational} co-occurring with {UAV, safety-impact metrics}).

2.10.2. Emerging themes. We surface novel or accelerating ideas by combining temporal signals with qualitative synthesis:

1) **Time-series trend analysis.** Annualized frequencies per (attack, channel, phase) are detrended for corpus growth (per-year normalization). We flag themes with (i) statistically significant upward slopes (Theil–Sen), (ii) burst detection (Kleinberg), or (iii) sudden post-2022 inflections (change-point tests).
2) **Topic discovery and validation.** We apply lightweight topic modeling (e.g., contextual embeddings with clustering) to titles/abstracts and *defense descriptions*, then manually validate cluster labels. "Emerging" clusters must satisfy: recentness (median year ≥ 2022), dispersion across at least two UxV types or channels, and at least one field or lab study.
3) **Standards and ecosystem hooks.** We tag studies that reference standards (e.g., 802.11s/1609.2, Remote ID, EASA/FAA guidance). Themes linked to new or evolving guidance are highlighted as near-term *practice drivers*.

2.10.3. Gap analysis. We operationalize "gaps" as low-evidence or misaligned areas with clear operational importance:

1) **Coverage matrix.** We form a completeness heatmap over the Cartesian grid of *channel* $\times$ *phase* (rows) and *attack/defense classes* (columns). Cells with (i) zero studies or (ii) $<$ pth percentile after year-normalization are flagged as *under-studied*. We report absolute counts and recency (last-publication year).
2) **Evidence–risk misalignment.** For each cell, we estimate *risk salience* by combining (a) cross-domain citations/incident mentions in the notes and (b) dependency centrality (e.g., GNSS for timing across channels). Gaps where risk salience is high but evidence is sparse are prioritized.
3) **Evaluation shortfalls.** We mark cells where defenses exist but lack: (i) explicit threat models, (ii) common metrics (FPR/FNR, PER, latency, time-to-regain-control), or (iii) field validation. These are *method gaps*.
4) **Reproducibility and artifacts.** We identify topics with no public artifacts (datasets, traces, code) or missing parameterization details; these become *infrastructure gaps*.

Reviewer agreement and auditability. Two reviewers independently code a 10–20% calibration subset; disagreements are reconciled and the codebook refined before full extraction. We track Cohen's κ on key categorical fields (attack, channel, phase, defense).

TABLE 2. REPRESENTATIVE SURVEY PAPERS BY UXV TYPE

UxV Type	Representative Survey Papers
Unmanned Aerial Vehicles (UAVs)	[3]–[16]
Unmanned Ground Vehicles (UGVs)	[17]–[19]
Unmanned Surface Vehicles (USVs)	[20]–[22]
Unmanned Underwater Vehicles (UUVs)	[23], [24]

Outputs. We release: (i) the coded corpus; (ii) cross-cutting pattern tables with association scores and defense coverage; (iii) emerging-theme timelines and validated topic labels; and (iv) gap heatmaps and prioritized research agendas, including metric templates to close *method* and *infrastructure* gaps.

Reproducibility and Limitations All bibliographic sources and mappings are maintained in the references to ensure reproducibility and citation traceability. While this SoK provides a broad view of UxV cybersecurity research, it excludes proprietary military evaluations and classified threat intelligence due to obvious access restrictions.

3. Two-Dimensional Attack Surface Taxonomy

Building on the surveys in Table 2, this section introduces a two-dimensional taxonomy for UxV attack surfaces. The taxonomy is organized by *communication method* (wired, wireless, optical, acoustic, satellite) and *lifecycle phase* (pre-deployment, operational, post-deployment). In the subsections that follow, each lifecycle phase is examined in turn. For every phase, we describe the main communication methods used, the key threats on those links, typical attack indicators, available detection strategies. This structure supports direct comparison across UxV domains and channels, and sets up the cross-domain analysis in Section 4.

3.1. Pre-deployment Phase

The pre-deployment phase covers manufacturing, provisioning, firmware installation, calibration, and maintenance. UxVs in this stage use electrical wired links, removable media, and short-range wireless (Wi-Fi/Bluetooth) for test, configuration, and data transfer. Because these paths are often treated as "trusted," they create exposure: adversaries can use the same interfaces to implant malware or alter firmware before fielding. Critically, these links also carry mission staging; operators upload waypoints, geofences, payload schedules, and autonomy parameters over the very maintenance channels used for diagnostics. Any weakness therefore becomes a *mission-plan integrity* risk. This is amplified in remote, contested, or bandwidth-limited deployments where stable GCS connectivity is impractical and platforms operate semi-autonomously for extended periods [25]–[27]. Compromise at this stage (e.g., route edits, geofence changes, time-triggered behaviors, or payload manipulation) can yield unsafe trajectories, covert loitering, or data exfiltration during the mission. To reduce latent risk that

persists into operations, pre-deployment workflows require hardware attestation, cryptographic signing/verification of firmware and mission plans, and disciplined maintenance procedures. The specific communication methods (wired, removable media, and short-range wireless) are analyzed below and summarized in Table 3.

3.1.1. Wired and physical interfaces. such as USB, Ethernet, and serial connections, which are commonly used for firmware updates, mission parameter loading, or telemetry extraction. These channels are susceptible to *malicious firmware injection* [28], *rogue peripheral attacks*, or the use of *compromised cables* [29] to deliver payloads. Documented cases have shown how compromised maintenance laptops or counterfeit USB programming adapters can install backdoors into flight controllers or onboard computers, compromising system integrity prior to deployment [30]–[32].

Compromise on wired links often leaves clear traces. On the maintenance host, indicators include unexpected new USB device types, changes in VID/PID or serial for known programmers, repeated connect–disconnect cycles during flashing, or unexplained write attempts to system directories or tool logs. On the UxV, indicators include sudden firmware version changes, checksum or signature mismatches, secure-boot warnings, or booting into recovery/debug modes without a recorded maintenance action. Detection relies on measured boot and attestation: the flight controller or companion computer records hashes of firmware and key configuration blocks, which a trusted maintenance tool verifies before accepting mission plans or arming. Attestation frameworks and PUF-based roots of trust for drones [33]–[35] bind these measurements to device identity, making wired update paths auditable and harder to abuse.

3.1.2. Removable media. including SD cards, USB mass storage devices, and portable SSDs. These are frequently used during pre-deployment for *offline updates*, *mission-file transfer*, and *data loading* to onboard storage. While convenient in environments with limited connectivity, such media introduce a significant *supply-chain and maintenance-stage attack surface*. Infected or counterfeit drives can deliver malware that embeds within file systems, firmware update packages, or mission-plan directories. Even seemingly benign configuration files may be modified to include hidden payloads or command sequences that activate during or post-deployment. Documented campaigns have leveraged air-gapped media infection to compromise industrial and defense platforms, demonstrating the persistence of this vector [36], [37]. Malicious use of removable media often shows up as unexpected or hidden files, mission or configuration files changed without a logged edit, mismatched timestamps, or mission plans whose hashes/signatures no longer match the baseline. Detection treats all media as untrusted: scan before use, mount in read-only or sandboxed environments, and verify cryptographic hashes or signatures of firmware images and mission files before import, as emphasized in studies of malware in air-gapped systems [38].

3.1.3. Short-range wireless connections. are used for diagnostics and configuration, particularly in commercial or multi-domain UxVs. These channels expose systems to *unauthorized access*, *default credential exploitation*, or *firmware-over-the-air (FOTA) spoofing*. Poor authentication practices and unencrypted diagnostic channels have been demonstrated to allow adversaries to reflash control firmware or exfiltrate sensitive calibration data [39]. Abuse of short-range wireless links typically appears as unknown SSIDs or Bluetooth devices, unexpected pairing or association attempts, FOTA prompts outside scheduled maintenance, or configuration changes without a matching operator action. Detection focuses on limiting and monitoring these channels: enforcing strong, non-default credentials and mutual authentication, disabling unused debug interfaces, requiring signed firmware/configuration for any over-the-air update, and logging or alerting on anomalous pairing, association, or FOTA events [39].

Prior work related to pre-deployment is often not UxV-specific, instead is shared across adjacent embedded and industrial systems. It converges on three themes. *First, maintenance and update-chain integrity*: studies and practice notes (both UxV-specific and platform-agnostic) emphasize secure boot, signed firmware, and trusted maintenance hosts to prevent pre-fielding tampering over USB/Ethernet tools [40]–[42]. *Second, provisioning and pre-flight hardening*: guidance and assessments (technologies commonly used by UxVs, but applicable to UxV fleets) stress credential hygiene, configuration control, software provenance, and disciplined update procedures before mission use [39], [43]. *Third, mission-plan integrity*: works on route/waypoint uploads (UxV-specific) and planning systems (technologies used by UxVs) show that trip programming often occurs over the same maintenance links; without cryptographic signing/verification and independent on-vehicle validation, plans are susceptible to covert modification [44]–[46].

3.2. Operational

Operational communications encompass all data exchanges that occur once a UxV is deployed and actively performing its mission. These interactions form the core of the UxV's command, control, coordination, and situational awareness functions. As illustrated in **Figure 1** and summarized in Table 4, operational connectivity typically spans four principal link types: *UxV-to-Ground Control Station (GCS)* for command, telemetry, and payload data; *UxV-to-UxV* for cooperative behaviors and swarm coordination; *UxV-to-Infrastructure* for integration with terrestrial networks, edge nodes, or tactical relays; and *UxV-to-Satellite* for beyond-line-of-sight (BLOS) operations. Each link type carries distinct security, latency, and reliability constraints, collectively shaping the mission's resilience and trustworthiness. Each is discussed in its own subsection.

3.2.1. UxV to Ground Control Station. Communication between a UxV and its Ground Control Station (GCS) constitutes the primary operational channel for command, telemetry, and payload data. These links vary by modality (radio wireless, electronic wired, fiber-optic tethered, optical, acoustic, and hybrid) and each modality brings distinct performance tradeoffs and security considerations. While operators choose a link based on range, bandwidth, and

Channel	Typical Pre-deployment Use	Primary Exploit Vectors	Attack Indicators	Detection Approaches
Wired (USB / Ethernet / Serial)	Firmware flashing, calibration, log/telemetry extraction, mission-plan upload	Malicious firmware via compromised host [28]; BadUSB/rogue cable [47]; device impersonation (fake programmer) [48]; MITM on service tools [49]	Unexpected new USB device types; changes in USB VID/PID or serial for known programmers; repeated connect–disconnect cycles; sudden firmware version changes; checksum/signature mismatches; secure-boot warnings; boot into recovery/debug without recorded maintenance	Measured boot and attestation of firmware/configuration; verification of hashes/signatures before mission upload or arming; trusted maintenance hosts and device whitelisting; PUF-based roots of trust binding measurements to device identity [28], [33]–[35]
Removable Media (SD / USB Mass Storage)	Media offload, configuration transfer, offline updates	Infected media seeding payloads [36]; config/mission-file tampering [50]; covert exfiltration via hidden files [37]	Unexpected or hidden files/directories; mission or configuration files changed without logged edits; timestamps inconsistent with maintenance logs; mission plans whose hashes/signatures no longer match the baseline	Treat media as untrusted input; scan before use; mount in read-only or sandboxed environments; verify cryptographic hashes/signatures of firmware images and mission files before import; follow air-gapped malware-handling practices [36]–[38]
Short-range Wireless (Wi-Fi / Bluetooth)	App-based setup, diagnostics, quick file transfer, pairing	Rogue AP / evil-twin [51]; default/weak credentials [52]; FOTA spoofing or downgrade attacks [53]	New/unknown SSIDs or Bluetooth devices; unexpected pairing/association attempts; frequent re-association; FOTA prompts outside scheduled maintenance; unsigned/failed update checks; configuration changes without matching operator actions	Enforce strong, non-default credentials and mutual authentication; disable or rate-limit unused debug interfaces; require signed firmware/configuration for over-the-air updates; log and alert on anomalous pairing, association, and FOTA events [39], [53]

TABLE 3. PRE-DEPLOYMENT COMMUNICATION CHANNELS, EXPLOITATION PATHWAYS, ATTACK INDICATORS, AND DETECTION APPROACHES. INDICATORS ARE CONCISE CUES FOR STAGING-TIME DETECTION; PAIR WITH SIGNED FIRMWARE/MISSION FILES, TRUSTED MAINTENANCE HOSTS, HARDWARE ATTESTATION, AND AUDITED CHAIN-OF-CUSTODY.

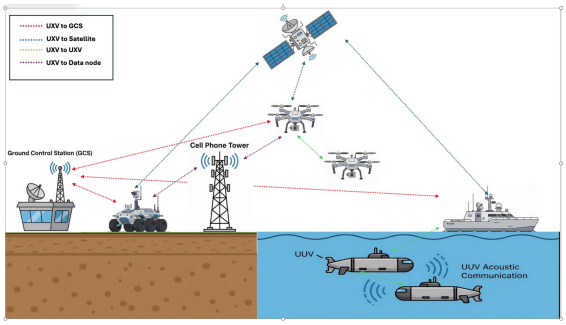

Figure 1. Representative operational communication architecture illustrating UxV-to-Ground Control Station (GCS), UxV-to-UxV, UxV-to-Infrastructure, and UxV-to-Satellite links. Each channel supports distinct command, coordination, or data exchange functions and exhibits unique bandwidth, latency, and security constraints.

environmental constraints, adversaries frequently exploit the modality-specific weaknesses of these channels to disrupt control, manipulate telemetry, or introduce malicious code or commands.

Radio Frequency (RF).
These links—spanning *sub-GHz ISM FHSS* telemetry (e.g., 433/868/915 MHz) [54], [55], *2.4/5.8 GHz Wi-Fi/OFDM* [56] and proprietary C2/video systems (e.g., DJI Lightbridge/OcuSync) [57], *licensed or SDR MANET/mesh* radios (802.11s/TDMA variants) [58], *LP-WAN* for low-rate telemetry (LoRa/FSK) terminals operating in L/S/Ku/Ka bands [59], which provide flexible, long-range connectivity but are especially exposed to over-the-air threats such as interception, jamming [60], [61], and spoofing [62], [63], which heavily covered in literature. An attacker that successfully mimics or injects into an RF control channel can present false telemetry, issue unauthorized commands, or force the UxV into unsafe behaviors; operational indicators of such activity include sudden increases in packet loss or error rates, inconsistent position or status reports, abnormal signal-strength or frequency changes, and unexpected re-association events with unknown transmitters [64], [65]. Detection mechanisms build directly on these indicators by monitoring packet loss, RSSI/CNR, association patterns, and traffic statistics against mission-specific baselines. Physical- and link-layer anomaly detectors, as well as ML-based IDS and jamming detectors for UAV networks, learn normal RF behaviour and flag deviations indicative of attacks on the control link, as shown in work on open-set attack detection and learning-based jamming detection in drone networks [66]–[68].

Tethered (Wired) Links
Physically tethered links (either electric tethers or hybrid power/data tethers with embedded fiber) deliver continuous power and remove energy-limited flight as a constraint, enabling persistent ISR and relay missions. Lab and field efforts demonstrate on the order of 1 kW over lightweight, high-voltage tethers for multirotors, supporting long-duration station-keeping and heavier payloads than battery-only sorties [69]. Surveys of tethered UAVs consistently note that the tether functions both as a power conduit and as a deterministic backhaul, simplifying link budgets and stabilizing control relative to contested RF [70] [71]. For command and video, fiber-optic tethers provide very high throughput with low, stable latency and are inherently immune to intentional RF interference because the signal is guided light rather than a radiated waveform; conventional RF jamming or spoofing does not affect this path. In underwater and subsea settings (where RF range is intrinsically limited) tethers (often fiber-bearing) have long been standard to achieve robust, high-rate telemetry over operational distances while simultaneously delivering power to UUVs [72] [73].

From a security standpoint, fiber links resist RF and electromagnetic interference but remain exposed at the physical layer. Optical networking work documents both intrusive and non-intrusive taps—controlled bends, evanescent coupling, and in-line splitters—that siphon optical power with minimal service disruption, as well as active in-line devices that can manipulate or degrade signals [74]. Measurements on Layer-1 components (connectors, splices, splitters) show these perturbations as insertion-loss changes, reflections, polarization shifts, or spectral artifacts [74]. Practical indicators include unexpected loss or SNR degradation, new/reflected events in OTDR traces, latency/jitter excursions beyond normal tolerances, and abnormal acoustic/strain signatures seen by distributed fiber sensing. Although direct access to a tether is often limited (especially for UAVs compared to UGVs or UUVs), risk persists wherever maintenance

access or exposed ground segments exist.

Overall, cabled or hybrid fiber-electric UxVs provide resilient, high-performance communications in RF-restricted or underwater environments, but still require physical-layer protections and condition-based monitoring to detect tampering, covert taps, or malicious in-line inserts; by design, tethers also constrain maneuverability and operational range, particularly in dynamic or confined environments. Detection builds on these indicators via continuous physical-layer monitoring: OTDR traces, received power, and polarization or spectral statistics are compared against a baseline to flag possible taps, bends, or in-line inserts [74]. Work on distributed optical fiber sensor perimeter systems with UAV video linkage and on jamming/insertion detection in optical UAV networks shows that distributed fiber sensing and pattern recognition over physical-layer features can reliably distinguish normal cable dynamics from deliberate tampering, and the same techniques can be applied to tether health and intrusion monitoring [75].

Wireless Optical

Optical free-space links (lasercom) deliver very high data rates with narrow beams that reduce unintended interception and are immune to RF jamming, but they remain vulnerable to pointing–acquisition–tracking (PAT) and atmospheric effects. Misalignment or tracking oscillations are common in mobile free space optical (FSO) and often trigger reacquisition cycles, making PAT a primary fragility in contested or dynamic scenarios [76], [77]. Adversaries can also saturate or "dazzle" receivers with directed light, temporarily blinding sensors and degrading SNR while raising BER without necessarily causing immediate outage [78]. Background illumination, especially solar noise at ground terminals, adds shot/thermal noise that lowers sensitivity and throughput, producing measurable daytime SNR/BER penalties [77]. Atmospheric turbulence induces scintillation, beam wander, and spreading, which in turn cause bursty fades, pointing jitter, and link dropouts unless mitigated (e.g., with adaptive optics or diversity) [79].

Beyond denial and degradation, weak encryption or link authentication enables injection and deception. Modulating-retroreflector (MRR) terminals (widely studied for small-platform lasercom) provide a mechanism by which a rogue terminal or retroreflector could impersonate a legitimate endpoint absent robust authentication [80], [81]. Optical-wireless security surveys likewise describe spoofing via substitution of a rogue optical source and emphasize the need for authentication [82]. Although FSO's narrow beams offer low probability of intercept, physical-layer analyses show that off-axis or geometrically positioned eavesdroppers can still capture energy and recover data; secrecy capacity depends on geometry, turbulence, and receiver placement [83], [84]. Consequently, despite electromagnetic interference immunity, resilient operation requires strong encryption and mutual authentication layered atop PAT robust designs and turbulence mitigation [85]. From a detection standpoint, attacks on FSO links leave characteristic physical-layer traces: jamming and dazzling appear as correlated SNR/BER spikes, sharp drops in received optical power, and frequent PAT reacquisition cycles under otherwise stable geometry, while turbulence-only conditions tend to follow slower or more predictable patterns. Recent work on jamming attack detection in optical UAV networks uses these measurements and learned classifiers to separate benign channel variation from deliberate interference, and similar schemes have been proposed for packet insertion detection in optical UAV networks by combining timing and sequence-number checks with cryptographic authentication [86], [87].

Acoustic

For UUV, acoustic communications are often the only practical long-range solution, whereas optical and RF links attenuate rapidly underwater; as a result, most operational systems rely on acoustics for range and robustness [88]. These channels, however, are vulnerable to jamming, replay, and signal-injection/spoofing attacks that exploit the propagation environment and protocol/decoder behavior [89], [90]. Typical indicators of acoustic interference include elevated ambient-noise levels accompanied by reduced delivery ratio and rising delays, anomalous propagation delays or Doppler signatures revealed by channel/feature monitoring, repeated malformed frames at the modem interface, and unexpected control events that correlate with local acoustic disturbances rather than operator inputs [88], [91], [92]. In practice, these indicators support detection based on joint monitoring of channel and modem features: UxVs can track ambient-noise level, delay/Doppler spreads, packet error rates, and modem error flags against mission-specific baselines to distinguish normal environmental variation from deliberate jamming or spoofing. Passive acoustic threat-detection schemes and countermeasure reviews for underwater unmanned systems show that combining such physical-layer features with simple classifiers or rule-based detectors can reliably flag anomalous acoustic activity and trigger link reconfiguration or fallback behaviors [93], [94].

Hybrid

Operational architectures that combine multiple modalities (hybrid RF/tether/optical configurations) seek resilience through redundancy but can also broaden the attack surface [95], [96]. Cross-channel manipulation [97], downgrade strategies that force a fallback to a weaker link [98], or coordinated multi-modal attacks can mask tampering on one channel by maintaining apparently normal behavior on another [99]. Detection in these systems hinges on cross-checking redundant telemetry, validating consistency across modalities, and flagging unauthorized fallback or divergence events [100].

3.2.2. UxV to UxV. Peer links among vehicles (air/-ground/surface/underwater) are prime targets for availability and integrity attacks because they carry neighbor discovery, consensus, and task-allocation traffic. RF jamming—barrage, tone, reactive, or protocol-aware—disrupts link establishment and flooding/consensus timing, triggering neighbor-set churn, MCS downgrades, and formation breakup; coordinated or mobile jammers exploit swarm geometry to maximize outage while minimizing radiated power [101], [102]. Route manipulation (blackhole/grayhole/selective forwarding) and control-plane spoofing force suboptimal paths, partition clusters, or starve leaders, often masquerading as congestion dynamics [103], [104]. Eavesdropping and traffic analysis against inter-UAV relays enable inference of roles and rendezvous points, while targeted cooperative

eavesdropping from elevated platforms leverages LoS to multiple peers [105].

Identity abuse undermines peer trust: Sybil attacks inject many forged nodes to bias voting, quorum, or formation anchoring; impersonation of high-value roles (leader/relay) corrupts scheduling and control dissemination [106]–[108]. On the physical layer, RF-fingerprinting evasion and spoofed PHY features (e.g., manipulated transients/constellations) defeat device-specific classifiers, enabling stealthy impostors even when upper layers are encrypted [109], [110]. Time-synchronization attacks (clock skewing, delay injection) desynchronize consensus and TDMA/FHSS schedules, amplifying packet collisions and causing split-brain formations.

At the control layer, Byzantine behaviors (malicious state broadcasts, falsified relative pose/velocity) and deception attacks on formation tracking push followers into oscillations or collision-risk trajectories; DoS on event triggers floods controllers with spurious updates to exhaust computation or bandwidth [111]–[113]. Cross-layer blends are common: a low-rate jammer that induces retransmissions can mask selective forwarding or wormhole tunnels used to reorder or delay consensus messages.

Finally, ML-enabled cooperation introduces adversarial ML threats: adversarial examples on vision/radar frames corrupt joint perception and target handoff; label-flipping/model poisoning during in-swarm updates biases detection and tracking models toward attacker-chosen errors; and triggered backdoors activate only under specific textures or viewpoints, degrading mission products without obvious link anomalies [114]–[116]. Across these vectors, observable footprints include PER/BER bursts aligned with attacker motion, inconsistent inter-vehicle geometry from falsified states, abnormal consensus latency/jitter, and abrupt neighbor-graph reconfigurations that do not match expected kinematics. These footprints support a range of detection mechanisms: swarm-focused IDS and sensing methods monitor PER/BER, neighbor-set evolution, spectrum features, and consensus residuals to distinguish normal mobility from jamming, route manipulation, or Byzantine behaviors [112], [117]. Recent work formulates "security situation assessment" and attack detection in UAV swarms as learning problems over link, traffic, and topology features, using deep models or reinforcement learning to flag communication and GPS-spoofing attacks in near real time [118], [119].

3.2.3. UxV to Infrastructure. UxV–infrastructure links leverage terrestrial networks and fixed assets cellular (LTE/5G/NR, incl. mmWave and IAB), Wi-Fi/WLAN, LPWAN (e.g., LoRa/LoRaWAN), public-safety/mission-critical systems, and edge/cloud nodes to extend range, backhaul payload data, and offload computation. These paths enable Beyond Visual Line of Sight (BVLOS) operations and high-throughput services but expose vehicles to attacks rooted in access-network procedures, handovers, and shared-spectrum contention, as well as to control-/user-plane abuse in virtualized cores and open radio access network stacks. Empirical campaigns and 3GPP studies on connected drones detail altitude driven interference patterns, atypical neighbor lists, and mobility behaviors that stress association, Radio resource control (RRC) state transitions, and uplink power control factors attackers can exploit to cause denial, downgrade, or interception [120]–[123]

On cellular links, over-the-air jamming of synchronization and control channels degrades attach, scheduling, and feedback; uplink jamming is particularly effective at altitude due to broader LoS to multiple cells. Rogue or misconfigured base stations can lure UxVs into unsafe handovers, force cipher/null-integrity fallbacks, or trigger re-attachment loops [121]. Network-side attacks amplify impact: PFCP/SMF abuse in the core can blackhole slices or starve Quality of service (QoS) bearers used by UxVs [124], while Radio access network integrated mobility/-control apps can be turned into denial vectors or policy downgrade levers [125]. Studies of Inter-Cell Interference Coordination (ICIC) and clustered-user scenarios show that forcing handover flapping or polluting the Channel Quality Indicator (CQI)/Channel State Information (CSI) around stadiums/emergencies can throttle command-and-control (C2) or video feeds [126], [127]. Passive attacks persist as well: measurement-based works demonstrate that off-axis capture and Reference Signal Received Power (RSRP)/Reference Signal Received Quality (RSRQ) fingerprinting at altitude can aid traffic classification or localization unless higher-layer protections are enforced [128], [129].

Wi-Fi/WLAN used as backhaul or facility access brings familiar infrastructure threats: evil-twin/rogue APs, deauth/disassoc storms, and captive-portal spoofing to inject payloads or siphon telemetry [130], [131]. LPWAN integration helps with low-rate telemetry and Remote ID but is fragile under interference and spreading-factor collisions; papers on LoRa/LoRaWAN-enabled UxVs discuss multi-user interference and spoofing potential when authentication and frame counters are weak [132], [133]. In hybrid Space–Air–Ground Integrated Network (SAGIN) designs and Integrated Access and Backhaul topologies, attackers can chain cross-domain effects, e.g., jam ground 5G to force satellite fallback, then degrade high-latency links enough to trip autonomy fail-safes [134]–[136].

Edge offload and cloud connectivity add software and supply-chain attack surfaces: poisoned model updates, slice misbinding, or API token abuse can compromise fleet behavior even when the RF link is healthy [137]–[139]. Infrastructure-centric defenses (beamforming, passive reflectors, robust handover policies) measurably improve aerial coverage and reduce interference, but also introduce new configuration dependencies that adversaries can target [106], [140], [141]

Operationally, compromise or interference on UxV–infrastructure links tends to surface as abnormal RRC churn, attach/hand-in failure spikes, CQI/CSI and RSRP/RSRQ volatility inconsistent with platform dynamics, bearer QoS downgrades or slice reassignments not requested by the GCS, sudden RTT/jitter excursions in otherwise stable backhaul, and repeated associations with unexpected cells/SSIDs. Correlating these symptoms with localized RF conditions, with control-plane anomalies, and with application-layer integrity checks is critical to discriminating contested spectrum from network-side abuse. In short, infrastructure links unlock scale and reach for UxVs, but their procedural richness expands the attack surface; resilient operation requires mutual authentication, encrypted C2/payload paths, strict

handover and cell-selection policies, anomaly-aware QoS/slice monitoring, and fallback logic that resists downgrade steering across cellular, Wi-Fi, LPWAN, and SAGIN tiers. On the detection side, many approaches treat the cellular and WLAN stack as a sensor: UxVs and ground systems monitor RRC state transitions, attach/handover failures, CQI/CSI, and RSRP/RSRQ statistics for deviations from learned baselines to flag jamming, unsafe handovers, or abnormal QoS changes. Jamming-specific methods for 5G-connected UAVs use feature extraction and deep models (e.g., PCA-enhanced Transformers or multi-stage detectors) to distinguish deliberate interference from normal channel variation on the infrastructure link [142], [143]. For LPWAN and Remote ID, fingerprinting and behavior-based techniques can detect misbehaving or spoofed nodes: for example, LoRa-based RF fingerprints for UAVs and misbehaving Remote ID detection frameworks build models of legitimate signal or trajectory patterns and raise alarms when observed identities or traffic diverge [144], [145].

3.2.4. UxV to Satellite. UxV–satellite links fall into two security-relevant classes: (i) navigation (GNSS/GPS) used for timing/position/velocity, and (ii) SATCOM used for beyond-line-of-sight (BLOS) command, telemetry, and payload data. Each faces distinct attack surfaces, symptoms, and defenses.

Navigation (GNSS/GPS)

GNSS links are exposed to deception (spoofing/meaconing, selective satellite forgery, slow "carry-off" biasing, swarm-aware coordinated attacks) and denial (broad-/narrowband jamming) that corrupt or suppress positioning, velocity and time (PVT) functions. Operational indicators include abnormal carrier-to-noise (C/No) trends that drift or drop without masking or maneuver; navigation-filter residual spikes alongside inconsistent Dilution of Precision; divergence between code and carrier, and across dual-frequency observables; angle-of-arrival patterns that contradict sky geometry on multi-antenna systems; unexpected disciplining of the local clock; and growing disagreement with independent references, sometimes coordinated across vehicles that should share common-mode error. These symptoms often co-occur with low-jerk solution "dragging," fix-mode flapping, frequent reacquisitions or constellation switches, and geofence/airspeed plausibility violations driven by navigation state rather than commanded motion [141], [146]–[152]. These symptoms are the basis for most GNSS attack detectors: signal- and receiver-level schemes monitor C/No, code–carrier divergence, dual-frequency consistency, and filter residuals against learned baselines or RAIM-like integrity thresholds to flag spoofing and jamming events [141], [146], [147], [151]. More recent work applies machine learning—e.g., LSTM and attention-based models over navigation residuals and C/No traces, or adaptive multi-feature fusion to separate benign dynamics from deception, and to classify attack types in real time on UAV platforms [148]–[150], [152].

SATCOM (BLOS C2 / Payload; incl. LEO NTNs)

SATCOM links face several concrete threats: attackers can jam the uplink or downlink, cause interference on the same or nearby channels, spoof the uplink, or hijack a session if control-plane authentication is weak. They can also eavesdrop if command/payload traffic is not properly encrypted, or compromise the terminal itself via unpatched modems, exposed management ports, or malicious configuration updates. Newer Low Earth Orbit (LEO) / Non-Terrestrial Network (NTN) features—such as beam hopping, frequent handovers, and mixed RF/free-space-optical backhaul add failure modes: attackers can force downgrades to weaker waveforms, trigger rapid handover "thrashing" under targeted interference, or exploit geometry to leak energy outside the main lobe (reducing low-probability-of-intercept/detect).

Operational signs of attack include sudden drops in Eb/No or C/No not explained by pointing or weather; bursty BER/FER while vehicle attitude and RF front-end temperatures are stable; repeated re-associations to beams/spots or gateways; control-plane resets or unexplained modem reboots; unexpected changes in waveform, coding, or power-control settings; uplink-only degradation (a hallmark of targeted uplink jamming); management-plane access from unknown IPs or certificates and failed signature checks on configs/firmware; outages that align with local interference reports rather than vehicle dynamics; mismatches between SATCOM-reported position/beam geometry and independent GNSS/INS; and latency/jitter spikes that do not match routing changes or satellite visibility windows [105], [135], [153]–[157]. Detection on SATCOM links therefore combines physical-layer monitoring with control-plane checks. At the waveform level, anti-jamming schemes for satellite–UAV MIMO and integrated satellite–terrestrial networks estimate interference subspaces, SINR, and BER patterns to detect and localize jammers before applying beam, power, or routing adaptations [158]–[160]. At the protocol level, access and handover authentication mechanisms for UAV-aided satellite–terrestrial integration networks validate beam/spot changes and gateway switches using cryptographic tokens and context information, allowing rogue or misconfigured satellite/ground nodes to be detected and rejected during mobility procedures [161].

3.3. Post-Deployment

The *communication channels* involved after mission completion are the same as in pre-deployment (wired, removable media, short range wireless). What changes is the *threat posture*: interactions during recovery, data offload, and maintenance can be abused to pivot from the UxV into ground assets or to extract/weaponize on-vehicle secrets if the asset is seized.

3.3.1. UxV returns to the GCS. When a vehicle lands and connects for post-mission data offload—over USB/Ethernet/serial, with removable media (SD/USB), or via on-prem Wi-Fi/Bluetooth—the trust boundary flips: the UxV can now threaten the GCS. Real risks include malware hidden on removable media that executes when ingest tools parse files [36], [37]; BadUSB-style device impersonation from compromised onboard ports or in-line adapters that show up as HID/composite peripherals [29], [47], [49]; protocol-level injection on maintenance links when telemetry/config exchanges are unsigned or tools (e.g., MAVLink utilities) are vulnerable [50], [62];

Link Group	Channel / Medium	Typical Operational Use	Primary Exploit Vectors	Attack Indicators	Detection Approaches
UxV↔GCS	**RF (sub-GHz FHSS, 2.4/5.8 GHz Wi-Fi/OFDM, MANET/mesh, LPWAN)**	Command/telemetry; video; Remote ID / low-rate telemetry	Jamming/denial [60], [61]; protocol spoofing/injection (e.g., MAVLink) [62], [63]; eavesdropping on weak/absent crypto; rogue SSID/bind and re-association abuse [64], [65]	PER/packet-loss spikes; sudden RSSI/CNR anomalies; inconsistent position/status frames; frequent re-associations with unknown transmitters; unexpected MCS/rate downgrades [64], [65]	Link/RF monitoring against mission-specific baselines (loss, RSSI/CNR, association history); physical-/MAC-layer anomaly detection and ML-based IDS or jamming detectors for UAV networks that learn normal RF behaviour and flag deviations [66]–[68]
	Tethered (wired / fiber-optic)	Deterministic C2/video backhaul; continuous power (tethered UAV/USV/UUV)	Physical taps / in-line inserts (bends, evanescent coupling, splitters); connector/splice manipulation [74]	Unexplained insertion-loss/SNR drop; new/reflected events in OTDR traces; latency/jitter excursions; abnormal acoustic/strain signatures along the cable [74]	Continuous physical-layer monitoring (OTDR, received power, polarization/spectral statistics) against baseline traces; distributed fiber sensing and pattern recognition to distinguish normal cable dynamics from deliberate tampering or intrusion [74], [75]
	Wireless Optical (FSO / lasercom)	High-rate payload backhaul; LPI/LPD C2	Receiver dazzling/saturation; PAT mis-tracking [76]–[78]; spoofed terminals/retroreflectors under weak auth [80], [82]; off-axis eavesdropping [83], [84]	Abrupt SNR drops and BER bursts; frequent PAT re-acquisitions or oscillations; unexplained pointing offsets; link dropouts tied to localized optical emissions/atmospherics rather than platform motion [76], [77]	Physical-layer feature monitoring (received optical power, SNR/BER, PAT state) with thresholding or learned classifiers to separate turbulence from deliberate jamming/dazzling, plus sequence/timing checks and cryptographic authentication to detect packet insertion or endpoint spoofing [86], [87]
UxV↔UxV (peer / swarm)	**Ad-hoc/FANET (RF; FSO occasional; acoustic underwater)**	Formation/consensus; cooperative sensing; relay; task allocation	RF jamming and route manipulation (blackhole/grayhole) [101]–[104]; Sybil/identity abuse and weak group authentication [106]–[108]; PHY-auth/RF-fingerprinting evasion [109], [110]; Byzantine control messages and adversarial ML on shared models [111], [113], [114]	PER/BER bursts aligned with attacker motion; neighbor-set churn and partitioning; inconsistent inter-vehicle geometry or relative states; abnormal consensus latency/jitter; sudden topology changes that do not match expected kinematics	Swarm-focused IDS that monitors PER/BER, neighbor evolution, spectrum features, and consensus residuals; "security situation assessment" using deep models or RL on link/-traffic/topology features to flag jamming, route manipulation, and spoofing in near real time [112], [117]–[119]
UxV↔ Infrastructure	**Cellular (LTE/5G/NR), Wi-Fi/WLAN, LPWAN**	BVLOS backhaul; MEC/edge offload; facility/enterprise access; Remote ID	Cellular sync/control-channel jamming; rogue/misconfigured base stations and unsafe handovers [121]; core-side PFCP/slice abuse and ORAN/edge-app misuse [124], [125]; Wi-Fi evil-twin/deauth/captive-portal spoofing [130], [131]; LPWAN interference and spoofing when auth/frame counters are weak [132]	Abnormal RRC churn; attach/hand-in failure spikes; CQI/CSI and RSRP/RSRQ volatility inconsistent with vehicle dynamics; bearer QoS downgrades or slice reassignments not requested by the GCS; repeated associations with unexpected cells/SSIDs; RTT/jitter excursions on otherwise stable backhaul	Treat cellular/WLAN stack as a sensor: monitor RRC events, CQI/CSI, and RSRP/RSRQ against baselines to flag jamming, unsafe handovers, or suspicious QoS/slice changes; UAV-specific jamming detectors using feature extraction and deep models for 5G links [142], [143]; RF fingerprinting and behaviour-based methods for LPWAN/Remote ID to spot spoofed or misbehaving nodes [144], [145]
UxV↔ Satellite	**SATCOM (BLOS C2 / payload; incl. LEO/NTN)**	Beyond-LOS command/telemetry; payload backhaul	Uplink/downlink jamming or adjacent-channel interference; session hijack under weak control-plane auth; modem management compromise; forced waveform/downgrade via interference or misconfiguration [135], [153], [154], [157]	Eb/N_0/C/N_0 depressions not explained by pointing/weather; BER/FER bursts; repeated beam/gateway re-associations; unexplained modem reboots or config changes; uplink-only impairment; latency/jitter spikes that misalign with routing or visibility	Physical-layer anti-jamming for satellite–UAV and satellite–terrestrial networks that estimate interference subspaces, SINR, and BER patterns to detect/localize jammers and drive beam/power/routing adaptation [158]–[160]; access and handover authentication schemes that validate beam/spot and gateway changes with cryptographic tokens and context to exclude rogue/misconfigured nodes [161]
	GNSS (Navigation/Timing)	Timing/position/velocity for control, geofencing, and timebase	Spoofing/meaconing/carry-off; broad/narrowband jamming [146]–[148]	Abnormal C/No trends; navigation-filter residual spikes; HDOP/PDOP anomalies; code–carrier and dual-frequency inconsistencies; AoA contradictions on multi-antenna systems; divergence from INS/visual odometry or fleet-common references	Integrity and RAIM-like schemes that monitor C/No, residuals, and multi-frequency consistency against thresholds or learned baselines to flag spoofing/jamming [141], [146], [147], [151]; ML-based detectors (LSTM/attention and multi-feature fusion) over residuals and C/No traces to distinguish benign dynamics from deception and classify attack types on UAV platforms [148]–[150], [152]

TABLE 4. OPERATIONAL COMMUNICATION CHANNELS AND EXPLOITATION PATHWAYS. *UxV↔GCS* NESTS RF, TETHERED, AND WIRELESS OPTICAL; *UxV↔Satellite* NESTS SATCOM AND GNSS. COLUMNS SEPARATE TYPICAL OPERATIONAL USE, PRIMARY EXPLOIT VECTORS, ATTACK INDICATORS, AND REPRESENTATIVE DETECTION APPROACHES.

and low-visibility fiber taps or malicious in-line components on tethered ground segments used for high-rate offload [74]. Forensics also shows that mission artifacts (video, logs, metadata) can persist and trigger exploitation on analysis hosts [7], [162], [163]. Many consumer/prosumer platforms expose auxiliary media-access paths (USB mass-storage, ad-hoc Wi-Fi/BLE) that simplify retrieval but enlarge the attack surface during handling [57]. Alongside the wired/media indicators discussed for pre-deployment, post-mission compromise often manifests as unexpected HID or composite device enumeration on ingest workstations, auto-mount and autorun-like behavior when UxV media is inserted, crashes or abnormal resource use in parsing/analysis tools when opening flight artifacts, or new outbound connections from isolated ingest networks shortly after a vehicle is connected. Detection therefore treats the returning platform as an untrusted peripheral: ingest hosts enforce device whitelisting, mount UxV media read-only, sandbox and scan parsing workflows, and correlate OS/EDR/IDS alerts with media-insert and tether-connect events, consistent with guidance from air-gapped malware and UxV forensics studies [7], [38], [162], [164].

3.3.2. UxV does not return (adversary capture). Loss or seizure gives an adversary sustained physical access to a vehicle's communications trust anchors and mission data. They can *extract credentials and keys* (C2/session keys, SATCOM profiles, Wi-Fi/cellular credentials, Remote ID) for later eavesdropping, cloning, or impersonation [39], [50], [57]; *dump and modify firmware* to create trojanized images for a recovered airframe or identical fleet hardware

[28]; and *reverse-engineer radio parameters* (frequencies, hopping plans, network IDs) to craft targeted jamming or spoofing against RF links [60], [61], [63]. *Mission logs and telemetry* further expose procedures and basing for follow-on targeting [163]. If the platform is returned, it may embed a *hardware implant* (tampered storage, modified debug/aux boards) or a *logic bomb* that triggers on reconnection—consistent with maintenance-chain and peripheral attacks [29], [47], [49]. Historical capture cases illustrate how such compromise undermines confidence in navigation and communications stacks [30].

In hostile custody, the same channels become data-leak paths. Forensic studies show many UAVs retain flight logs, media, wireless pairings, and configuration artifacts in internal flash/SD or on service ports, enabling reconstruction of operations and collection of network material for later impersonation and protocol-aware interference [57], [164]. Even without disassembly, residual emissions (e.g., active SATCOM on a downed node, Wi-Fi/BLE beacons) can disclose identifiers and session metadata. Contemporary UAS guidance—strong crypto, mutual authentication, secure boot, and rapid key rotation—seeks to bound the utility of captured nodes; absent these controls, adversaries can clone, re-provision, or insert rogue participants into UxV-to-UxV networks [165]. Forensics guidance also stresses chain-of-custody and controlled extraction because common access points (USB-serial/UART pads, JTAG, exposed storage) permit firmware dumps, key recovery, and persistent implants that compromise the same trust anchors relied upon in later deployments [164].

From an operator viewpoint, capture-related compromise manifests both during and after the loss event. In-mission indicators include abrupt and persistent loss of C2 and telemetry in otherwise benign RF conditions, failure or abnormal triggering of return-to-home or lost-link behaviors, and repeated loss patterns in the same geographical area or against the same fleet type, especially when correlated with normal environmental and network conditions. These symptoms are particularly suspicious when they coincide with unexpected mode transitions, unexplained parameter changes, or deviations from previously validated mission profiles. If a vehicle is later recovered, additional indicators appear at the platform level: changed firmware versions or hash values relative to the approved baseline, altered or missing keys and certificates, new or modified debug wiring and labels, unexpected services or beacons on RF/BLE/Wi-Fi/SATCOM interfaces, and behavior that no longer matches fleet baselines under identical test scenarios. Alongside the pre-deployment integrity checks discussed earlier, effective detection therefore relies on treating any suspected-captured platform as untrusted: enforcing secure boot and remote/local attestation on first power-up, revoking and re-issuing credentials before reintegration, performing structured forensic triage of storage and debug interfaces under controlled chain-of-custody, and using fleet-wide monitoring to spot cloned identifiers, duplicate Remote ID/Radio profiles, or anomalous configuration drift, as recommended in UAS security and forensics work [28], [39], [57], [164], [165].

4. Cross domain analysis

In this section, we present our findings on UxV communications. Using the methodology discussed in Section 2, we identify cross-cutting patterns, emerging themes, and a gap analysis; each is discussed in its own subsection. Before the detailed discussion, we distill the main cross-domain observations into a set of SoK-style takeaways: the "SoK Takeaways (Communications×Lifecycle Lens)" box below consolidates the dominant patterns and failure modes that underpin the subsequent analysis.

SoK Takeaways
(Communications × Lifecycle Lens)

- **Link interdependence dominates:** many incidents span multiple channels; defending one link can expose another via unintended fallbacks.
- **Redundancy paradox:** multi-link resilience enables *downgrade steering* unless handover logic is authenticated, explainable, and policy-bound.
- **Phase flips trust:** maintenance/offload paths (pre-/post-deployment) become high-risk channels even when operational RF looks healthy.
- **Universal failure fingerprints:** across RF/FSO/acoustic/tethered, compromise presents as PER/BER spikes, (re)association churn, C/N_0/SNR anomalies, and latency/jitter excursions misaligned with vehicle dynamics.
- **Identity is the anchor:** most integrity failures start as identity/control-plane failures (rogue endpoints, Sybil peers, unsafe handovers); fast, fleet-scale auth/attestation is foundational.
- **Navigation vs. comms split:** denial commonly targets C2 links; deception dominates PNT (often concurrently) necessitating cross-checks before control modes are engaged.
- **Practice implication:** logging *why* a link change occurred (and its crypto/auth state) is as important as the change itself; cross-modal consistency checks should gate autonomy.

4.1. Cross-cutting patterns

In this section, patterns that recur across vehicles, channels, and phases are discussed.

(P1) Common failure fingerprints across media. Despite very different physics (RF, optical, acoustic, tethered), compromise tends to look the same: spikes in PER/BER or retransmissions, association/re-association churn, link-quality anomalies (RSSI/C/N_0/SNR) that decouple from vehicle dynamics, and latency/jitter excursions. These universal indicators justify unified telemetry schemas and cross-modal health scoring.

(P2) Downgrade and cross-channel steering. Adversaries often win by steering systems into weaker modes or links (e.g., induce RF trouble to force cellular/SATCOM fallback, or nudge stacks from authenticated to legacy/unauth modes). Defenses must log *why* a fallback occurred and verify the cryptographic/authorization posture of the target link before accepting it.

(P3) Identity is the linchpin Integrity breaks usually start as identity failures: spoofed nodes, Sybil peers, rogue APs/eNodeBs/gNBs, unauthenticated optical endpoints,

Scenario	Channel	Typical Use	Primary Exploit Vectors	Attack Indicators	Detection Approaches
UxV returns (post-mission offload)	Maintenance I/O (wired, removable, local wireless)	Post-mission log/video offload, configuration sync, small updates between sorties	UxV acting as hostile peripheral or media source toward the GCS; BadUSB-style device impersonation; malware or crafted files on mission media; protocol-level injection into ingest or maintenance tools when exchanges are unsigned [29], [36], [37], [47], [49], [50], [62]	New or unexpected USB/HID/-composite devices; autorun-like behavior on media insert; mission or configuration files that differ from pre-flight hashes; AV/EDR alerts tied to specific UxV media; wireless offload sessions to unknown SSIDs/devices	Treat returning UxVs as untrusted clients; dedicated, hardened maintenance hosts; device-class whitelisting and disabled autorun; pre-ingest media scanning and sandboxed mounts; signed and authenticated telemetry/mission-file transfers
	Ground tether / fiber segment	High-rate bulk offload of mission data over tethered power/data links	Low-visibility optical taps or malicious in-line components on ground segments that leak or alter payloads/logs [74]	Unexplained loss/SNR drops on the tether leg; new or shifted events in OTDR traces; latency/jitter excursions on offload without corresponding platform dynamics	Baseline OTDR and received-power profiles with continuous monitoring; threshold alarms on loss/reflectance changes; periodic inspection of exposed connectors/patch panels; fiber intrusion-detection or distributed sensing on critical routes [74]
	Data handling / analysis pipeline	Ingest, processing, and archiving of mission artifacts on enterprise or lab systems	Malicious payloads embedded in logs, video, or metadata that exploit viewers, parsers, or ML pipelines and pivot into ground networks [7], [162], [163]	Crashes or abnormal behavior of analysis tools on specific files; new outbound connections or processes spawned by ingest workflows; recurring issues correlated with particular platforms or sorties	Quarantine and sandboxed triage of incoming mission data; content disarm and reconstruction for risky formats; AV/EDR and network IDS on analysis hosts; controlled ingestion paths with audit trails and least-privilege access
UxV does not return (adversary capture)	On-device storage and service ports	Maintenance/debug access to internal flash/SD and exposed UART/USB-serial or JTAG pads	Extraction of logs, media, configs, and paired credentials (Wi-Fi/cellular/Remote ID), enabling later impersonation, cloning, or targeted eavesdropping [57], [164]	Later RF sightings of cloned IDs or Remote ID beacons; unexplained reuse of legacy credentials; forensic traces of direct flash/port access on any recovered wreckage	Capture-aware incident response: rapid revocation/rotation of keys and credentials; monitoring for duplicate IDs and Remote ID beacons; forensic playbooks and controlled extraction procedures for any later-recovered platform [164], [165]
	Firmware / RF configuration and active links	Storage of firmware images, bootloaders, radio profiles (bands, hopping plans, IDs), and any live SATCOM/Wi-Fi/BLE connectivity	Firmware dump and modification to craft trojan images for re-introduction; reverse-engineering RF parameters for future jamming/spoofing; residual beacons from downed nodes revealing identifiers and session metadata [28], [60], [61], [63], [165]	Subsequent missions experiencing structured jamming/spoofing aligned with old configs; unexpected beacons from known-lost IDs; secure-boot or integrity failures on returned airframes	Secure and verified boot with signed updates; post-loss re-keying and RF-profile changes at fleet scale; geo-fenced monitoring for lost-node identifiers; quarantine and full re-attestation of any recovered hardware before reuse [28]
	Supply-chain reinsertion	Refurbishment and reintroduction of previously lost, seized, or heavily damaged UxVs	Hardware implants or logic bombs (tampered storage, hidden aux boards, modified cabling) that trigger on reconnection and attack GCS or peers [29], [30], [47], [49]	Physical discrepancies versus platform baseline (added boards, altered wiring); abnormal power draw; enumeration of unexpected devices on attach; reproducible crashes or odd behavior when reintegrated	Treat captured or unexplained-return platforms as hostile until proven otherwise; physical inspection against trusted hardware baselines; staged testing in isolated environments; independent firmware and configuration attestation before operational release

TABLE 5. POST-DEPLOYMENT SCENARIOS AND CHANNELS. THE UNDERLYING MEDIA MIRROR PRE-DEPLOYMENT (WIRED, REMOVABLE, WIRELESS, TETHERED), BUT THE *threat direction and timing change*: RETURNING UXVS CAN COMPROMISE GROUND SYSTEMS, WHILE CAPTURED UXVS BECOME SOURCES OF LONG-TERM DATA/CREDENTIAL LEAKAGE AND FUTURE IMPERSONATION, JAMMING, OR SPOOFING.

or unauthenticated middleware (e.g., MAVLink/ROS services). Fleet-wide, low-latency identity, with attestation and fast key rotation,must anchor all higher-layer controls.

(P4) Availability–integrity twin: jamming everywhere, GNSS spoofing dominates. Jamming is the universal availability attack across RF, cellular, and even acoustic links; in parallel, navigation integrity is dominated by GNSS spoofing/meaconing (carry-off, slow biasing). Expect denial on the C2 path and deception on the nav path—often concurrently.

(P5) Mobility is both a vulnerability and a defense. Motion enlarges the attack surface (FSO pointing fragility, altitude-driven cellular interference, RF multipath changes), yet it can be weaponized defensively via trajectory/power co-design, spatial diversity, and geometry-aware routing to escape jammers and reduce intercept probability.

(P6) The redundancy paradox. Multi-link designs (RF+FSO+tether+cellular) improve availability but also widen the attack surface and can mask tampering on one channel behind "healthy" telemetry on another. Cross-channel consistency checks—state agreement, time-alignment, and path-quality plausibility—are required to harvest redundancy's benefits safely.

(P7) Maintenance pathways are first-class attack vectors. Pre-deployment service paths (USB, SD, UART/Ethernet, ad-hoc Wi-Fi/BLE) reappear post-mission for offload and updates; treating them as "trusted" invites code/credential injection and BadUSB-style device impersonation. Quarantine, signing/verification, and attestation should gate every maintenance interaction.

(P8) UAVs dominate, with maritime domains underrepresented. The vast majority of titles target UAVs; USV/UUV work appears but is comparatively sparse. Even in maritime, RF and middleware dominate; acoustic security shows up, but far less than one might expect given underwater reliance—highlighting a cross-domain imbalance in attention.

4.2. Emerging themes

(E1) Renewed interest in wired/tethered links under contested RF. Wired and tethered links—including power-over-tether and fiber umbilicals—are being revisited to preserve C2 and payload transport when RF is jammed or unreliable, trading maneuverability for stable throughput and deterministic latency; OTDR, strain, and related monitoring also treat tether health as a security signal for tampering or damage [69]–[75].

(E2) SATCOM is an emerging direction for BLOS C2, with LEO/NTN-specific failure modes. SATCOM-based BLOS control, especially via LEO/NTN services, is growing but brings beam-hopping handovers, gateway churn, and drops to weaker modes; proposed defenses include authenticated control planes, GNSS/INS cross-checks, and satellite-aware failover logic [153], [154], [156]–[161].

(E3) Policy-driven multi-link orchestration is emerging beyond ad hoc failover. Rather than static

priority lists, recent studies explore policy engines coordinating RF, cellular, SATCOM, FSO, and tethered links under trust, cost, energy, and mission-phase constraints, with *anti-downgrade* and *explainable* fallback so attacker-steered transitions can be detected and rejected [95]–[100].

(E4) Resilient PNT increasingly relies on multi-sensor fusion and signals of opportunity. To resist GNSS spoofing and jamming, recent studies combine GNSS with INS, visual odometry, radar, and signals such as LTE/5G and LEO downlinks, using code–carrier checks, dual-frequency validation, and integrity monitors that gate autopilot or geofence actions before corrupted states affect control [141], [146]–[152].

(E5) Lightweight cryptography and fast identity remain an active design direction for constrained links. Acoustic and very low-bit-rate optical links still need authentication, encryption, and rekey mechanisms that fit strict bandwidth, latency, and energy budgets; current work explores compact AEAD, forward-secret group keys, and hardware-rooted attestation, but accepted designs remain open [92], [166], [167].

(E6) Mission-aware, cross-modal telemetry is a promising cross-domain direction. Another promising direction is to align heterogeneous-link telemetry with mission timelines and operational context, since link-quality anomalies, reassociation churn, timing irregularities, and physical-layer deviations suggest mission-aware baselines can reduce false positives across modalities [66], [67], [75], [86], [100], [142], [143], [145].

4.3. Gap analysis

Our cross-domain analysis identifies recurring gaps in research, engineering/deployment, and evaluation.

(G1) Secure maintenance and mission-plan integrity (Engineering/Deployment Gap). Public UAS guidance remains high-level and rarely specifies a verifiable lifecycle for *firmware* and *mission-plan* files, including signing/verification, host–device attestation, and post-mission quarantine/sanitization; maintenance paths link trusted setup to compromise. Unsigned route or payload files transferred via USB/UART/Ethernet/SD/BLE may persist into deployment and undermine control integrity [39], [168].

(G2) Lightweight identity and cryptography for constrained links (Research Gap). Underwater acoustic and very low-bit-rate optical links still lack accepted identity/attestation and AEAD schemes for group operation under severe bandwidth and latency limits; safety-critical coordination cannot support heavyweight handshakes or repeated recovery traffic. JANUS-style authentication helps, but loss-tolerant handshakes and fleet-scale recovery remain open [166], [167].

(G3) Authenticated handover and anti-downgrade control (Engineering/Deployment + Research Gap). Multi-link architectures improve resilience but still lack standard ways to bind fallback decisions to cryptographic state, trust level, mission phase, and operator visibility. Attackers may force fallback into weaker or unauthenticated modes while connectivity appears intact, so controllers should log why fallback occurred, whether the new link preserves authentication/integrity, and whether cross-channel checks passed [95], [98]–[100].

(G4) SATCOM/LEO/NTN security and resilience (Engineering/Deployment + Evaluation Gap). For BLOS C2 over SATCOM, especially LEO/NTN, open issues include handovers, beam hopping, Doppler, interference/jamming, and secure coupling to terrestrial cores. These can degrade availability or integrity in ways hard to separate from normal dynamics, and open evaluable mission-linked frameworks remain limited [169], [170].

(G5) Reproducible mission-linked datasets (Evaluation/Benchmarking Gap). GNSS spoofing work still depends heavily on TEXBAT and OAKBAT, risking narrow benchmarking. Comparable datasets linking communications telemetry, ground truth, operator actions, autonomy-state transitions, and *mission outcomes* remain scarce, especially for FSO, tethered, and acoustic links, making resilience claims hard to compare [171]–[173].

5. Conclusion

In this SoK we unified a fragmented literature by framing the UxV cyber surface along two orthogonal axes—communication channels (RF, FSO, acoustic, tethered/cabled, cellular/5G, SATCOM/GNSS, and peer links) and lifecycle phases (pre-deployment, operational, post-deployment)—and used that lens to map attacks, observable indicators, detection approaches, and evaluation metrics that tie link health to mission outcomes. Treating communications as first-class elements revealed recurring fingerprints across media (PER/BER spikes, reassociation churn, C/N_0 and SNR anomalies, latency/jitter excursions), the prevalence of jamming and GNSS deception, and the centrality of identity and control-plane integrity, while also surfacing downgrade steering and cross-channel masking as systemic risks in multi-link designs. Our cross-domain synthesis highlights underexplored but operationally critical areas—including lifecycle-secure maintenance paths and mission-plan integrity, lightweight fleet-scale cryptography and attestation for constrained acoustic/optical links, resilient swarm coordination, and BLOS C2 over LEO/NTN with authenticated handovers—and argues for mission-aware, modality-agnostic telemetry and consistency checks as the basis for robust detection and response. To support comparable progress, we release a reusable artifact (taxonomy, coded corpus, and evaluation templates) and advocate future work that (i) couples communications and navigation integrity with autonomy safeguards, (ii) publishes red-teamable, mission-linked datasets and HIL/field testbeds spanning all media, and (iii) standardizes metrics such as FPR/FNR, PER, C/N_0, and time-to-regain-control so that defenses can be assessed on their ability to preserve safety and task completion at scale.

Artifact Availability

The appendices document the search strings, filtering rules, and extraction codebook. The merged, deduplicated dataset and the scripts can be made available.

Acknowledgments

This work was supported by the NATO Science for Peace and Security Programme under project SPS G6246, Ai4CUAV.

References

[1] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan *et al.*, "The prisma 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, vol. 372, p. n71, 2021.

[2] L. Bauer, A. Doupé, and J. Clark, "Sok: Lessons learned from 30 years of systems security research," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 110–127.

[3] S. Niyonsaba, K. Konate, and M. M. Soidridine, "A survey on cybersecurity in unmanned aerial vehicles: Cyberattacks, defense techniques and future research directions," *International Journal of Computer Networks And Applications*, vol. 10, p. 688, 2023. [Online]. Available: https://www.researchgate.net/publication/375142426_A_Survey_on_Cybersecurity_in_Unmanned_Aerial_Vehicles_Cyberattacks_Defense_Techniques_and_Future_Research_Directions

[4] A. Mahalle, S. Khandelwal, A. Dhore, V. Barbudhe, and V. Waghmare, "Cyber attacks on uav networks: A comprehensive survey," *Review of Computer Engineering Research*, vol. 11, pp. 45–57, 2024. [Online]. Available: https://archive.conscientiabeam.com/index.php/76/article/view/3636

[5] A. Yu, I. Kolotylo, H. A. Hashim, and A. E. E. Eltoukhy, "Electronic warfare cyberattacks, countermeasures and modern defensive strategies of UAV avionics: A survey," *IEEE Access*, 2025, iEEE Access, vol. 13, pp. 68660–68681, 2025.

[6] S. Shrestha, M. Ababneh, S. Misra, H. M. Cathey Jr, R. Vishwanathan, M. Jansen, J. Choi, R. Bobba, and Y. Jang, "A comprehensive survey of unmanned aerial systems' risks and mitigation strategies," *arXiv preprint arXiv:2506.10327*, 2025. [Online]. Available: https://arxiv.org/abs/2506.10327

[7] V. Sihag, G. Choudhary, P. Choudhary, and N. Dragoni, "Cyber4drone: A systematic review of cyber security and forensics in next-generation drones," *Drones*, vol. 7, no. 7, p. 430, 2023.

[8] Y. Renu and V. Sarveshwaran, "A review of cyber security challenges and solutions in unmanned aerial vehicles (UAVs)," *Inteligencia Artificial*, vol. 28, pp. 199–219, 2025.

[9] Y. S. Khammas, H. Mahdi, and H. Al-Samarraie, "A survey of cyberattack countermeasures for unmanned aerial vehicles," *IEEE Access*, vol. 9, pp. 141 513–141 544, 2021.

[10] E. Yaacoub, H. Al-Hussaini, S. Hoteit, and A. Rabaa, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Wireless Networks*, vol. 26, pp. 4177–4193, 2020.

[11] J. Walatkiewicz and O. Darwish, "A survey on drone cybersecurity and the application of machine learning on threat emergence," in *International Conference on Advances in Computing Research*. Springer, 2023, pp. 523–532.

[12] A. E. Omolara, M. Alawida, and O. I. Abiodun, "Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey," *Neural computing and applications*, vol. 35, no. 31, pp. 23 063–23 101, 2023.

[13] 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, 2023.

[14] N. Bai, X. Hu, and S. Wang, "A survey on unmanned aerial systems cybersecurity," *Journal of Systems Architecture*, vol. 156, p. 103282, 2024.

[15] B. Cordill, D. Fang, and S. Xu, "A comprehensive survey of security and privacy in uav systems," *IEEE Access*, 2025.

[16] Z. Yu, Z. Wang, J. Yu, D. Liu, H. H. Song, and Z. Li, "Cybersecurity of unmanned aerial vehicles: A survey," *IEEE Aerospace and Electronic Systems Magazine*, vol. 39, no. 9, pp. 182–215, 2023.

[17] S. Beycimen, D. Ignatyev, and A. Zolotas, "A comprehensive survey of unmanned ground vehicle terrain traversability for unstructured environments and sensor technology insights," *Engineering Science and Technology, an International Journal*, vol. 47, p. 101457, 2023.

[18] B. B. Madan, M. Banik, and D. Bein, "Securing unmanned autonomous systems from cyber threats," *The Journal of Defense Modeling and Simulation*, vol. 16, no. 2, pp. 119–136, 2019.

[19] A. Oruc, "Potential cyber threats, vulnerabilities, and protections of unmanned vehicles," *Drone Systems and Applications*, vol. 10, no. 1, pp. 51–58, 2022.

[20] O. Ivanchenko, V. Kharchenko, N. Smyrynska, and O. Veprytska, "Cybersecurity of unmanned surface vessels: Imeca based assessment and protection against ai powered attacks," *Annual of Navigation*, no. 29, pp. 35–37, 2024.

[21] R. Zagan, G. Raicu, and A. Sabau, "Studies and research regarding vulnerabilities of marine autonomous surface systems (mass) and remotely operated vessels (rovs) from point of view of cybersecurity," *Int J Modern Manuf Technol*, vol. 14, pp. 310–318, 2022.

[22] P. Solnør, Ø. Volden, K. Gryte, S. Petrovic, and T. I. Fossen, "Hijacking of unmanned surface vehicles: A demonstration of attacks and countermeasures in the field," *Journal of Field Robotics*, vol. 39, no. 5, pp. 631–649, 2022.

[23] A. Wibisono, M. J. Piran, H.-K. Song, and B. M. Lee, "A survey on unmanned underwater vehicles: Challenges, enabling technologies, and future research directions," *Sensors*, vol. 23, no. 17, p. 7321, 2023.

[24] H. Alamleh and B. Karabacak, "Exploring the security landscape of underwater positioning and navigation systems: An attack surface analysis," in *2024 IEEE 49th Conference on Local Computer Networks (LCN)*, 2024, pp. 1–7.

[25] M. Johnson, J. Gordon, and P. Wilson, "Distributed operations in a contested environment: Implications for usaf force presentation," 2019, accessed: 2025-10-30. [Online]. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2959/RAND_RR2959.pdf

[26] Defense Advanced Research Projects Agency (DARPA), "Collaborative operations in denied environment (code)," https://www.darpa.mil/research/programs/collaborative-operations-in-denied-environment, 2020, accessed: 2025-10-30.

[27] Joint Air Power Competence Centre (JAPCC), "Remotely piloted aircraft systems in contested environments," 2016, accessed: 2025-10-30. [Online]. Available: https://www.japcc.org/wp-content/uploads/JAPCC-RPAS-Operations-in-Contested-Environments.pdf

[28] A. Regenscheid *et al.*, "Platform firmware resiliency guidelines," National Institute of Standards and Technology, Tech. Rep. NIST Special Publication 800-193, 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

[29] D. J. Tian, A. Bates, and K. R. B. Butler, "Defending against malicious usb firmware with goodusb," in *Proceedings of the 31st Annual Computer Security Applications Conference (ACSAC)*, Los Angeles, CA, 2015. [Online]. Available: https://www.cise.ufl.edu/~butler/pubs/acsac15.pdf

[30] N. Shachtman, "Exclusive: Computer virus hits u.s. drone fleet," *WIRED*, accessed: 2025-10-30. [Online]. Available: https://www.wired.com/2011/10/virus-hits-drone-fleet/

[31] I. Arghire, "Chinese hackers hit drone sector in supply chain attacks," *SecurityWeek*, accessed: 2025-10-30. [Online]. Available: https://www.securityweek.com/chinese-hackers-hit-drone-sector-in-supply-chain-attacks/

[32] C. Cimpanu, "Fbi: Fin7 hackers target us companies with badusb devices to install ransomware," *The Record (from Recorded Future News)*, accessed: 2025-10-30. [Online]. Available: https://therecord.media/fbi-fin7-hackers-target-us-companies-with-badusb-devices-to-install

[33] Z. O. Imam, M. Lacoste, and G. Arfaoui, "Towards a modular attestation framework for flexible data protection for drone systems," in *2021 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2021, pp. 96–102.

[34] V. Pal, B. S. Acharya, S. Shrivastav, S. Saha, A. Joglekar, and B. Amrutur, "Puf based secure framework for hardware and software security of drones," in *2020 asian hardware oriented security and trust symposium (AsianHOST)*. IEEE, 2020, pp. 01–06.

[35] S. Al Majmaie, N. P. Bhatta, P. P. Kharat, and F. Amsaad, "Puf-based hardware security for trusted internet of drones: Challenges and future directions," in *2025 1st International Conference on Secure IoT, Assured and Trusted Computing (SATC)*. IEEE, 2025, pp. 1–7.

[36] A. Dorais-Joncas and E. Research, "Jumping the air gap: 17 malware frameworks that used removable media," ESET, Tech. Rep., 2021. [Online]. Available: https://web-assets.esetstatic.com/wls/en/papers/white-papers/eset_jumping_the_air_gap_wp.pdf

[37] E. Research, "Acad/medre.a: 10,000s of autocad designs leaked in suspected industrial espionage," ESET, Tech. Rep., 2012. [Online]. Available: https://web-assets.esetstatic.com/wls/white-papers/ESET_ACAD_Medre_A_whitepaper.pdf

[38] M. A. Hussain, K. Samrouth, and N. Bakir, "A survey on malware attacks in industrial air-gap systems: Md. a. hussain et al." *International Journal of Information Security*, vol. 24, no. 3, p. 146, 2025.

[39] CISA, "Pre-flight cybersecurity considerations for uncrewed aircraft systems," Tech. Rep., 2025.

[40] A. Marchand, Y. Imine, H. Ouarnoughi, T. Tarridec, and A. Gallais, "Firmware integrity protection: A survey," *IEEE Access*, vol. 11, pp. 77 952–77 979, 2023.

[41] Y. Wu, J. Wang, Y. Wang, S. Zhai, Z. Li, Y. He, K. Sun, Q. Li, and N. Zhang, "Your firmware has arrived: A study of firmware update vulnerabilities," in *33rd USENIX Security Symposium (USENIX Security 24)*, 2024, pp. 5627–5644.

[42] TCG, "Secure firmware update and supply-chain practices for embedded systems," Tech. Rep., 2020.

[43] V. KARLOS, M. LARCHER *et al.*, *Protection against Unmanned Aircraft Systems: Handbook on UAS Risk Assessment & Principles for Physical Hardening of Buildings and Sites*, 2023.

[44] A. Rugo, C. A. Ardagna, and N. E. Ioini, "A security review in the uavnet era: Threats, countermeasures, and gap analysis," *ACM Computing Surveys (CSUR)*, vol. 55, no. 1, pp. 1–35, 2022.

[45] S. Azam, F. Munir, A. M. Sheri, J. Kim, and M. Jeon, "System, design and experimental validation of autonomous vehicle in an unconstrained environment," *Sensors*, vol. 20, no. 21, p. 5999, 2020.

[46] M. S. Alkatheiri, S. Saleem, M. A. Alqarni, A. O. Aseeri, S. H. Chauhdary, and Y. Zhuang, "A lightweight authentication scheme for a network of unmanned aerial vehicles (uavs) by using physical unclonable functions," *Electronics*, vol. 11, no. 18, 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/18/2921

[47] K. Nohl and J. Lell, "Badusb – on accessories that turn evil," in *Black Hat USA Briefings*, Las Vegas, NV, 2014. [Online]. Available: https://www.blackhat.com/us-14/briefings.html

[48] T. Fuchs, "Hydradancer: Faster usb emulation for facedancer," Quarkslab Blog, April 2024. [Online]. Available: https://blog.quarkslab.com/hydradancer-faster-usb-emulation-for-facedancer.html

[49] D. Spill and A. Stasiak, "Usbproxy: An open and affordable usb man in the middle device," in *ShmooCon Proceedings*, Washington, D.C., 2014. [Online]. Available: https://shmoo.gitbook.io/2014-shmoocon-proceedings/build_it/02_usbproxy

[50] J. A. Marty, "Vulnerability analysis of the mavlink protocol for command and control of unmanned aerial vehicles," Master's thesis, Air Force Institute of Technology, 2014. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA598977

[51] Wifiphisher Project, "Wifiphisher: Automated phishing attacks against wi-fi networks," Open-source project documentation, 2015. [Online]. Available: https://wifiphisher.org/

[52] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, "Understanding the mirai botnet," in *26th USENIX Security Symposium (USENIX Security 17)*, Vancouver, BC, 2017, pp. 1093–1110. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[53] B. Moran, H. Tschofenig, D. Brown, and M. Meriac, "A firmware update architecture for internet of things," IETF, RFC 9019, April 2021. [Online]. Available: https://www.rfc-editor.org/info/rfc9019

[54] ArduPilot Dev Team, "Sik telemetry radio — ardupilot documentation," 2025. [Online]. Available: https://ardupilot.org/copter/docs/common-sik-telemetry-radio.html

[55] M. W. Shafer, G. Vega, K. Rothfus, and P. Flikkema, "Uav wildlife radiotelemetry: System and methods of localization," *Methods in Ecology and Evolution*, vol. 10, no. 10, pp. 1783–1795, 2019.

[56] H. Zhao, J. Zhang, and J. Zhou, "The application of ofdm in uav telemetry," in *Proceedings of the 26th Conference of Spacecraft TT&C Technology in China: Shared and Flexible TT&C (Tracking, Telemetry and Command) Systems*. Springer, 2012, pp. 89–97.

[57] N. Schiller, T. Holz, C. Rossow *et al.*, "Drone security and the mysterious case of dji's droneid," in *Network and Distributed System Security Symposium (NDSS)*, 2023. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2023/02/ndss2023_f217_paper.pdf

[58] L. Davoli, E. Pagliari, and G. Ferrari, "Hybrid lora-ieee 802.11 s opportunistic mesh networking for flexible uav swarming," *Drones*, vol. 5, no. 2, p. 26, 2021.

[59] R. Singh, J. H. Jepsen, K. D. Ballal, S. Nwabuona, M. Berger, and L. Dittmann, "An investigation of 5g, lte, lte-m and nb-iot coverage for drone communication above 450 feet," in *2023 IEEE 24th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2023, pp. 370–375.

[60] K. Pärlin, M. M. Alam, and Y. Le Moullec, "Jamming of uav remote control systems using software defined radio," in *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, 2018, pp. 1–6.

[61] O. Šimon, T. Götthans, and M. Popela, "Commercial uav jamming possibilities," in *2022 32nd International Conference Radioelektronika (RADIOELEKTRONIKA)*, 2022, pp. 1–6.

[62] M. Ficco, R. Palmiero, M. Rak, and D. Granata, "Mavlink protocol for unmanned aerial vehicle: Vulnerabilities analysis," in *2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*. IEEE, 2022, pp. 1–6.

[63] J. El Fiorenza, R. Lokku, K. Sivakumar, and M. Stephanie, "Versatile exploitation techniques: Drone hacking and jamming with raspberry-pi and wi-fi pineapple," *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, no. 1, 2019.

[64] J. Colter, M. Kinnison, A. Henderson, S. M. Schlager, S. Bryan, K. L. O'Grady, A. Abballe, and S. Harbour, "Testing the resiliency of consumer off-the-shelf drones to a variety of cyberattack methods," in *2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC)*, 2022, pp. 1–5.

[65] V. S. Kumar, G. N. Mori, S. K. K. R, P. J. Josephson, N. Kumar, and R. Nithya, "Detecting jamming and spoofing attacks on unmanned aerial vehicles with advanced neural network models," in *2025 Global Conference in Emerging Technology (GINOTECH)*, 2025, pp. 1–6.

[66] Z. Zhang, Y. Zhang, J. Niu, and D. Guo, "Unknown network attack detection based on open-set recognition and active learning in drone network," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 10, p. e4212, 2022.

[67] C. Greco, P. Pace, S. Basagni, and G. Fortino, "Jamming detection at the edge of drone networks using multi-layer perceptrons and decision trees," *Applied Soft Computing*, vol. 111, p. 107806, 2021.

[68] O. M. Ayegun, K. F. Akingbade, J. J. Popoola, and B. C. Ubochi, "Leveraging on artificial intelligence for universal jamming attack detection in unmanned aerial vehicle communication," *Computers and Electrical Engineering*, vol. 127, p. 110602, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790625005452

[69] A. Yingst and V. Marojevic, "Power tether for long duration multicopter flight," *HardwareX*, vol. 15, p. e00466, 2023.

[70] F. Fattori and S. Cocuzza, "Tethered drones: A comprehensive review of technologies, challenges, and applications," *Drones*, vol. 9, no. 6, p. 425, 2025.

[71] M. N. Marques, S. A. Magalhães, F. N. Dos Santos, and H. S. Mendonça, "Tethered unmanned aerial vehicles—a systematic review," *Robotics*, vol. 12, no. 4, p. 117, 2023.

[72] R. B. Wynn, V. A. Huvenne, T. P. Le Bas, B. J. Murton, D. P. Connelly, B. J. Bett, H. A. Ruhl, K. J. Morris, J. Peakall, D. R. Parsons *et al.*, "Autonomous underwater vehicles (auvs): Their past, present and future contributions to the advancement of marine geoscience," *Marine geology*, vol. 352, pp. 451–468, 2014.

[73] Y. He, D. B. Wang, and Z. A. Ali, "A review of different designs and control models of remotely operated underwater vehicle," *Measurement and Control*, vol. 53, no. 9-10, pp. 1561–1570, 2020.

[74] V. Spurny, P. Munster, A. Tomasov, T. Horvath, and E. Skaljo, "Physical layer components security risks in optical fiber infrastructures," *Sensors*, vol. 22, no. 2, p. 588, 2022.

[75] K. Liu, L. Zhang, J. Jiang, P. Ma, Z. Sun, L. Weng, and T. Liu, "Distributed optical fiber sensor perimeter security system based on uav video linkage," *Journal of Optoelectronics· Laser*, vol. 30, pp. 1244–51, 2019.

[76] Y. Kaymak, R. Rojas-Cessa, J. Feng, N. Ansari, M. Zhou, and T. Zhang, "A survey on acquisition, tracking, and pointing mechanisms for mobile free-space optical communications," *IEEE communications surveys & tutorials*, vol. 20, no. 2, pp. 1104–1123, 2018.

[77] L. B. Stotts and L. C. Andrews, "Adaptive optics model characterizing turbulence mitigation for free space optical communications link budgets," *Optics Express*, vol. 29, no. 13, pp. 20 307–20 321, 2021.

[78] O. Steinvall, "Laser dazzling: an overview," *Technologies for Optical Countermeasures XIX*, vol. 12738, pp. 17–31, 2023.

[79] O. O. Kolawole, T. J. Afullo, and M. Mosalaosi, "Analysis of scintillation effects on free space optical communication links in south africa," in *Photonics*, vol. 9, no. 7. MDPI, 2022, p. 446.

[80] G. G. Peter, S. R. William, R. Mahon, L. M. James, S. F. Mike, R. S. Michele, R. S. Walter, B. X. Ben, R. B. Harris, I. M. Christopher *et al.*, "Modulating retro-reflector lasercom systems at the naval research laboratory," in *2010-MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE*. IEEE, 2010, pp. 1601–1606.

[81] J. Yuan, X. Wang, M. Jin, W. Liu, R. Wu, Z. Wei, D. Deng, and H. Liu, "A novel system of mixed rf/fso uav communication based on mrr and ris by adopting hybrid modulation," in *Photonics*, vol. 9, no. 6. MDPI, 2022, p. 379.

[82] X. Zhang, G. Klevering, X. Lei, Y. Hu, L. Xiao, and G.-H. Tu, "The security in optical wireless communication: A survey," *ACM Computing Surveys*, vol. 55, no. 14s, pp. 1–36, 2023.

[83] R. Zhong, J. Ji, Z. Wang, K. Wang, and Y. Song, "Physical layer security of fso communication system based on gg correlation channel," *Optoelectronics Letters*, vol. 20, no. 11, pp. 658–662, 2024.

[84] H. Wu, D. Kang, J. Ding, J. Yang, Q. Wang, J. Wu, and J. Ma, "Secrecy performance analysis in the fso communication system considering different eavesdropping scenarios," *Optics express*, vol. 30, no. 23, pp. 41 028–41 047, 2022.

[85] S. S. Patil, C. Joseph, D. Varpe, and A. Raj, "A comprehensive review on security in free-space optical communication," *Int. J. Eng. Res. Rev.*, vol. 12, no. 3, pp. 150–180, 2024.

[86] M. Sliti, W. Abdallah, and N. Boudriga, "Jamming attack detection in optical uav networks," in *2018 20th international conference on transparent optical networks (ICTON)*. IEEE, 2018, pp. 1–5.

[87] N. Ramdhan, M. Sliti, and N. Boudriga, "Packet insertion attack detection in optical uav networks," in *2018 20th International Conference on Transparent Optical Networks (ICTON)*. IEEE, 2018, pp. 1–5.

[88] W. Aman, S. Al-Kuwari, M. Muzzammil, M. M. U. Rahman, and A. Kumar, "Security of underwater and air–water wireless communication: State-of-the-art, challenges and outlook," *Ad Hoc Networks*, vol. 142, p. 103114, 2023.

[89] W. Aman, S. Al-Kuwari, and M. Qaraqe, "Performance analysis of underwater acoustic channel amid jamming by random jammers," *Internet Technology Letters*, vol. 8, no. 4, p. e595, 2025.

[90] J. Ryu and S. Kim, "Mitigating jamming attacks in underwater sensor networks using m-qubed-based opportunistic routing protocol," *ETRI Journal*, vol. 47, no. 3, pp. 559–571, 2025.

[91] J. Shi, K. Tian, and J. Zhang, "Delay-fluctuation-resistant underwater acoustic network access method based on deep reinforcement learning," *Sensors*, vol. 25, no. 21, 2025. [Online]. Available: https://www.mdpi.com/1424-8220/25/21/6673

[92] L. Bragagnolo, F. Ardizzon, N. Laurenti, P. Casari, R. Diamant, and S. Tomasin, "Authentication of underwater acoustic transmissions via machine learning techniques," in *2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS)*. IEEE, 2021, pp. 255–260.

[93] J. Dzielski, M. DeLorme, A. Sedunov, P. Sammut, and M. Tsionskiy, "Guidance of an unmanned underwater vehicle using a passive acoustic threat detection system," in *2010 International WaterSide Security Conference*. IEEE, 2010, pp. 1–4.

[94] Y. Qin, Z. Li, and S. Huang, "Analysis and review of key countermeasure technologies for underwater unmanned systems," in *International Conference on Autonomous Unmanned Systems*. Springer, 2024, pp. 119–127.

[95] S. Khemiri, M. A. Kishk, and M.-S. Alouini, "Exploiting tethered and untethered uavs: a hybrid aerial communication system," *Scientific Reports*, vol. 15, no. 1, p. 15882, 2025.

[96] S. Phuchortham and H. Sabit, "A survey on free-space optical communication with rf backup: models, simulations, experience, machine learning, challenges and future directions," *Sensors*, vol. 25, no. 11, p. 3310, 2025.

[97] Z. Chi, Y. Li, X. Liu, W. Wang, Y. Yao, T. Zhu, and Y. Zhang, "Countering cross-technology jamming attack," in *Proceedings of the 13th ACM conference on security and privacy in wireless and mobile networks*, 2020, pp. 99–110.

[98] I. Anagnostis, P. Kotzanikolaou, and C. Douligeris, "Understanding and securing the risks of unmanned aerial vehicle services," *IEEE Access*, 2025.

[99] H. Sathaye, G. Noubir, and A. Ranganathan, "On the implications of spoofing and jamming aviation datalink applications," in *Proceedings of the 38th Annual Computer Security Applications Conference*, 2022, pp. 548–560.

[100] R. Chen and L. Zhao, "Multi-level autonomous integrity monitoring method for multi-source pnt resilient fusion navigation," *Satellite Navigation*, vol. 4, no. 1, p. 21, 2023.

[101] L. Xiang, F. Wang, W. Xu, T. Zhang, M. Pan, and Z. Han, "Dynamic uav swarm collaboration for multi-targets tracking under malicious jamming: Joint power, path and target association optimization," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 4, pp. 5410–5425, 2024.

[102] Z. Xing, Y. Qin, C. Du, W. Wang, and Z. Zhang, "Deep reinforcement learning-driven jamming-enhanced secure unmanned aerial vehicle communications," *Sensors (Basel, Switzerland)*, vol. 24, no. 22, p. 7328, 2024.

[103] X. Tang, K. Zhao, C. Shen, C. Lin, S. Liu, B. Wang, D. Niyato, and Z. Han, "Graph attention network-driven hierarchical learning for anti-jamming uav communications," *IEEE Transactions on Wireless Communications*, 2025.

[104] L. Cheng, Z. Xu, J. Zhou, D. Tian, X. Duan, K. Qu, and D. Zhao, "Adaptive spectrum anti-jamming in uav-enabled air-to-ground networks: A bimatrix stackelberg game approach," *Electronics*, vol. 12, no. 20, p. 4344, 2023.

[105] C. Zou, C. Li, Y. Li, and X. Yan, "Ris-assisted robust beamforming for uav anti-jamming and eavesdropping communications: A deep reinforcement learning approach," *Electronics*, vol. 12, no. 21, p. 4490, 2023.

[106] Y. Aydin, G. K. Kurt, E. Ozdemir, and H. Yanikomeroglu, "Group authentication for drone swarms," in *2021 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)*. IEEE, 2021, pp. 72–77.

[107] W. Jiang, Z. Du, X. Rong, Y. Fu, S. Zheng, and Y. Chen, "Bcua: A uav group authentication protocol based on the cvmerkle tree structure," *IEEE Transactions on Vehicular Technology*, 2025.

[108] S.-F. Chou and C.-Y. Huang, "Blockchain-aided uav delivery networks for enhanced data security and parcels traceability," in *2025 IEEE 101st Vehicular Technology Conference (VTC2025-Spring)*. IEEE, 2025, pp. 1–5.

[109] L. Senigagliesi, G. Ciattaglia, and E. Gambi, "Autoencoder based physical layer authentication for uav communications," in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*. IEEE, 2023, pp. 1–6.

[110] Y. Zheng, X. Zhang, S. Wang, and W. Zhang, "Convolutional neural network and ensemble learning-based unmanned aerial vehicles radio frequency fingerprinting identification," *Drones*, vol. 8, no. 8, p. 391, 2024.

[111] C. Liu, L. Liu, J. Cao, and Y. Luo, "Event-triggered secure formation tracking of delayed multi-uav systems subject to dos attacks," *IEEE Transactions on Network Science and Engineering*, 2025.

[112] S. Liu and J. Huang, "Decentralized adaptive event-triggered fault-tolerant cooperative control of multiple unmanned aerial vehicles and unmanned ground vehicles with prescribed performance under denial-of-service attacks," *Mathematics*, vol. 12, no. 17, p. 2701, 2024.

[113] Y. Cui, Y. Liang, Q. Luo, Z. Shu, and T. Huang, "Resilient consensus control of heterogeneous multi-uav systems with leader of unknown input against byzantine attacks," *IEEE Transactions on Automation Science and Engineering*, vol. 22, pp. 5388–5399, 2024.

[114] J. Tian, B. Wang, R. Guo, Z. Wang, K. Cao, and X. Wang, "Adversarial attacks and defenses for deep-learning-based unmanned aerial vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22 399–22 409, 2021.

[115] J. Akram, A. Anaissi, A. Akram, R. S. Rathore, and R. H. Jhaveri, "Adversarial label-flipping attack and defense for anomaly detection in spatial crowdsourcing uav services," *IEEE Transactions on Consumer Electronics*, 2024.

[116] V. U. Ihekoronye, U. U. Izuazu, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "Asr-fed: Agnostic straggler resilient federated algorithm for drone networks security," in *IEEE INFOCOM 2024-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2024, pp. 1–6.

[117] Y. Bing, L. Wang, and Z. Chen, "A spectrum sensing method for uav swarms under byzantine attack," in *International Conference on Autonomous Unmanned Systems*. Springer, 2021, pp. 1748–1758.

[118] J. Yu, Y. Zhang, and C. Sun, "End-to-end multi-task reinforcement learning-based uav swarm communication attack detection and area coverage," *Knowledge-Based Systems*, vol. 316, p. 113390, 2025.

[119] D. Zhao, P. Shen, X. Han, and S. Zeng, "Security situation assessment in uav swarm networks using transrese: A transformer-resnext-se based approach," *Vehicular Communications*, vol. 50, p. 100842, 2024.

[120] S. D. Muruganathan, X. Lin, H.-L. Määttänen, J. Sedin, Z. Zou, W. A. Hapsari, and S. Yasukawa, "An overview of 3gpp release-15 study on enhanced lte support for connected drones," *IEEE Communications Standards Magazine*, vol. 5, no. 4, pp. 140–146, 2021.

[121] A. S. Abdalla and V. Marojevic, "Security threats and cellular network procedures for unmanned aircraft systems: Challenges and opportunities," *IEEE Communications Standards Magazine*, vol. 6, no. 4, pp. 104–111, 2023.

[122] J. Urama, R. Wiren, O. Galinina, J. Kauppi, K. Hiltunen, J. Erkkila, F. Chernogorov, P. Etelaaho, M. Heikkila, J. Torsner *et al.*, "Uav-aided interference assessment for private 5g nr deployments: Challenges and solutions," *IEEE Communications Magazine*, vol. 58, no. 8, pp. 89–95, 2020.

[123] I. Kovacs, R. Amorim, H. C. Nguyen, J. Wigard, and P. Mogensen, "Interference analysis for uav connectivity over lte using aerial radio measurements," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*. IEEE, 2017, pp. 1–6.

[124] G. Amponis, P. Radoglou-Grammatikis, T. Lagkas, W. Mallouli, A. Cavalli, D. Klonidis, E. Markakis, and P. Sarigiannidis, "Threatening the 5g core via pfcp dos attacks: the case of blocking uav communications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, p. 124, 2022.

[125] P. Cumino, J. Baranda, M. Luis, D. Rosario, E. Cerqueira, J. Mangues, and S. Sargento, "Enhancing mobile network performance through oran-integrated uav-based mobility management," in *IEEE INFOCOM 2024-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2024, pp. 1–8.

[126] A. Kumbhar, S. Singh, and I. Guvenc, "Uav assisted public safety communications with lte-advanced hetnets and feicic," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 2017, pp. 1–7.

[127] A. Kumbhar, "Performance improvement using icic for uav-assisted public safety networks with clustered users during emergency," in *Telecom*, vol. 4, no. 4. MDPI, 2023, pp. 816–835.

[128] R. Mozny, P. Masek, M. Stusek, K. Molnar, M. Palenska, D. Moltchanov, and J. Hosek, "Experimental quality assessment of cellular networks and their utilization for uav services," in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*. IEEE, 2023, pp. 1–6.

[129] M. Gharib, B. Hopkins, J. Murrin, A. Koka, and F. Afghah, "5g wings: Investigating 5g-connected drones performance in non-urban areas," in *2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2023, pp. 1–6.

[130] A. Stateczny, K. Gierlowski, and M. Hoeft, "Wireless local area network technologies as communication solutions for unmanned surface vehicles," *Sensors*, vol. 22, no. 2, p. 655, 2022.

[131] P. Kozak, V. Platenka, and M. Vrsecka, "Analysis of communication protocols of uav control sets," in *2022 New Trends in Signal Processing (NTSP)*. IEEE, 2022, pp. 1–6.

[132] O. Mujumdar, H. Celebi, I. Guvenc, M. Sichitiu, S. Hwang, and K.-M. Kang, "Use of lora for uav remote id with multi-user interference and different spreading factors," in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*. IEEE, 2021, pp. 1–7.

[133] M. E. Sunny, P. Umesh, K. Gangadharan, and D. Shetty, "Development of a lorawan-enabled unmanned aerial system for autonomous real-time surveillance and monitoring," in *ASME International Mechanical Engineering Congress and Exposition*, vol. 87639. American Society of Mechanical Engineers, 2023, p. V006T07A016.

[134] X. Li, W. Feng, J. Wang, Y. Chen, N. Ge, and C.-X. Wang, "Enabling 5g on the ocean: A hybrid satellite-uav-terrestrial network solution," *IEEE Wireless Communications*, vol. 27, no. 6, pp. 116–121, 2020.

[135] Y. Zou, J. Zhu, T. Wu, H. Guo, and H. Wei, "Cooperative drone communications for space-air-ground integrated networks," *IEEE Network*, vol. 35, no. 5, pp. 100–106, 2021.

[136] A. Fouda, A. S. Ibrahim, I. Guvenc, and M. Ghosh, "Uav-based in-band integrated access and backhaul for 5g communications," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*. IEEE, 2018, pp. 1–5.

[137] S. Liu, H. Yang, M. Zheng, and L. Xiao, "Multi-uav-assisted mec in iov with combined multi-modal semantic communication under jamming attacks," *IEEE Transactions on Mobile Computing*, 2025.

[138] J. Qiu, Z. Kuang, Z. Huang, and S. Lin, "Security offloading scheduling and caching optimization algorithm in uav edge computing," *IEEE Systems Journal*, 2025.

[139] Y. Ding, Y. Feng, W. Lu, S. Zheng, N. Zhao, L. Meng, A. Nallanathan, and X. Yang, "Online edge learning offloading and resource management for uav-assisted mec secure communications," *IEEE Journal of Selected Topics in Signal Processing*, vol. 17, no. 1, pp. 54–65, 2022.

[140] K. Upadhya, K. Valkealahti, M. Moisio, D. Korpi, T. Ihalainen, and M. A. Uusitalo, "Passive reflectors for enhancing cellular uav coverage," in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2022, pp. 896–901.

[141] W. Miao, C. Luo, G. Min, Y. Mi, and Z. Yu, "Location-based robust beamforming design for cellular-enabled uav communications," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9934–9944, 2020.

[142] J. Viana, H. Farkhari, P. Sebastião, and V. P. G. Jimenez, "Pca-featured transformer for jamming detection in 5g uav networks," *IEEE Open Journal of the Communications Society*, 2025.

[143] T. Assaf, M. Al-Jarrah, A. Al-Dweik, Z. Ding, E. Alsusa, and A. Pandey, "Two-stage jamming detection and channel estimation for uav-based iot systems," *IEEE Transactions on Information Forensics and Security*, 2025.

[144] M. Veksler, D. L. Rodríguez, A. Aris, K. Akkaya, and A. S. Uluagac, "Lofin: Lora-based uav fingerprinting framework," in *MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM)*. IEEE, 2022, pp. 980–985.

[145] M. Keizer, S. Sciancalepore, and G. Oligeri, "Ghostbuster: Detecting misbehaving remote id-enabled drones," in *2024 IEEE 21st Consumer Communications & Networking Conference (CCNC)*. IEEE, 2024, pp. 324–332.

[146] 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, p. e507, 2021.

[147] R. D. Restivo, L. C. Dodson, J. Wang, W. Tan, Y. Liu, H. Wang, and H. Song, "Gps spoofing on uav: A survey," in *IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2023, pp. 1–6.

[148] Z. Wen, X. Qi, T. Sato, K. Tamesue, Y. Katsuyama, K. Sako, J. Katto, and T. Sato, "Lstm-based gnss spoofing detection for drone formation flights," in *IECON 2023-49th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2023, pp. 1–6.

[149] J. Zhou, W. Wang, and C. Zhang, "A gnss antijamming method in multiuav cooperative system," *IEEE Transactions on Vehicular Technology*, 2025.

[150] L. Wang, X. Wei, H. Zhang, and L. Jia, "Attdet: Attitude angles-based uav gnss spoofing detection," in *2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2024, pp. 2468–2473.

[151] S. Hacohen, O. Medina, T. Grinshpoun, and N. Shvalb, "Improved gnss localization and byzantine detection in uav swarms," *Sensors*, vol. 20, no. 24, p. 7239, 2020.

[152] S. Bang and J. Kim, "Adaptive switching strategy of an aerial drone's gnss antennas with metallic shielding for gnss anti-jamming," *Sensors*, vol. 25, no. 18, p. 5778, 2025.

[153] M. M. I. Mamun, C. Beard, and D. Medhi, "A uav-assisted multiuser non-terrestrial cyclic postfixed windowed ofdm system," in *2022 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2022, pp. 1–6.

[154] C. Han, A. Liu, K. An, H. Wang, G. Zheng, S. Chatzinotas, L. Huo, and X. Tong, "Satellite-assisted uav trajectory control in hostile jamming environments," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 4, pp. 3760–3775, 2021.

[155] X. Fang, W. Feng, Y. Wang, Y. Chen, N. Ge, Z. Ding, and H. Zhu, "Noma-based hybrid satellite-uav-terrestrial networks for 6g maritime coverage," *IEEE Transactions on Wireless Communications*, vol. 22, no. 1, pp. 138–152, 2022.

[156] C. Liu, W. Feng, Y. Chen, C.-X. Wang, and N. Ge, "Cell-free satellite-uav networks for 6g wide-area internet of things," *IEEE journal on selected areas in communications*, vol. 39, no. 4, pp. 1116–1131, 2020.

[157] X. Li, G. Duan, S. Yan, Z. Zhao, J. Shi, and Z. Li, "Optimizing uav jammer for covert communication of leo satellite system," in *2022 10th International Conference on Information Systems and Computing Technology (ISCTech)*. IEEE, 2022, pp. 156–161.

[158] Y. Qin, H. Zhang, N. Ma, J. Li, and H. Hu, "Anti-mobile uav cluster interference algorithm based on online bss for multi-satellite mimo communication system with ffr," in *2024 IEEE 7th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, vol. 7. IEEE, 2024, pp. 1632–1640.

[159] C. Liao, K. Xu, X. Xia, G. Hu, C. Li, Y. Wang, W. Xie, X. Yang, Y. Shi, and L. Wan, "Irs-assisted anti-jamming transmission for an integrated satellite-uav-terrestrial network with imperfect csi: A game-based perspective," *IEEE Internet of Things Journal*, vol. 10, no. 23, pp. 20 484–20 497, 2023.

[160] C. Liao, K. Xu, H. Zhu, X. Xia, Q. Su, and N. Sha, "Secure transmission in satellite-uav integrated system against eavesdropping and jamming: A two-level stackelberg game model," *China Communications*, vol. 19, no. 7, pp. 53–66, 2022.

[161] X. Ren, J. Cao, R. Ma, Y. Luo, J. Guan, Y. Zhang, and H. Li, "A novel access and handover authentication scheme in uav-aided satellite-terrestrial integration networks enabling 5g," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 3880–3899, 2023.

[162] A. S. Editya, T. Ahmad, H. Studiawan, and S. Silalahi, "Yolofor: Yolo and optical flow for forensic analysis of attacked drone case," *ICIC Express Letters, Part B: Applications*, vol. 14, no. 12, pp. 1285–1293, 2023.

[163] A. Adel and T. Jan, "Watch the skies: a study on drone attack vectors, forensic approaches, and persisting security challenges," *Future internet*, vol. 16, no. 7, p. 250, 2024.

[164] Z. Baig, M. A. Khan, N. Mohammad, and G. B. Brahim, "Drone forensics and machine learning: Sustaining the investigation process," *Sustainability*, vol. 14, no. 8, p. 4861, 2022.

[165] T. Wierzbicki, "Investigating drones using open-source forensic software," Ph.D. dissertation, Monterey, CA; Naval Postgraduate School, 2020.

[166] B. Z. Téglásy, E. Wengle, J. R. Potter, and S. Katsikas, "Authentication of underwater assets," *Computer Networks*, vol. 241, p. 110191, 2024.

[167] P. Casari, R. Diamant, S. Tomasin, J. Neasham, L. Lampe *et al.*, "Practical security for underwater acoustic networks: published results from the safe-ucomm project," in *PROCEEDINGS OF FORUM ACUSTICUM*. European Acoustics Association, 2023, pp. 5685–5692.

[168] W. Shafik, S. M. Matinkhah, and F. Shokoor, "Cybersecurity in unmanned aerial vehicles: A review," *International Journal on Smart Sensing and Intelligent Systems*, vol. 16, no. 1, 2023.

[169] M. Kang, S. Park, and Y. Lee, "A survey on satellite communication system security," *Sensors*, vol. 24, no. 9, p. 2897, 2024.

[170] C. Wu, X. Wang, Y. Hu, S. Han, and D. Niyato, "Interplay between ai and space-air-ground integrated network: The road ahead," *arXiv preprint arXiv:2505.09259*, 2025.

[171] S. Islam, M. Z. H. Bhuiyan, M. Liaquat, I. Pääkkönen, and S. Kaasalainen, "An open gnss spoofing data repository: characterization and impact analysis with fgi-gsrx open-source software-defined receiver," *GPS Solutions*, vol. 28, no. 4, p. 176, 2024.

[172] A. Lemmenes, P. Corbell, and S. Gunawardena, "Detailed analysis of the texbat datasets using a high fidelity software gps receiver," in *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, 2016, pp. 3027–3032.

[173] L. Marata, M. Z. H. Bhuiyan, and E. S. Lohan, "On cross-testing datasets for rf-fingerprinting based deep-learning gnss spoofing detection," in *2025 IEEE 26th International Workshop on Signal Processing and Artificial Intelligence for Wireless Communications (SPAWC)*. IEEE, 2025, pp. 1–5.

[174] M. Zhang, P. Parsch, H. Hoffmann, and A. Masrur, "Analyzing can's timing under periodically authenticated encryption," in *Proceedings of the 25th Design, Automation and Test in Europe Conference (DATE)*, Antwerp, Belgium, 2022.

[175] M. Lewis, H. Li, and K. Sycara, "Deep learning, transparency, and trust in human robot teamwork," in *Trust in Human-Robot Interaction*, C. S. Nam and J. B. Lyons, Eds. Elsevier, 2021, pp. 321–352.

Appendices

Tables

The distribution in Table 6 highlights a strong concentration of research on RF wireless links during the operational phase, which reflects the predominance of jamming, spoofing, and PHY/MAC–layer attacks in current UxV security literature. Satellite-based channels, largely associated with GNSS spoofing and Satcom integrity, form the second most represented category, while optical and acoustic channels remain comparatively niche. Wired and tethered links appear infrequently, mostly in pre-deployment analyses of onboard protocols. Notably, explicit post-deployment investigations involving a clearly identified communication channel are almost absent from titles, indicating that forensic and incident-analysis studies rarely specify the underlying link type at the abstract or title level. This asymmetry suggests that the literature prioritizes real-time threat models over post-incident evidence pathways, leaving a gap in channel-aware forensic methodologies.

Table 7 maps the high-level attack classes observed in the survey to the dominant defense strategies of prevention, detection, and recovery. The pattern shows that eavesdropping is treated almost exclusively as a preventive problem, whereas jamming, MITM, supply-chain tampering, and malware/backdoor injection benefit from more balanced, multi-stage defenses. Spoofing sits in an intermediate position with strong prevention and detection coverage but relatively little attention to post-compromise recovery, reinforcing the bias toward preemptive rather than restorative controls.

Table 8 refines the channel–phase view by differentiating across UxV domains (UAV, UGV, USV, UUV). RF links exhibit the broadest cross-domain coverage in both pre-deployment and operational phases, while acoustic and optical channels remain tightly coupled to their "native" domains (UUV and UAV, respectively). The presence of all four UxV domains in post-deployment wired/tethered studies again suggests that forensic or post-incident analyses, when they do appear, are often anchored in internal buses or diagnostic links rather than external RF or satellite interfaces.

Table 9 summarizes how mitigation strategies are distributed across the lifecycle phases. Pre-deployment work is almost entirely prevention-focused, with little emphasis on detection or recovery beyond design-time assurances. Operational-phase studies are more comprehensive, spanning all three categories, whereas post-deployment efforts concentrate on detection and recovery with almost no preventive mechanisms explicitly targeting the post-incident context. This reinforces the earlier observation that post-deployment research is framed around incident response rather than proactive hardening.

Table 10 examines the experimental settings used to validate attacks and defenses across channels. RF wireless and satellite links show a relatively balanced mix of simulation, lab, and field tests, reflecting their operational importance and regulatory relevance. Optical and acoustic channels, by contrast, rely more heavily on simulation, with only a small number of lab and field deployments, indicating that many results are still preliminary or exploratory rather than operationally validated.

Table 11 highlights the native security features of representative UxV communication protocols and standards. Legacy or domain-specific protocols such as MAVLink, ADS-B, AIS, and JANUS lack built-in authentication, encryption, and integrity protection, making them structurally vulnerable unless encapsulated or extended. In contrast, general-purpose connectivity technologies like Wi-Fi, Bluetooth, and 4G/5G provide full cryptographic stacks, but the literature shows that these capabilities are not always correctly configured or fully leveraged in UxV deployments.

Table 12 provides a simple maturity index for evaluation practices across channels, based on realism, scenario diversity, and adherence to standards. RF wireless research scores highest on all three dimensions, consistent with its long-standing use in traditional wireless security. Optical and acoustic channels show lower scores, particularly for scenario diversity and standards adherence, underscoring the need for more systematic benchmarking and standardized testbeds beyond bespoke or simulation-only setups.

Table 13 consolidates representative attack vectors, target domains, and observable indicators of compromise. The listed effects—such as sudden navigation deviations, link-quality collapses, telemetry mismatches, and abnormal process behavior—provide concrete signals that can inform channel-aware monitoring and forensic workflows. By coupling attack descriptions with explicit references, this table can serve as a lookup resource for practitioners designing detection rules or incident triage procedures.

Table 14 offers a qualitative "heatmap" of threat coverage across channels and attack vectors. Dense clusters of checkmarks around RF wireless and satellite channels highlight extensive work on GPS spoofing, RF jamming, and MITM-style attacks, while wired/tethered and optical/acoustic links remain comparatively underexplored beyond a handful of specific phenomena (e.g., bus injection, beam degradation, spoofed echoes). The "Other" column further emphasizes that many channel-specific effects (e.g., GNSS drift, DoS, beam degradation) are treated as side observations rather than first-class threat categories.

Table 15 evaluates the depth and redundancy of defenses for each attack vector. RF jamming, MITM, and swarm Byzantine attacks benefit from multiple distinct defensive mechanisms, including recovery paths and, in some cases, standards-aligned countermeasures. In contrast, GPS spoofing, supply-chain malware, acoustic spoofing, and adversarial ML attacks are typically addressed with only one or two defenses and lack well-defined recovery workflows or standardized protections, revealing clear opportunities for more resilient, layered designs.

Table 16 summarizes the assumed adversary capabilities, targeted layers, and realism levels across the surveyed threat models. High-realism scenarios tend to focus on over-the-air RF jammers and GPS spoofers that exploit commodity hardware and open bands, whereas supply-chain actors, malicious insiders, and satellite hijackers are modeled with lower or medium realism due to their elevated access requirements. The table also makes explicit that many recent studies elevate perception and consensus

layers (e.g., adversarial ML, Byzantine swarm nodes) to first-class attack surfaces alongside traditional PHY/MAC-level adversaries.

Finally, Table 17 maps each representative attack vector to the affected layers of the communication stack. Most physical-layer threats, such as RF jamming, GPS spoofing, FSO interference, and acoustic spoofing, are confined to the PHY domain, while protocol-centric attacks (replay, MITM, swarm Byzantine behavior) span the data-link, network, and application layers. Supply-chain malware and adversarial ML perturbations appear exclusively at the application or AI model layer, reinforcing the need for cross-layer defenses that bridge classical communication security with software and perception-centric safeguards.

TABLE 6. ATTACK SURFACE COVERAGE BY COMMUNICATION CHANNEL AND LIFECYCLE PHASE. CELL VALUES INDICATE THE NUMBER OF PAPERS WHOSE TITLE EXPLICITLY ADDRESSES THAT CHANNEL–PHASE COMBINATION.

Communication Channel	Pre-Deployment	Operational	Post-Deployment
Wired/Tethered	15	10	0
RF Wireless	331	576	1
Optical (FSO)	9	13	0
Acoustic	4	6	0
Satellite (GNSS/Satcom)	58	178	0

TABLE 7. COVERAGE OF ATTACK CLASSES BY DEFENSE STRATEGY. A CHECKMARK (✓) INDICATES THE DEFENSE STRATEGY IS APPLIED TO MITIGATE THAT ATTACK CLASS, AND A CROSS (✗) INDICATES NO DOCUMENTED MITIGATION IN THAT CATEGORY.

Attack Class	Prevention	Detection	Recovery
Eavesdropping	✓	✗	✗
Jamming	✗	✓	✓
Spoofing	✓	✓	✗
Man-in-the-Middle (MITM)	✓	✓	✓
Supply-Chain Tampering	✓	✓	✓
Malware/Backdoor Injection	✓	✓	✓

TABLE 8. UXV DOMAIN COVERAGE ACROSS COMMUNICATION CHANNELS AND LIFECYCLE PHASES. EACH CELL LISTS THE VEHICLE TYPES (UAV: AERIAL, UGV: GROUND, USV: SURFACE, UUV: UNDERWATER) WITH RESEARCH COVERAGE IN THAT CHANNEL-PHASE COMBINATION; "–" DENOTES NO COVERAGE IDENTIFIED.

Communication Channel	Pre-Deployment	Operational	Post-Deployment
Wired/Tethered	UAV, UGV, USV, UUV	UAV, UUV	UAV, UGV, USV, UUV
RF Wireless	UAV, UGV, USV	UAV, UGV, USV	UAV, UGV, USV
Optical (FSO)	–	UAV	–
Acoustic	–	UUV	–
Satellite	–	UAV, USV	–

TABLE 9. MITIGATION TECHNIQUES CATEGORIZED BY LIFECYCLE PHASE. (✓: AT LEAST ONE MITIGATION OF THIS TYPE IS EMPLOYED IN THE PHASE; ✗: NO NOTABLE MITIGATION OF THAT TYPE IN PHASE.)

Lifecycle Phase	Prevention	Detection	Recovery
Pre-Deployment	✓	✗	✗
Operational	✓	✓	✓
Post-Deployment	✗	✓	✓

TABLE 10. EVALUATION SETTINGS (SIMULATION VS. LAB VS. FIELD TESTS) USED PER COMMUNICATION CHANNEL IN SURVEYED STUDIES. EACH CELL SHOWS THE NUMBER OF PAPERS UTILIZING THAT SETTING FOR THE GIVEN CHANNEL.

Channel	Simulation	Lab Experiments	Field Tests
Wired/Tethered	5	3	1
RF Wireless	15	10	5
Optical (FSO)	6	2	1
Acoustic	4	3	1
Satellite	8	5	2

TABLE 11. SECURITY FEATURES IN UXV COMMUNICATION PROTOCOLS/STANDARDS. (✓: FEATURE SUPPORTED NATIVELY; ✗: NO BUILT-IN SUPPORT.)

Protocol / Standard	Authentication	Encryption	Integrity
MAVLink	✗	✗	✗
ADS-B	✗	✗	✗
AIS (Marine)	✗	✗	✗
802.11 Wi-Fi	✓	✓	✓
Bluetooth	✓	✓	✓
4G/5G Cellular	✓	✓	✓
Acoustic (JANUS)	✗	✗	✗

TABLE 12. METRIC MATURITY INDEX SCORES (1 = LOW, 5 = HIGH) FOR EACH CHANNEL, EVALUATING REALISM OF EXPERIMENTS, SCENARIO DIVERSITY, AND USE OF STANDARD-COMPLIANT SETUPS IN THE LITERATURE.

Channel	Realism	Diversity	Standards Adherence
Wired/Tethered	3	2	4
RF Wireless	4	4	5
Optical (FSO)	2	1	1
Acoustic	3	2	3
Satellite	3	2	4

TABLE 13. REPRESENTATIVE ATTACKS ON UXV COMMUNICATION SURFACES WITH TARGET PLATFORMS, OBSERVABLE INDICATORS, AND REFERENCES

Attack Vector	Target UxV Domains	Indicators of Compromise / Attack Effects	References
GPS Spoofing	UAV, UGV, USV	Sudden location shift; deviation from planned path; GNSS lock loss; inconsistent nav outputs	[146]–[148]
RF Jamming	UAV, UGV, USV	Link quality drops; C2 loss; packet retransmissions; mission abort	[60], [61], [64], [65]
Replay Attack (MAVLink)	UAV, USV	Reused command patterns; actuator anomalies; telemetry mismatch	[50], [62], [63]
Acoustic Spoofing	UUV	False obstacle echoes; misclassified sonar readings; path deviation	[88], [92], [166]
Supply Chain Malware	UAV, UGV, USV, UUV	Hidden background processes; unexpected beaconing; malware signatures	[29], [36], [57]
FSO Interference	UAV, USV	SNR/BER spikes; loss of optical lock; tracking oscillations	[76]–[78]
Satellite Spoofing / Hijack	UAV, USV	Uplink desync; altered control plane; spoofed GNSS time/location	[153], [154], [157]
Adversarial ML Perturbation	UAV, UGV	Target confusion; wrong object detection; control oscillations	[114]–[116]
Swarm Data Injection (Byzantine node)	UAV Swarms	Unstable consensus; position conflicts; failed role verification	[107], [108], [112]

TABLE 14. THREAT COVERAGE HEATMAP: COMMUNICATION CHANNELS VS. ATTACK VECTORS

Channel	GPS Spoofing	RF Jamming	MITM	Replay	ML Attack	Supply Chain	Other
RF Wireless	✓	✓✓✓	✓✓	✓	✓	–	DoS
Optical (FSO)	–	✓	–	–	–	–	Beam Degradation
Acoustic	–	✓	–	–	–	–	Spoofed Echo
Satellite	✓✓	✓✓	✓	–	–	✓	GNSS Drift
Tethered/Wired	–	–	✓	✓	–	–	Bus Injection

TABLE 15. DEFENSE REDUNDANCY MATRIX: ATTACK VECTORS VS. DEPTH OF DEFENSIVE COVERAGE

Attack Vector	**# of Distinct Defenses**	**Recovery Path Present?**	**Standards-Aligned Defense?**	**References**
GPS Spoofing	3 (e.g., signal fingerprinting, cross-sensor validation, LSTM filtering)	✗	✗	[146]–[148]
RF Jamming	4 (e.g., frequency hopping, adaptive beamforming, redundancy switching, link shielding)	✓	✓	[60], [61], [64], [65]
Replay Attacks (MAVLink)	2 (e.g., sequence number hardening, secure checksum)	✗	✗	[62], [63]
MITM Injection	3 (e.g., session encryption, challenge-response auth, timing-based anomaly detection)	✓	✓	[50], [174]
Supply Chain Malware	2 (e.g., firmware integrity verification, air-gapped vetting)	✗	Partial (some custom policies)	[29], [36]
Acoustic Spoofing (UUV)	1 (e.g., adaptive filter authentication)	✗	✗	[88]
Adversarial ML Attacks	2 (e.g., adversarial training, dropout ensembling)	✗	✗	[114], [116]
Swarm Data Injection (Byzantine)	3 (e.g., consensus weighting, blockchain voting, role validation)	✓	✗	[107], [108]

TABLE 16. ADVERSARY CAPABILITY MATRIX: THREAT MODELS, LAYER TARGETS, AND REALISM ACROSS UXV SYSTEMS

Adversary Type	Attack Surface Access	Targeted System Layer	Realism Level	Example Effects	Representative References
Remote RF Jammer	Over-the-air access via unlicensed ISM bands	Physical (PHY)	High	Loss of C2 link, autopilot failsafe triggers, mission abortion	[60], [61], [64], [65]
GPS Spoofer	RF injection of counterfeit GNSS signals	Physical/Navigation Layer	High	UxV deviates from mission path; spoofed return-to-home; fails GPS sanity checks	[146]–[148]
MITM Attacker (UAV Ground Link)	Passive or active RF link hijack, requires physical proximity or SDR	Network / Transport	Medium	Command injection, silent telemetry drops, control override	[50], [62], [174]
Supply Chain Actor (Firmware Level)	Insider or vendor-compromised component at manufacturing or integration stage	Firmware / Application	Medium	Persistent backdoors, remote beaconing, root-level override	[29], [36], [57]
Malicious Insider (Ground Control)	Privileged operator or compromised terminal	Application / Human-Machine Interface (HMI)	Low–Medium	Bypass safety interlocks, plant false navigation data, simulate fail-safe conditions	[57], [175]
Adversarial ML Attacker	Remote access to visual inputs or data poisoning of training datasets	Perception / AI Model Layer	Medium	Target misidentification, collision risks, object confusion	[114]–[116]
Acoustic Spoofer (UUV)	Underwater emitter spoofing sonar or acoustic modems	Physical (Sonar)	Medium	Navigation deviation, false echo detections, spoofed underwater handshake	[88], [92], [166]
Satellite Signal Hijacker	Requires SDR uplink capacity (e.g., SATCOM/GNSS spoofing)	Control Plane / Comms	Low–Medium	Interception or redirection of telemetry; GPS time/position manipulation	[153], [154], [157]
Byzantine Node in Swarm	Compromised peer in decentralized coordination (authenticated access)	Consensus / Swarm Control	Medium	Instability in consensus; fake telemetry sharing; voting deadlocks	[107], [108], [112]

TABLE 17. ATTACK VECTORS MAPPED TO COMMUNICATION STACK LAYERS WITH REFERENCES

Attack Vector	Physical	Data Link	Network	Application	Representative References
GPS Spoofing	✓	–	–	–	[146]–[148]
RF Jamming	✓	–	–	–	[60], [61], [64], [65]
Replay Attack (MAVLink)	–	✓	✓	✓	[50], [62], [63]
Man-in-the-Middle (MITM)	–	✓	✓	✓	[50], [174]
Adversarial ML Perturbation	–	–	–	✓	[114]–[116]
Supply Chain Malware	–	–	–	✓	[29], [36], [57]
FSO Injection / Interference	✓	–	–	–	[76]–[78]
Acoustic Spoofing (UUV)	✓	–	–	–	[88], [92], [166]
Satellite Spoofing / Hijack	✓	–	✓	–	[153], [154], [157]
Swarm Byzantine Node	–	–	✓	✓	[107], [108], [112]

Annex A. Search Strategy, Research Questions, and Data Collection Pipeline

A.1 Research Question

This study is guided by the following research question:

> **RQ.** *What is the state of the scientific evidence on cyber attacks, vulnerabilities, and detection or defence mechanisms across all classes of Unmanned Vehicles (UxVs), including UAV, UGV, USV, and UUV platforms, over the 2015–2025 period?*

The objective is to map attack surfaces, exploited system components, vulnerable communication channels, protocol- and middleware-level weaknesses, and observable detection signals across the UxV cyber stack.

A.2 Databases Consulted

Scopus was used as the primary indexed database due to its structured metadata, expressive query language, and broad coverage of IEEE and ACM venues. Google Scholar was consulted only for backward and forward snowballing checks. IEEE Xplore and ACM DL were probed manually to confirm that no major families of UxV-security publications were missing.

The final corpus used in this SoK originates entirely from Scopus (core query plus three recall boosters).

A.3 Core Query (Q1)

The core query applied a `TITLE`-only constraint on security terms to increase precision; additional recall was recovered through RB1–RB3.

```
TITLE(
  "unmanned vehicle*" OR UxV OR UAV OR UAS OR drone*
  OR UGV OR UUV OR USV OR AUV
  AND
  (
    security OR cybersecurity OR attack*
    OR vulnerab* OR spoof* OR jamming
    OR "threat" OR "attack surface"
  )
)
AND PUBYEAR > 2014
AND PUBYEAR < 2026
AND (
  LIMIT-TO(SUBJAREA,"ENGI")
  OR LIMIT-TO(SUBJAREA,"COMP")
)
AND (
  LIMIT-TO(DOCTYPE,"cp")
  OR LIMIT-TO(DOCTYPE,"ar")
  OR LIMIT-TO(DOCTYPE,"re")
)
```

Scopus filters applied: `SUBJAREA = ENGI, COMP`; `DOCTYPE = cp, ar, re`. These filters restrict results to engineering and computer science venues and to peer-reviewed journals, conference proceedings, and reviews.
Returned: 1 925 records.

A.4 Recall Boosters (RB1–RB3)

RB1–RB3 were designed to recover relevant publications that may not contain explicit security terms in their titles but describe vulnerabilities at protocol, communication, or GNSS layers.

RB1: Protocols and Middleware (MAVLink, PX4, ROS 2, CAN bus).

```
TITLE(
  UAV OR drone* OR UxV OR UGV OR UUV OR USV
)
AND TITLE-ABS-KEY(
  MAVLink OR "MAVLink 2" OR PX4 OR ArduPilot
  OR "ROS" OR "ROS 2" OR DDS OR "SROS2"
  OR "Micro XRCE-DDS" OR uORB OR UAVCAN
  OR "CAN bus" OR SBUS OR PPM
  OR "SiK radio" OR RFD900
)
AND TITLE-ABS-KEY(
  security OR vulnerab* OR attack* OR exploit*
  OR spoof* OR jam* OR encrypt* OR auth*
)
AND PUBYEAR > 2014
AND PUBYEAR < 2026
AND (
  LIMIT-TO(SUBJAREA,"ENGI")
  OR LIMIT-TO(SUBJAREA,"COMP")
)
AND (
  LIMIT-TO(DOCTYPE,"cp")
  OR LIMIT-TO(DOCTYPE,"ar")
  OR LIMIT-TO(DOCTYPE,"re")
)
```

Returned: 371 records.

RB2: Communication and C2 Links (RF, LTE/5G, SATCOM).

```
TITLE(
  UAV OR drone* OR UxV OR UGV OR UUV OR USV
)
AND TITLE-ABS-KEY(
  "command and control" OR "C2 link" OR telemetry
  OR "RC link" OR "433 MHz" OR "915 MHz"
  OR "2.4 GHz" OR "802.11" OR "Wi-Fi"
  OR LTE OR "4G" OR "5G"
  OR SATCOM OR Iridium
  OR "mesh network" OR MANET
  OR "Remote ID" OR "ADS-B"
)
AND TITLE-ABS-KEY(
  jam* OR spoof* OR "denial of service"
  OR interference OR encrypt*
  OR authentication OR "key management"
)
AND PUBYEAR > 2014
AND PUBYEAR < 2026
AND (
  LIMIT-TO(SUBJAREA,"ENGI")
  OR LIMIT-TO(SUBJAREA,"COMP")
)
AND (
  LIMIT-TO(DOCTYPE,"cp")
  OR LIMIT-TO(DOCTYPE,"ar")
  OR LIMIT-TO(DOCTYPE,"re")
)
```

Returned: 556 records.

RB3: GNSS/GPS Spoofing, Jamming, Interference.

```
TITLE(
  UAV OR drone* OR UxV OR UGV OR UUV OR USV
)
AND TITLE-ABS-KEY(
  (
    spoof* OR jam* OR interference
  )
  AND (
    GNSS OR GPS OR Galileo
    OR "satellite navigation" OR "RTK"
  )
)
AND PUBYEAR > 2014
AND PUBYEAR < 2026
AND (
  LIMIT-TO(SUBJAREA,"ENGI")
  OR LIMIT-TO(SUBJAREA,"COMP")
)
AND (
  LIMIT-TO(DOCTYPE,"cp")
  OR LIMIT-TO(DOCTYPE,"ar")
  OR LIMIT-TO(DOCTYPE,"re")
)
```

Returned: 538 records.

A.5 Merging and Deduplication

All Scopus exports (Q1, RB1, RB2, and RB3) were merged and harmonised at the column level. Deduplication proceeded in two stages:

1) Normalised DOI (lowercased and trimmed) as primary key.
2) Normalised title (punctuation stripped, case-folded) for entries with missing DOIs.

The resulting dataset contains:

2 935 unique records, retrieved on 30 October 2025.

A.6 Snowballing

Backward and forward snowballing was applied to all papers included after title/abstract screening:

- Backward snowballing: inspecting references cited by each included paper.
- Forward snowballing: identifying works citing the included papers (via Scopus).

Only papers explicitly describing UxV cybersecurity threats or defences were added.

A.7 Replicability

To support reproducibility:

- All queries (Q1 and RB1–RB3) are provided in this annex.
- Retrieval date: 30 Oct 2025.
- The merged and deduplicated dataset (`deduplicated_uxv_sok.csv`) is released as supplementary material.
- Snowballing follows a transparent, manually replicable procedure.

Annex B. Inter-Rater Agreement (Cohen's κ)

This annex reports the inter-rater agreement statistics for the title/abstract screening phase. Two reviewers independently labelled each record using a three-category scheme (*include*, *exclude*, *uncertain*). Records marked *uncertain* by either reviewer were excluded from the reliability analysis, as is standard practice for PRISMA-aligned assessments. Cohen's κ was computed on the remaining binary subset.

B.1 Dataset for Agreement Analysis

After removing all records with at least one *uncertain* label, the agreement dataset consisted of:

$$N = 2\,919 \text{ records.}$$

The binary include/exclude decisions for the two reviewers produced the 2×2 contingency table in Table 18.

The cells sum to 2 919 records, confirming completeness of the binary subset.

TABLE 18. 2×2 AGREEMENT MATRIX FOR BINARY INCLUDE/EXCLUDE DECISIONS.

	Rev. B: include	**Rev. B: exclude**
Rev. A: include	1865	19
Rev A: exclude	9	1026

B.2 Computation of Cohen's κ

Let:

$p_o =$ observed agreement, $\quad p_e =$ expected agreement by chance.

Cohen's κ is defined as:

$$\kappa = \frac{p_o - p_e}{1 - p_e}.$$

Using the contingency table:
- Observed agreement:

$$p_o = \frac{1865 + 1026}{2919} = 0.9904.$$

- Expected agreement:

$$p_e = \frac{(1865 + 19)(1865 + 9) + (9 + 1026)(19 + 1026)}{2919^2} = 0.5413.$$

Thus,

$$\kappa = \frac{0.9904 - 0.5413}{1 - 0.5413} = 0.9791.$$

B.3 Confidence Interval

A non-parametric bootstrap (multinomial resampling of the four cell frequencies, 10^5 iterations) was used to estimate the sampling distribution of κ. The resulting 95% confidence interval was:

$$\kappa_{95\%\,CI} \in [0.9709,\ 0.9865].$$

B.4 Interpretation

Following conventional benchmarks, values above 0.80 represent *almost perfect* agreement. The estimate $\kappa \approx 0.98$ indicates extremely high concordance between reviewers.

B.5 Full-text assessment of uncertain records

During the screening phase, 16 records were labelled as "uncertain" by at least one reviewer and were therefore retrieved for full-text analysis. This verification focused on the presence of security-relevant content (threat model, attack feasibility, or defensive evaluation). Fifteen studies satisfied all predefined inclusion criteria and were included in the final corpus. One record, although initially flagged as potentially relevant, did not contain any actual security analysis and was excluded. All decisions were reached through consensus without requiring arbitration.

Annex C. Data Extraction Codebook and Dataset Schema

This annex summarizes the data extraction schema used to derive the machine-readable corpus analyses in this SoK. Extraction was performed manually following a structured codebook to ensure consistency across UxV domains and communication media.

C.1 Extraction Fields

For each included study, the following fields were extracted:

- **Metadata:** title, authors, venue, year, DOI.
- **Vehicle domain:** UAV, UGV, USV, or UUV (multi-domain allowed).
- **System component:** C2 link, GNSS, sensors/actuators, middleware (ROS/ROS 2, MAVLink, PX4/ArduPilot), in-vehicle networks (CAN/ECUs), backhaul (SATCOM, 4G/5G, Wi-Fi/802.11).
- **Attack vector:** jamming, spoofing, injection, replay/MITM, firmware/config manipulation, protocol misuse.
- **Adversary goal:** confidentiality, integrity, availability, safety impact (one or more).
- **Evaluation setup:** simulation, laboratory, field, datasets, metrics.
- **Proposed defences:** mechanism type, assumptions, validated effectiveness.
- **Taxonomy mapping:** communication medium $\times$ lifecycle phase (pre-deployment, operational, post-deployment).

C.2 Codebook Summary

Each field follows a controlled vocabulary:

- **Vehicle domain:** enumerated (UAV/UGV/USV/UUV).
- **System components:** normalised to one of the stack layers: *C2 link*, *Positioning*, *Sensing/Actuation*, *Middleware*, *Internal networks*, *Backhaul*.
- **Attack classes:** grouped into *interference/jamming*, *spoofing/deception*, *injection/MITM*, *configuration/firmware compromise*.
- **Lifecycle phases:** *pre-deployment*, *operational*, *post-deployment*.

Ambiguous terminology in source papers (e.g., "GPS spoofing", "navigation deception", "malicious PVT injection") was normalised to a single attack label. Middleware variants (ROS 1/2, DDS, SROS2, Micro XRCE-DDS) were grouped under *middleware/protocol layer*.

C.3 Data Structure

The structured dataset produced through this extraction process contains one entry per included study with all fields of the codebook applied uniformly. The dataset is maintained in tabular form and follows the controlled vocabulary described above. A machine-readable version can be generated from the extraction template upon request.

Annex D. Grey Sources Consulted

This annex summarises representative grey sources examined to complement the academic corpus. These materials informed terminology, operational context, and real-world threat models but were not included in the quantitative dataset to preserve replicability. The list below is not exhaustive and is organised by category.

D.1 Security Advisories and Vulnerability Reports

- National Vulnerability Database (NVD) summaries of UxV-related protocol and firmware issues (e.g., MAVLink, PX4, ROS 2).
- CISA and ICS advisories on UAV control links, GNSS interference, and operational guidance for critical infrastructure.
- Vendor advisories for autopilot firmware and radio modules (e.g., SiK, RFD900, CAN-based actuator controllers).

D.2 Aviation and Navigation Safety Bulletins

- ICAO, EASA, and national aviation authority notices on GNSS jamming and spoofing affecting commercial and unmanned aircraft.
- Incident reports documenting interference in civil airspace, cross-border regions, and conflict zones.

D.3 Policy and Governance Documents

- CISA, DHS, and related agencies: secure-by-design procurement guidelines for UxVs and critical-infrastructure operations.
- Government memoranda on privacy, data retention, and cloud exposure risks associated with UxV telemetry and sensor payloads.

D.4 Industry and Vendor Documentation

- Technical manuals and protocol specifications for UxV middleware (e.g., MAVLink, PX4, ROS 2, DDS variants).
- Radio link and onboard network documentation (e.g., 802.11/2.4 GHz, LTE/5G backhaul modules, CAN/ECU interfaces).

D.5 Counter-UAS and Operational Guidance

- Public-safety best practice guides for UxV detection, incident response, and risk management.
- Security agency briefs on emerging threats from UxV misuse and physical–cyber blended attack scenarios.

Grey sources provided operational grounding and contextual insight into real-world UxV deployments. However, their variability in structure, verification, and update frequency motivated our decision not to include them in the quantitative corpus.