Intelligent Automation & Soft Computing

Tech Science Press

https://doi.org/10.32604/iasc.2026.082765

ARTICLE

Cybersecurity Threat Modeling and Privacy Risk Assessment in Collaborative Civilian UAV Systems

Ahmed Murtaza[1], Abdullah Memon[2], Sana Hafeez[3], Muzammil Ali[2] and Ghulam E Mustafa Abro[4,*]

[1]Department of Information Technology, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Pakistan
[2]Department of Control & Instrumentation Engineering, King Fahd University of Petroleum & Minerals (KFUPM), Dhahran, Saudi Arabia
[3]Digital Innovation Research Institute, School of Computer Science & Mathematics, Liverpool John Moores University, Liverpool, UK
[4]Research Unit for Robophilosophy and Integrative Social Robotics (RISR), Aarhus University, Aarhus, Denmark

*Corresponding Author: Ghulam E Mustafa Abro. Email: Mustafa.abro@ieee.org

Received: 22 March 2026; Accepted: 15 July 2026; Published: 28 August 2026

ABSTRACT: Civilian Unmanned Aerial Systems (UAS) are increasingly deployed in smart-city monitoring, infrastructure inspection, logistics, and emergency response applications. However, their integration with wireless networks, cloud services, and AI-driven analytics significantly expands cybersecurity and privacy risks. Existing studies mainly focus on isolated technical vulnerabilities such as GNSS spoofing, jamming, and communication attacks, while lacking a unified framework that systematically connects cyber threats with quantitative privacy risk assessment. To address this research gap, this study proposes a layered threat-modeling framework for collaborative civilian UAS based on multidimensional attack-surface analysis and STRIDE-oriented threat mapping. In addition, a quantitative privacy risk model is developed by integrating compromise likelihood, data sensitivity, contextual amplification, downstream misuse potential, and regulatory exposure. The proposed framework is evaluated through three representative deployment scenarios: smart-city surveillance, critical infrastructure monitoring, and mega-event security operations. The findings demonstrate that technical compromises in UAS ecosystems can propagate into large-scale societal and privacy harms, particularly in highly connected urban environments. The study contributes a structured cybersecurity and privacy assessment methodology, a UAS-specific privacy risk quantification model, and engineering as well as governance-oriented mitigation strategies to support resilient, privacy-aware, and regulation-compliant civilian UAS deployment.

KEYWORDS: Unmanned aerial systems; cybersecurity; privacy risk; threat modeling; civilian UAV; attack surface; risk quantification; resilience engineering

1 Introduction

1.1 Growth of Civilian UAV Deployment

Civilian and commercial UAVs now support parcel delivery, urban traffic monitoring, infrastructure inspection, environmental sensing, journalism, and entertainment, often operating as part of larger smart city and industrial internet of things (IIoT) infrastructures [1,2]. Reductions in cost, high payload capacity, and enhanced autonomy have facilitated dense UAV deployments and increasingly complex multi-UAV operations, such as flying ad hoc networks (FANETs), and Internet of UAVs (IoUAV) designs [2,3]. These systems are increasingly being combined with terrestrial 4G/5G networks, edge/cloud networks, and city

data platforms, which is making UAS an essential cyber-physical infrastructure in urban settings [2,4]. With this growth, there are proportions of exposure to cyber-attacks and breaches of privacy. UAVs fly in open-air space, are dependent on wireless and GNSS, and are commonly equipped with powerful imaging payloads, which impose both safety and privacy externalities on bystanders and critical infrastructure [5,6]. Cases around airports and major events prove that drones may be misused, interfere with operations, pose safety risks, and be used to conduct illegal surveillance [7,8].

1.2 Convergence of Cybersecurity and Privacy

The essence of civilian UAS lies in being data-centric: the applications require sensor data, RGB video, LiDAR, thermal imagery, RF measurements, and derived analytics, with most frequently a personal or sensitive contextual background [6]. The privacy risks are increased by:

- Continuous, large area aerial surveillance capabilities, such as high resolution and multi-sensor fusion [9].
- Integration with networked backends (LTE/5G, Wi-Fi, satellite links, edge and cloud services) that expose the airframe to having a larger attack surface [2,3].
- Use of machine learning and AI analytics on the collected data, which can be used to re-identify, infer sensitive attributes, and perform large-scale behavioural profiling [5,10].

The surveys of UAV security and privacy also have a consistent theme that confidentiality and privacy are first-order security requirements, rather than second in line with safety and availability [3,6].

1.3 Motivation and Research Gap

The issue of UAV security has been considered for a long time, but the preponderance of the technical discussion still deals with the threats of integrity and availability of navigation information, which comprise spoofing, jamming, and link-level denial-of-service attacks. Although the vectors are admittedly important to the level of flight safety, they fail to adequately reflect the overall privacy and societal implications of the breach of civilian unmanned aerial systems (UAS) when civilians are the victims of the threat. Several gaps in structure encourage this manuscript:

- **Disjointed threat modeling solutions:** The present analyses often take traditional cyber-technology security models and do not appreciate the cyber-physical intimacy, mobility limitations, sensing potential, and regulatory vulnerability peculiar to UAS. Consequently, the threat surfaces can be characterized incompletely.
- **Lack of quantitative formulations of privacy risks:** The breach of privacy is usually characterized in qualitative or situation-based terms. Nevertheless, not many systematic approaches exist to transform the possibility of attacks, sensitivity of data, operational environment, and the magnitude of exposure into formal risk measures that can be used by engineers to make trade-offs.
- **Inadequate interaction between technical tradeoff and societal effect:** UAS-related security breaches may not just impact the individual systems but also affect the entire population in terms of safety, resilience of critical infrastructures, civil liberties, and trust in autonomous technologies. These downstream effects are normally talked of in a narrative and not in the framework of systematic risk assessment models.
- **Lack of specific threat modeling guidelines:** When dealing with the UAS, there is a tendency to use generalized threat modeling paradigms that were initially designed to be used in non-dynamic IT systems. These strategies are insufficient to support the UAS-specific limitations, such as real-time control loops, airspace integration, distributed sensing, and physical mobility across jurisdictional borders.

Despite the recent initiatives to format the UAV threats in hardware, software, and communication, sensing strata, an overall framework is still needed that integrates critical threat modeling and formal quantification of the privacy exposure and direct interpolation of system-level compromise to societal risk. The manuscript meets this requirement by suggesting a systematic approach to the civilian UAS architectures, making it possible to evaluate cybersecurity threats systematically and to quantify the privacy impact. Unlike existing UAV cybersecurity studies that primarily focus on isolated attack vectors, communication security, or qualitative privacy discussions, the proposed framework introduces an integrated cyber-physical and privacy-aware assessment methodology specifically tailored for civilian UAS ecosystems. The originality of this work lies in the systematic fusion of layered STRIDE-based threat modeling, multidimensional attack-surface analysis, quantitative privacy-risk propagation, and governance-aware contextual assessment within a single unified framework. In addition, the proposed model explicitly connects technical compromise pathways with societal and regulatory consequences through exposure, contextual amplification, downstream misuse potential, and compliance-aware risk metrics. This enables a more comprehensive evaluation of civilian UAS deployments in smart-city surveillance, critical infrastructure protection, and mega-event environments, thereby extending beyond conventional vulnerability-centric UAV security analyses.

1.4 Research Contributions and Innovations

This study contributes to the civilian UAS cybersecurity and privacy literature at three complementary levels. First, from a theoretical perspective, the work extends traditional STRIDE-oriented threat modeling toward collaborative, AI-enabled, and privacy-aware civilian UAS ecosystems by integrating societal, regulatory, and contextual risk dimensions into cyber–physical security analysis. Second, from a methodological perspective, the study proposes a unified layered framework combining multidimensional attack-surface taxonomy, quantitative privacy-risk propagation, context-aware threat assessment, and governance-oriented evaluation within a single analytical structure. Unlike many existing approaches that primarily focus on isolated communication threats, intrusion detection, or AI-driven anomaly analysis, the proposed framework systematically links technical compromise pathways to downstream societal and regulatory consequences. Third, from a practical deployment perspective, the framework supports scenario-based risk assessment for smart-city monitoring, critical infrastructure protection, mega-event operations, and collaborative UAV swarm environments, while enabling integration with federated learning, differential privacy, lightweight blockchain, and adaptive intrusion-detection mechanisms for resilient real-world implementation.

2 Civilian UAS Architecture and Data Flows

2.1 Layered System View

Recent literature and system-level analyses consistently characterize civilian UAS as a layered cyber–physical architecture comprising: (i) the physical platform and sensing payloads, (ii) onboard computing and software components, (iii) communication and networking subsystems, (iv) ground control and backend infrastructures, and (v) user, governance, and regulatory layers. Such a layered representation facilitates systematic analysis of attack surfaces, data propagation pathways, cybersecurity threats, and privacy-sensitive interactions across the entire UAS ecosystem [3,6]. This layered view is necessary for mapping attack surfaces and privacy flow. Fig. 1 illustrates the layered decomposition of civilian UAS architectures and highlights how mission data propagates across physical, computational, and networked domains. The figure emphasizes that privacy exposure is not confined to onboard sensors but extends across backend analytics and governance layers, significantly expanding the effective attack surface.

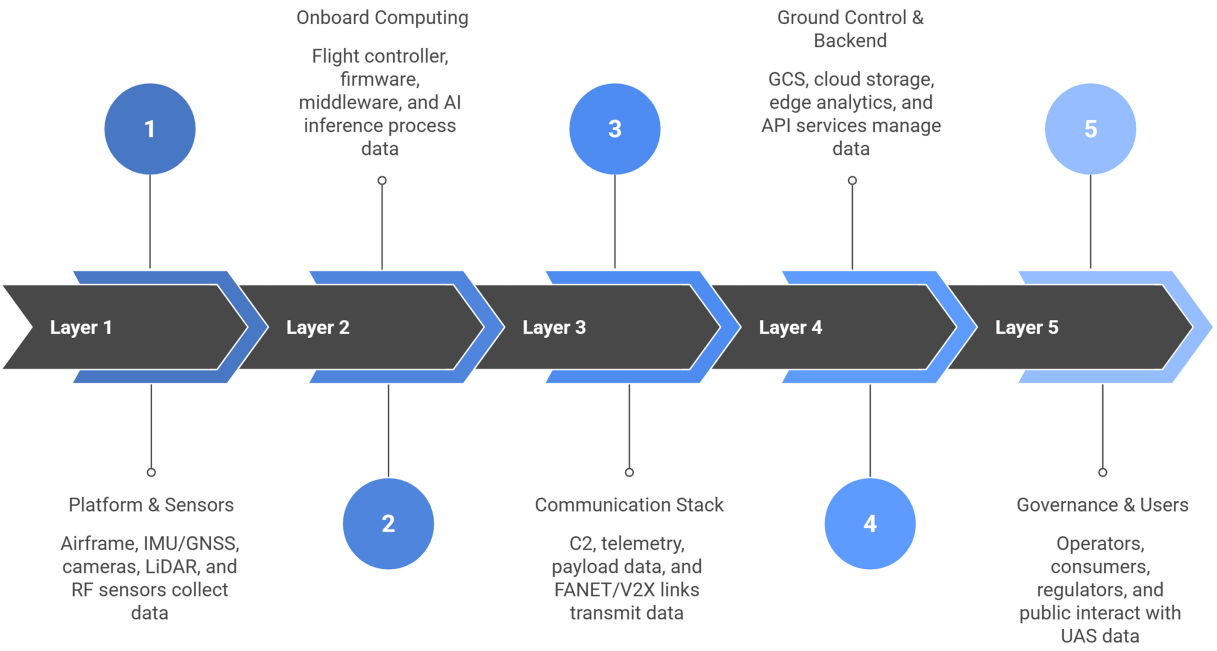

Figure 1: Layered civilian UAS architecture and data flow.

- **Platform and Sensors:**
  - Airframe, propulsion, navigation sensors (IMU, barometer, magnetometer, GNSS), and mission payload sensors (RGB/IR cameras, LiDAR, RF receivers).
  - Vulnerable to sensor spoofing, physical tampering, and side channel leakage [1,4].
- **Onboard Computing and Software:**
  - Flight controller firmware, operating system, middleware, and application logic.
  - Exposed to malware injection, firmware tampering, privilege escalation, and unsafe update mechanisms [3,11].
- **Communication Stack:**
  - C2 links (proprietary RF, Wi-Fi, LTE/5G, satellite), data links for telemetry and payload data, V2X for swarm/FANET coordination [4,12].
  - Susceptible to eavesdropping, man-in-the-middle, jamming, spoofing, routing attacks, and Sybil behavior [2,12].
- **Ground Control Stations (GCS) and Backend Service:**
  - Operator consoles, mission planning systems, cloud/edge analytics, storage, and integration with other critical infrastructures (e.g., traffic management, smart city platforms) [2].
  - Vulnerabilities mirror broader IoT and cloud threats: weak authentication, API abuse, misconfigured storage, and supply chain compromise [6].
- **Users and Governance Layer:**
  - Human operators, third-party data consumers, regulators, and affected communities.
  - Policy frameworks (e.g., GDPR style privacy regulations in the EU) and UAV-specific rules mediate acceptable use and redress mechanisms [5,6].

This architecture allows structured mapping from technical weaknesses to privacy-relevant data flows (for example, who can access the video streams, analytics outputs at each stage, or trajectory logs).

Table 1 consolidates the layered architecture described above by mapping each layer to its typical data assets, dominant threat classes, and representative technical/governance controls.

Table 1: Layered civilian UAS architecture: mapping of components, privacy-sensitive assets, threat classes, and representative controls.

Layer	Representative Components	Privacy-Sensitive Data Assets	Dominant Threats (STRIDE Mapping)	Representative Security & Privacy Controls
Platform & Sensors	Airframe, IMU, GNSS, RGB/IR camera, LiDAR	Raw imagery/video, bystander faces/plates, RF captures	Sensor spoofing, physical tampering, covert recording	Tamper-evidence, secure mounting, sensor fusion sanity checks
Onboard Computing & Software	Flight controller firmware, OS, middleware	Logs, stored frames, model weights	Firmware tampering, malicious updates, privilege escalation	Secure boot, signed OTA updates, least privilege
Communication Stack	C2 link (RF/LTE/5G), telemetry, payload data link	Telemetry, live video streams, cryptographic keys	Eavesdropping, MITM, jamming, replay attacks	Mutual authentication, encryption, anti-jamming modes, key rotation
GCS & Backend	Mission planner, cloud storage, analytics pipeline	Stored video, analytics outputs, identity inferences	API abuse, misconfigured storage, supply chain attacks	IAM, logging and audit, secure APIs, storage policy-as-code
Users & Governance	Operators, regulators, third parties	Data-sharing agreements, retention policies	Insider misuse, unlawful repurposing, compliance failure	DPIA/PRAM-style risk assessment, access governance, retention limits

Note: This table maps the layered civilian UAS architecture to associated privacy-sensitive assets, dominant threat classes aligned with STRIDE, and representative mitigation controls across technical and governance domains.

The proposed layered architecture distinguishes between physical sensing, onboard decision-making, communication coordination, backend intelligence processing, and governance/regulatory supervision layers to enable clearer attack-surface attribution and mitigation mapping. In collaborative UAV ecosystems, additional inter-layer dependencies emerge through swarm coordination channels, distributed sensing fusion, cooperative mission planning, and cross-domain supervisory infrastructures such as UTM integration. These collaborative interactions introduce new attack surfaces involving consensus manipulation, trust poisoning, synchronized routing attacks, and cascading compromise propagation across interconnected UAV fleets. Explicit separation of these architectural boundaries enables more systematic analysis of threat propagation paths and layered defense strategies in large-scale civilian UAS deployments.

2.2 Data Lifecycles and Privacy Sensitive Assets

The threat model developed with privacy in mind should cover the complete data life cycle, i.e., collection, transmission, processing, storage, sharing, and deletion. Modern surveys and regulatory studies indicate that there are several sets of privacy-sensitive data in civilian UAS [5,6]:

- **Direct identifiers:** faces, license plates, home addresses visible in imagery.

- **Location:** mobility traces and the location of individuals and vehicles.
- **Operational metadata:** timestamps, flight plans, mission logs that can show patterns of surveillance or infrastructure surveillance that is important.
- **Contextual inferences:** behavioral patterns, social interactions, or sensitive locations of facilities through analytics.

Zhi et al. emphasize that despite the innocent sharing of images on social media, the metadata (time, location) embedded in the images, as well as the visual context, may cause privacy leakage [9]. Extensive UAV security/privacy surveys also define commercial drone privacy intrusion, like voyeuristic surveillance, targeted surveillance, and mass surveillance [6]. Under regulatory review, most of the jurisdictions handle UAV information within general digital privacy regulations without much specific guidance on UAVs, although there are unique aerial surveillance risks [5]. To operationalize the data-lifecycle discussion, Table 2 characterizes each privacy-sensitive asset class by its identifiability, sensitivity, and exposure points across the lifecycle.

Table 2: Privacy-sensitive data assets in civilian UAS: identifiability, sensitivity, lifecycle exposure points, and recommended protections.

Data Asset Class	Examples	Identifiability	Sensitivity	Highest-Risk Lifecycle Stages	Practical Protections
Direct identifiers	Faces, plates, address imagery	High	High	Collection, sharing, storage	On-device redaction, access control, retention limits
Location traces	UAV path, subject mobility trace	Medium–High	High	Transmission, correlation/analytics	Encryption-in-transit, minimization, aggregation
Operational metadata	Flight plans, mission logs, timestamps	Medium	Medium–High	Storage, sharing with vendors	Role-based access, audit logs, need-to-know
Contextual inference outputs	Crowd density maps, identity re-ID	High	Very High	Processing, secondary use	Purpose limitation, review gates, bias/privacy checks

Note: This table summarizes privacy-sensitive data categories in civilian UAS along with their identifiability, sensitivity levels, lifecycle exposure points, and corresponding protection mechanisms.

3 UAV Cyber Threat Landscape and Taxonomies

3.1 Dimensions of the Attack Surface

The recent survey suggests multi-dimensional taxonomies to differentiate between the threat vectors, dependent on the architectural level and security objectives [3,6]. Consolidated view considers:

- **Attack level:** sensor, hardware, software, communication, network, multi-UAV/swarm, and supply chain [3,6].
- **Targeted security property:** confidentiality, integrity, availability, privacy, authentication, non-repudiation [6,13].
- **Physical vs. logical vectors:** Physical capture/tampering vs. all cyber exploits [12].

As illustrated in Fig. 2, UAV threats cannot be classified along a single axis. Instead, a multidimensional taxonomy enables structured mapping of attacks to both system components and violated security properties, facilitating systematic risk scoring and mitigation prioritization.

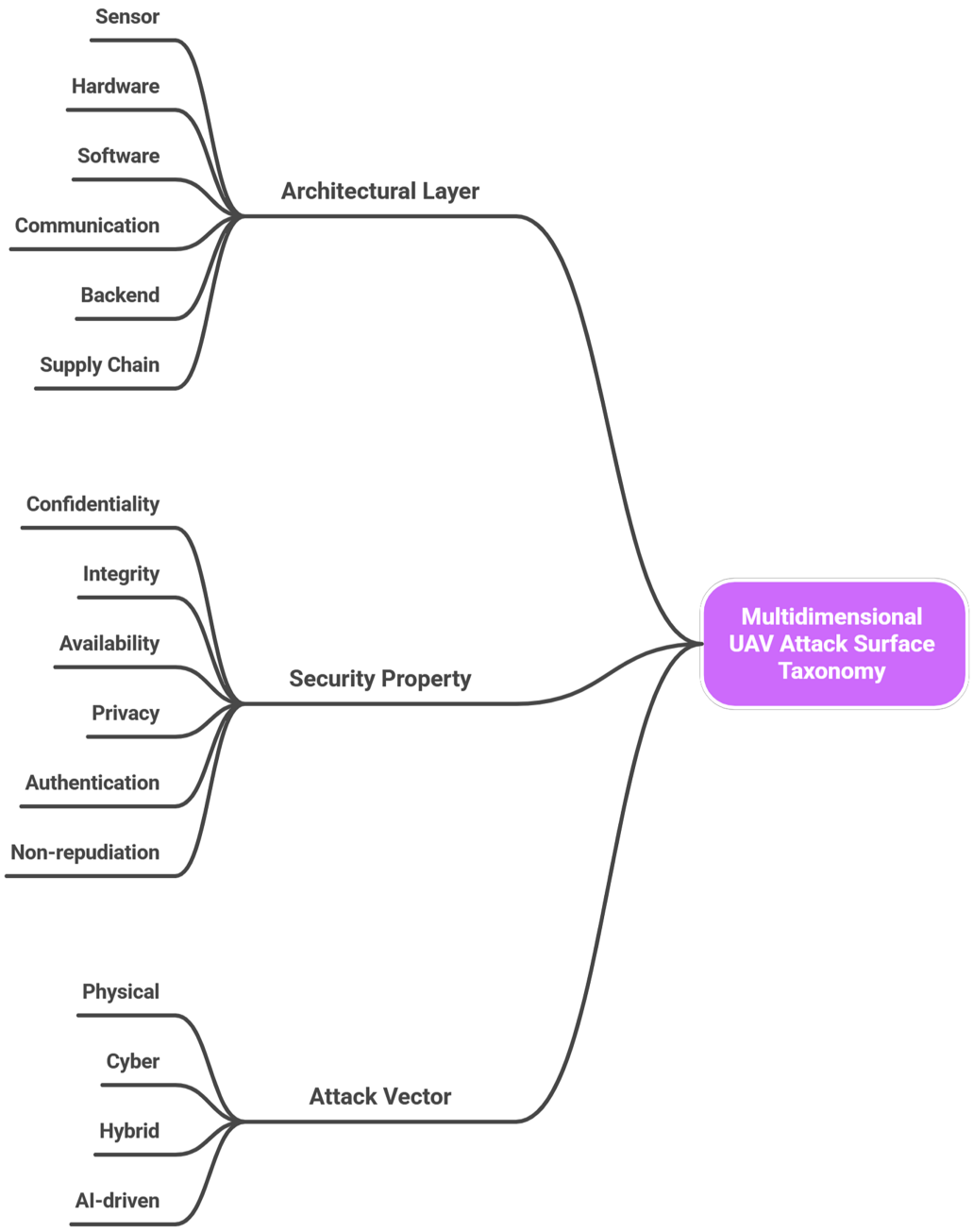

Figure 2: Multidimensional UAV attack surface taxonomy.

Mekdad et al. categorize the attacks as sensor, hardware, software, and communication-level threats and clearly identify the vulnerability, attacks, and countermeasures associated with each [6]. Bai et al. go further and present a list of threat groups, which includes physical, malware, sensor, communication, network, and supply chain, hardening defects, and a gap analysis is provided [3]. Beyond conventional

STRIDE-oriented cyber threats, large-scale civilian UAS ecosystems introduce additional attack dimensions associated with collaborative swarm coordination, AI-driven perception systems, and cross-airspace supervisory infrastructures. Swarm-oriented threats include distributed consensus manipulation, Sybil-assisted swarm deception, coordinated routing disruption, and malicious inter-UAV trust propagation. AI-enabled perception systems further introduce vulnerabilities related to adversarial image perturbation, sensor poisoning, model inversion, and inference manipulation within autonomous navigation and surveillance pipelines. In addition, cross-airspace supervisory integration with smart-city infrastructure, UTM systems, and multi-jurisdictional regulatory coordination expands the attack surface beyond isolated UAV platforms toward interconnected cyber–physical ecosystems. These emerging dimensions extend traditional STRIDE analysis and motivate the need for context-aware, collaborative, and AI-sensitive threat modeling for next-generation civilian UAS deployments.

3.2 Representative Attack Classes

In surveys and analyses based on the STRIDE framework, several attack categories recur as the main ones with the civilian UAVs [12,14]:

- **Spoofing and Impersonation:**
  - GNSS spoofing to mislead navigation; identity spoofing of UAVs or GCS; fake beacons in FANETs.
  - Maps to STRIDE "spoofing" and jeopardizes both safety and privacy (e.g., redirecting a surveillance drone to new targets).
- **Tampering and Malware Injection:**
  - Firmware modification, configuration tampering, malicious updates, payload manipulation.
  - Enables persistent compromise, covert surveillance, or data exfiltration.
- **Information Disclosure and Eavesdropping:**
  - Sniffing unencrypted telemetry or video streams; exploiting weak cryptography or key management; inference attacks on encrypted traffic [9].
  - Directly harmful to privacy when personal data is exposed.
- **Denial of Service (DoS) and Jamming:**
  - RF jamming of C2 links, resource exhaustion attacks on onboard or backend systems, routing layer flooding in FANETs [14].
  - Primarily affects availability but may cause secondary safety and societal failures (e.g., loss of control in overcrowded areas).
- **Privilege Escalation and Hijacking:**
  - Gaining unauthorized control over flight or payload; man-in-the-middle takeover of C2 sessions [6].
  - Blurs lines between cyber intrusion and physical attack, enabling targeted spying or weaponization.
- **Privacy Invasion Surveillance Attacks:**
  - Intentional misuse of legitimately controlled UAVs for illegal observation, covert recording, and tracking individuals without consent [6].
  - Compound when combined with data fusion and long-term storage.

Table 3 maps the representative attack classes to STRIDE categories and explains the primary pathway from technical compromise to privacy harm.

Table 3: Representative UAS attack classes mapped to STRIDE, architectural layers, and privacy harm pathways.

Attack Vector	Primary Layer(s)	STRIDE Category	Primary Security Property Violated	Typical Privacy Harm Mechanism	Impact
GNSS spoofing/route manipulation	Sensors, navigation	Spoofing	Integrity/ authenticity	Redirect surveillance to unintended subjects/areas	Target misidentification
Unencrypted telemetry/video capture	Comms stack	Information disclosure	Confidentiality	Exposure of identifiable imagery and location metadata	Privacy breach
Firmware/OTA update manipulation	Onboard software	Tampering/EoP	Integrity/ authorization	Persistent covert recording + data exfiltration	Long-term surveillance risk
C2 hijacking/session takeover	Comms + GCS	Spoofing/EoP	Authorization	Unauthorized operation of the payload and tracking	Loss of control
Cloud bucket misconfiguration	Backend	Information disclosure	Confidentiality	Mass leakage of stored footage + analytics outputs	Large-scale data exposure

Note: This table maps representative UAS attack vectors to STRIDE categories, affected architectural layers, violated security properties, and resulting privacy harm mechanisms.

The analysis of UAS and multi-UAV systems using STRIDE classifies these threats as spoofing, tampering, information disclosure, denial of service, repudiation, and elevation of privilege, and relates them to platform-specific mitigation measures [14]. Other issues covered under strategic risk discussions include autonomous decision-making, adversarial AI attacks, UAS use in information operations and warfare, and the spill over into civilian areas [13,15].

3.3 Emerging Threats: AI, Federated Learning, and Regulatory Misalignment

Recent research indicates the new vectors that are unique to AI-enabled and data-driven UAS:

- **Image poisoning and adversarial AI:** In intrusion detection and autonomous systems, these studies, which suggest privacy-preserving IDS and federated learning of IoUAV, also prove that there is a necessity to have a strong defense against poisoning, backdoor insertion, and gradient leakage [10,16].
- **Automated threat detection vulnerabilities:** UAVThreatBench demonstrates that, despite the strong performances of LLMs, availability-based threats, backend vulnerabilities, and regulatory clauses at the fine-grained level, these models systematically do not identify such threats when asked to reason about threats in the context of industrial UAVs [17].
- **Regulatory misalignment:** Comparative studies of privacy and safety regulations across the US, EU, and Japan indicate that the safety regulations of UAVs are much more developed compared to the privacy regulations of UAVs, which largely replicate general digital privacy regulations and do not address the specifics of aerial surveillance [5].

These advancements drive combined threat models, which involve AI pipelines, data protection requirements, and regulatory compliance requirements, into technical risk assessment. Recent UAV cybersecurity research between 2023 and 2026 has increasingly focused on AI-enabled intrusion detection, federated

learning, blockchain-assisted trust management, and LLM-based threat identification frameworks. These approaches primarily address specific operational challenges such as anomaly detection accuracy, secure distributed learning, communication integrity, or automated threat recognition. In contrast, the framework proposed in this study targets system-level cyber–physical and privacy-aware risk assessment by integrating layered STRIDE-based threat modeling, multidimensional attack-surface analysis, quantitative privacy-risk propagation, and governance-aware contextual evaluation within a unified civilian UAS framework. Consequently, the proposed methodology is complementary to AI-driven protection mechanisms and can serve as a higher-level assessment and decision-support layer for evaluating the broader societal and regulatory implications of UAV cybersecurity incidents.

While the studies reviewed in this section provide important advances in specific domains of UAV cybersecurity, their primary focus remains on individual technical mechanisms such as intrusion detection, federated learning, blockchain-assisted trust management, privacy-preserving data sharing, or automated threat identification. In contrast, the framework proposed in this work addresses a broader analytical objective by integrating cyber-physical threat modeling, privacy-risk quantification, contextual operational assessment, and regulatory exposure analysis within a unified assessment methodology. Unlike existing approaches that evaluate security performance metrics such as detection accuracy, communication resilience, or model robustness, the proposed framework explicitly traces how technical compromises propagate across sensing, communication, computation, and governance layers to produce societal, privacy, and compliance-related consequences. Furthermore, the framework is technology-agnostic and can be used to evaluate both conventional and AI-enabled UAV architectures, thereby providing a higher-level decision-support capability for risk-informed deployment, regulatory compliance, and privacy-aware system design in civilian UAS ecosystems.

To clarify the methodological gap addressed by this study, Table 4 compares representative recent UAV cybersecurity, privacy, and regulatory studies in terms of their scope, threat-modeling approach, privacy-assessment methodology, governance or regulatory consideration, and distinction from the framework proposed in this work.

Table 4: Comparative analysis of representative UAV cybersecurity and privacy-assessment studies and the proposed framework.

Study	Study Scope	Threat Model	Privacy-Assessment Methodology	Governance/ Regulatory Layer	Distinction from Proposed Framework
Mekdad et al. [6]	UAV security and privacy survey covering hardware, software, sensors, and communications	Taxonomy of UAV vulnerabilities, attacks, and countermeasures	Qualitative discussion of privacy threats and data exposure	Limited discussion of privacy and regulatory concerns	Broad security/privacy survey; does not integrate layered threat modeling with quantitative privacy-risk propagation and governance-aware assessment
Pandey et al. [12]	Security threats and mitigation techniques in UAV communications	Communication-oriented classification of attacks and countermeasures	Privacy mainly considered through confidentiality and secure communication	No explicit governance or regulatory assessment layer	Focuses primarily on communication security, whereas the proposed framework links multi-layer cyber threats to privacy, societal, and regulatory consequences

(Continued)

Table 4 (continued)

Study	Study Scope	Threat Model	Privacy-Assessment Methodology	Governance/ Regulatory Layer	Distinction from Proposed Framework
Ntizikira et al. [16]	Secure and privacy-preserving intrusion detection for the Internet of UAVs	IDS-oriented detection of network and cyber anomalies	Federated learning, differential privacy, and secure multi-party computation	No dedicated regulatory-risk modeling layer	Provides a technical privacy-preserving IDS; the proposed framework instead provides system-level threat modeling and quantitative privacy-risk assessment across the UAS ecosystem
Zhu et al. [18]	Privacy protection for blockchain-based federated learning in UAV-MEC networks	Threats associated with distributed learning, poisoning, and privacy leakage	Blockchain-assisted federated learning and adaptive gradient protection	No explicit governance or regulatory assessment	Targets privacy protection during distributed learning; the proposed framework evaluates broader cyber–physical compromise, downstream misuse, contextual amplification, and regulatory exposure
Lee et al. [5]	Comparative analysis of UAV safety and privacy regulations across jurisdictions	Regulatory and policy-oriented risk perspective rather than a technical cyber threat model	Qualitative analysis of privacy and safety requirements	Explicit cross-jurisdictional regulatory comparison	Provides strong regulatory analysis but does not integrate technical threat enumeration or quantitative privacy-risk scoring; the proposed framework combines both dimensions
Iyenghar [17]	UAV cybersecurity threat-identification benchmarking using LLMs	Dataset-driven identification of cybersecurity threats and regulatory clauses	Privacy addressed through threat and regulatory-clause identification rather than quantitative privacy scoring	Includes regulatory provisions associated with identified threats	Focuses on automated threat identification and benchmarking; the proposed framework additionally models attack surfaces, privacy-risk propagation, contextual impact, and scenario-based risk scoring
Proposed framework	Collaborative civilian UAS across sensing, onboard computing, communications, backend services, users, and governance	Layered STRIDE-based threat modeling combined with multidimensional attack-surface analysis	Quantitative privacy-risk model integrating compromise likelihood, exposure, context, downstream misuse, and regulatory impact	Explicit governance and regulatory layer incorporated into contextual risk assessment	Unifies cyber-physical threat modeling, quantitative privacy-risk propagation, societal consequences, and governance-aware assessment within one framework

Note: This table compares representative UAV cybersecurity, privacy, and regulatory studies with the proposed framework in terms of scope, threat modeling, privacy-assessment methodology, governance/regulatory consideration, and methodological distinction.

As summarized in Table 4, existing studies provide important contributions in individual areas such as communication security, intrusion detection, privacy-preserving learning, regulatory analysis, and

automated threat identification. However, these approaches generally address cybersecurity, privacy, and governance as separate or application-specific concerns. The proposed framework differs by integrating layered STRIDE-based threat modeling, multidimensional attack-surface analysis, quantitative privacy-risk assessment, contextual amplification, downstream misuse, and regulatory exposure within a unified methodology for collaborative civilian UAS. This integration enables technical compromise events to be traced systematically to privacy, societal, and governance consequences across heterogeneous deployment scenarios.

4 Formal Threat Modeling for Civilian UAS

4.1 STRIDE Derived Models for UAS Architectures

Some of the recent publications directly apply STRIDE and CPS-based threat modeling to UAS:

- Jacobsen and Marandi use multi-UAV inspection systems in the case of the application of STRIDE to map threats to specific components and rank them with the help of risk assessment to obtain security recommendations [4].
- Xi et al. expand on the idea of STRIDE to the full UAS network architecture and divide the problems into spoofing, tampering, information disclosure, DoS, service refusal, and privilege escalation, and classify them as challenges with corresponding defense measures [11].
- Enhanced UAS cybersecurity studies focus on the cyclical UAS design (including pre-design and development) and deployment to maintenance and decommissioning, such as industrial control systems and urban air mobility systems [18].

A strictly adhered to STRIDE-based approach to civilian UAS will typically go through:

- **System Decomposition:** Determine data flow diagrams (DFDs) between sensors, controllers, communication links, GCS, and backend services.
- **Threat Enumeration:** Instantiate STRIDE threat categories on each DFD element, with UAV-specific attack patterns from the surveys (e.g., GNSS spoofing, FANET routing attacks, video stream hijacking) [12,14].
- **Risk Scoring:** Estimate the likelihood and impact of each threat using characteristics that include the capabilities of the attacker, the duration of exposure, and the possible safety/privacy implications [11,14]. In line with standard risk concepts, each enumerated threat (i) can be scored as the product of likelihood and impact, as shown in Eq. (1).

$$R_i = L_i \cdot I_i \tag{1}$$

where:
R_i = risk score of threat i (dimensionless)
L_i = likelihood (probability or normalized likelihood rating) that threat i occurs/succeeds
I_i = impact (normalized impact rating) if threat i occurs, may include safety + privacy

- **Mitigation Mapping:** Extract security controls (cryptography, redundancy, IDS, operational procedures) and rank them (residual risk).

Fig. 3 operationalizes the STRIDE categories within the context of UAS architecture by explicitly mapping abstract threat classes to UAV-specific vulnerabilities. This structured mapping supports systematic threat enumeration during system design and certification.

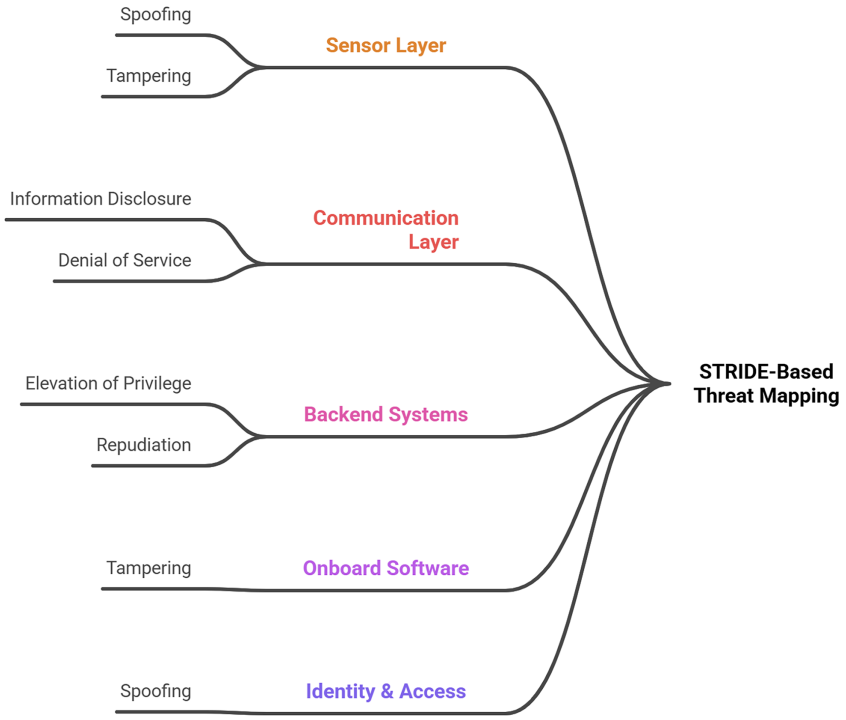

Figure 3: STRIDE-based threat mapping for civilian UAS.

Table 5 provides an example STRIDE enumeration matrix for key UAS data-flow elements, which can be adapted during system design reviews.

Table 5: STRIDE-by-component threat enumeration matrix for a civilian UAS data-flow model.

UAS Element (DFD Focus)	S	T	R	I	D	E
GNSS + navigation sensors	✓	✓	✓		✓	
Mission payload (camera/LiDAR)		✓		✓		✓
Flight controller firmware		✓	✓	✓	✓	✓
C2 link (RF/LTE/5G)	✓	✓	✓	✓	✓	✓
Ground Control Station workstation	✓	✓	✓	✓	✓	✓
Cloud API + storage	✓	✓	✓	✓	✓	✓
Mission logs/data lake		✓	✓	✓		✓

Note: This table presents a STRIDE-based threat enumeration across key UAS components. S = Spoofing; T = Tampering; R = Repudiation; I = Information Disclosure; D = Denial of Service; E = Elevation of Privilege. Checkmarks indicate the applicability of each STRIDE threat category to the corresponding UAS component.

Other threatened modeling designs, such as PASTAD, also incorporate PASTA-like, process-based approaches to UAS, combining layered architecture perspectives, mission context, and risk measures into a multi-stage process design specific to UAV deployments, such as airport surveillance [19].

4.2 Context-Aware Threat Modeling and Regulatory Constraints

Context awareness is paramount in civilian deployments: even the same technical weakness may cause very different effects on society based on the operating environment, the mission, and the regime. With

comparative regulatory studies, it is evident that differences in regulatory constraints (e.g., no-fly zones, altitude limits) or regulatory obligations (e.g., consent, data minimization under GDPR) influence the permissible behaviors in different jurisdictions [5].

An adaptable threat model is context-aware and hence includes:

- **Operational area:** city vs. rural; closeness to important infrastructure; mega event vs. routine inspection [8].
- **Stakeholder functions:** Public/private operator; law enforcement/commercial service; bystanders/data subject [6,7].
- **Legal/privacy obligations:** UAV-specific rules, general data protection regulations, and sector-specific mandates (e.g., airport security, sports event safety) [5].

The UAVThreatBench dataset gives a tangible illustration of binding threat detection to legal provisions and relates each threat to articles of the regulatory frameworks on network/resources integrity, personal information protection, and fraud/economic damage prevention [17]. This shows that technical threat modeling can be adjusted to compliance in safety-critical UAS environments.

5 Quantitative Privacy Risk Modeling for UAS

5.1 From Confidentiality Breach to Privacy Risk

UAV security surveys often equate confidentiality and privacy with closely related but different objectives, and it is necessary to clarify the meaning of confidentiality and privacy to prevent inferences and misuse that may hurt individuals and society [16]. In the case of UAS, the quantitative privacy risk models would have to take into consideration:

- **Likelihood of compromise:** conditioned on threat model and controls.
- **Volume, sensitivity, and identifiability of exposed data:** (e.g., number of individuals captured; resolution; presence of identifiers).
- **Contextual amplification factors:** including duration of observation, data fusion with other datasets, and potential adversarial uses.
- **Societal stakes:** such as exposure of critical infrastructure layouts, protest gatherings, or vulnerable populations [8].

The available literature on UAVs does provide some elements of this reasoning, but often does not bring them together into formal metrics. The privacy regulation analyses observe that the use of UAV data processing frequently involves the application of such principles as the purpose limitation, data minimization, and proportionality, which can be operationalized in risk scores [5,6].

5.2 A Layered Privacy Risk Metric

Based on these findings, we can formulate the UAS-specific privacy risk measure as:

$$I_i^{\mathrm{PRIV}} = \frac{w_E E_i + w_C C_i + w_U U_i + w_R R_i}{5(w_E + w_C + w_U + w_R)} \tag{2}$$

where:

I_i^{PRIV} = normalized privacy impact of threat i in [0, 1]

E_i = exposure score (1–5), capturing identifiability/volume of data exposed

C_i = context amplification score (1–5), capturing density/duration/situational sensitivity

U_i = downstream misuse potential score (1–5), capturing expected harmful secondary uses

R_i = regulatory/non-compliance penalty score (1–5), capturing legal exposure

w_E, w_C, w_U, w_R = weights (default 1 for equal weighting)

$$PR = \sum_{i=1}^{N} \left(P_i \, I_i^{\mathrm{PRIV}} \right) \tag{3}$$

where:

PR = overall privacy risk score for a mission/deployment (dimensionless)

N = number of threats included in the privacy-risk calculation

$P_i = P(\mathrm{Attack}_i)$ = probability of successful compromise for attack i

1. **Data Exposure Score:** It is a factor in the number of data subjects, identifiability, and sensitivity. The severity scales can be informed by surveys that record types of privacy invasions (e.g., voyeurism, stalking, wide-area surveillance) [9].
2. **Temporal/Spatial Coverage:** Longer, denser coverage increases inferential power and potential harm.
3. **Downstream Usage Potential:** Capacity of the exposed information to be associated with outer information sets or utilized in discriminating, blackmailing, or executing focused bodily assaults [5,6,16].
4. **Regulatory Non-Compliance Penalty:** Additional weight when breaches violate strong legal protections (e.g., GDPR level rules).

Table 6 defines the proposed scoring rubric and provides illustrative scores for the three deployment scenarios analyzed in Section 6. The scoring procedure follows a structured semi-quantitative risk-assessment approach adapted from the likelihood–impact principles of NIST SP 800-30. The 1–5 ordinal scale is anchored as follows: 1 = very low, representing negligible or highly limited exposure, contextual amplification, misuse potential, or regulatory consequence; 2 = low, representing limited but plausible consequences; 3 = moderate, representing meaningful consequences under realistic operating conditions; 4 = high, representing substantial exposure or consequences affecting sensitive data, operational contexts, or regulatory obligations; and 5 = very high, representing extensive exposure, severe contextual amplification, strong downstream misuse potential, or major regulatory consequences. These anchors are applied consistently to the exposure (E_i), context (C_i), downstream misuse (U_i), and regulatory (R_i) dimensions according to the characteristics of each deployment scenario.

Table 6: Privacy-risk scoring rubric (likelihood × normalized privacy impact) with illustrative scoring for the three case deployments.

Use Case	Threat Event (Example)	P(Attack)	E (Exposure 1–5)	C (Context 1–5)	U (Downstream Misuse 1–5)	R (Regulatory 1–5)	Normalized Impact I_i^{priv}	Privacy Risk (PRi)
Smart-city monitoring	Telemetry/video stream eavesdropping	0.35	5	4	4	4	0.85	0.297
Smart-city monitoring	Cloud storage/API misconfiguration	0.25	5	5	5	4	0.95	0.237
Critical infrastructure/airport	GNSS spoofing redirect + covert surveillance	0.30	4	4	5	3	0.80	0.240

(Continued)

Table 6 (continued)

Use Case	Threat Event (Example)	P(Attack)	E (Exposure 1–5)	C (Context 1–5)	U (Downstream Misuse 1–5)	R (Regulatory 1–5)	Normalized Impact I_i^{priv}	Privacy Risk (PRi)
Critical infrastructure/airport	C2 link hijacking	0.20	4	5	5	3	0.85	0.170
Mega-event deployment	Unauthorized facial recognition/over-collection	0.40	5	5	5	5	1.00	0.400
Mega-event deployment	Swarm ID spoofing + crowd tracking	0.25	4	5	4	5	0.90	0.225

Note: This table presents a privacy-risk scoring rubric combining likelihood of attack with normalized privacy impact across multiple dimensions. P(Attack) denotes the illustrative scenario-based probability of successful compromise; E = Exposure; C = Context; U = Downstream misuse potential; R = Regulatory impact. For E, C, U, and R, the ordinal scoring anchors are: 1 = very low, 2 = low, 3 = moderate, 4 = high, and 5 = very high. I_i^{priv} represents the normalized privacy impact score, and PRi denotes the resulting privacy risk. The P(Attack) values are scenario-based expert estimates used for comparative risk ranking rather than empirically calibrated attack frequencies.

The $P(\text{Attack})$ values in Table 6 are illustrative scenario-based likelihood estimates rather than probabilities derived from an empirical attack-frequency dataset. They were assigned through structured expert judgment by considering the accessibility of the attack surface, attacker capability, exposure of the relevant UAS component, known vulnerability patterns, and the security controls assumed in each scenario. Consistent with the NIST SP 800-30 approach, likelihood assessment considers both the possibility that a threat event will be initiated and the possibility that it will successfully result in compromise. The numerical probabilities are therefore used for comparative risk ranking across the representative scenarios and should not be interpreted as statistically calibrated attack frequencies [20].

The proposed 1–5 scoring mechanism is intended as a structured semi-quantitative risk-assessment approach suitable for civilian UAS environments where complete operational datasets are often unavailable due to security and privacy constraints. Although the present study does not perform formal statistical validation, the framework is designed to support future probabilistic extensions, including Bayesian risk inference, Monte Carlo uncertainty propagation, and data-driven parameter calibration. Variability in expert-defined exposure, contextual amplification, and misuse scores may influence final risk estimates; therefore, the proposed model should be interpreted as a decision-support and comparative risk-ranking framework rather than an absolute deterministic predictor. Future work will incorporate empirical UAV telemetry and attack datasets to statistically validate score distributions, confidence intervals, and sensitivity behavior across heterogeneous deployment scenarios. To further illustrate the behavior of the proposed semi-quantitative privacy-risk model, a brief sensitivity-oriented analysis can be considered by varying the principal scoring parameters associated with exposure severity, contextual amplification, downstream misuse potential, and regulatory impact. Because the privacy-risk formulation in Eq. (3) combines compromise likelihood with normalized privacy impact, incremental increases in highly weighted parameters proportionally increase the resulting privacy-risk score. In dense smart-city and mega-event deployments, the model exhibits greater sensitivity to contextual amplification and downstream misuse factors due to the higher potential for large-scale behavioral inference and secondary exploitation of collected data. In contrast, moderate variations in operational metadata exposure or regulatory weighting produce comparatively smaller changes in aggregate risk estimates. This behavior indicates that the proposed framework can support

comparative prioritization of mitigation strategies by identifying the parameters that most strongly influence privacy-risk escalation under different civilian UAS deployment contexts. Although the present analysis is intentionally lightweight and qualitative in nature, future work will extend the framework toward formal statistical sensitivity analysis and uncertainty propagation using empirical UAV operational datasets and probabilistic calibration techniques. Fig. 4 conceptualizes privacy risk as a propagation chain that begins with technical compromise and culminates in societal harm. The model highlights amplification factors such as inference capability and contextual density, which significantly influence final privacy impact scores.

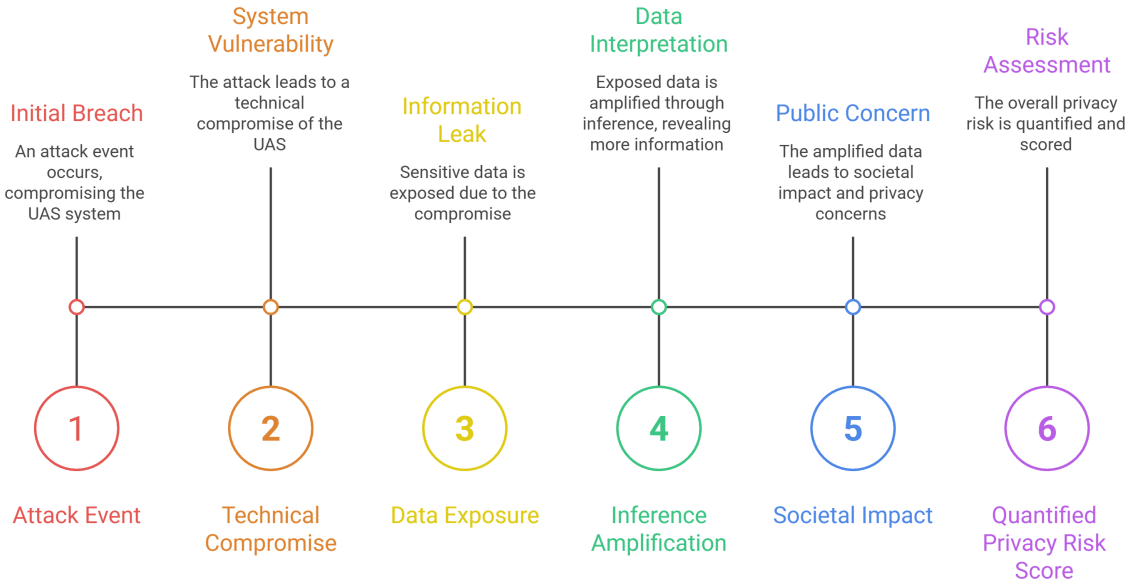

Figure 4: Privacy risk propagation model in civilian UAS.

Surveys that focus on engineering aspects underline the fact that the same technical countermeasure (e.g., encryption, anonymization) may affect these dimensions differently with implementation and resource utilization [12]. By including them as modular risk models, the UAS designers can investigate the trade-offs between the mission performance and system cost vs. privacy assurances.

The proposed framework supports full-process attack-path analysis by tracing the propagation of compromise events across sensing, communication, computation, backend analytics, and governance layers. For example, telemetry interception may initially expose communication confidentiality, subsequently enable behavioral inference, and ultimately escalate into societal-scale privacy violations through long-term data aggregation and cross-platform correlation. Similarly, GNSS spoofing combined with swarm coordination manipulation may trigger cascading operational and surveillance risks in collaborative UAV deployments. Based on the resulting privacy-risk scores, deployment scenarios can be categorized into low-, medium-, and high-risk operational profiles, enabling differentiated protection strategies such as adaptive encryption policies, mission-aware access control, swarm-isolation mechanisms, AI-assisted anomaly detection, and regulatory escalation procedures. This layered attack-path perspective enables more realistic evaluation of cumulative cyber–physical and privacy impacts in civilian UAS ecosystems.

6 Case-Based Societal Impact Analysis

6.1 Urban Surveillance and Smart City Monitoring

In the case of smart cities, UAVs assist in traffic monitoring, crowd management, environmental surveillance, and law enforcement [8,16]. There are security and privacy weaknesses of Internet of UAVs architectures, especially with intrusion detection, authentication, and data protection, which directly affect the trust of society and civil liberties [16]. Ntizikira et al. position smart city IoUAV implementations as the need to provide secure and privacy-sensitive IDS that can detect anomalies in real-time, noting that the broadcast wireless communications and the wide coverage of the aerial space beckon the threat of eavesdropping and location privacy attacks [16].

The unauthorized access to any of the following can:

1. Make it possible to track people or groups in real time.
2. Publicize policing patterns or vital infrastructure patrol routes.
3. Enable specific crime or repression, based on the perpetrator [8,16].

In regulatory reviews, it has been pointed out that, although there are general privacy laws, not many jurisdictions have specific limitations in UAV-related persistent aerial surveillance or automated analytics, creating gaps in addressing the risks posed by such technologies in society [5,6].

6.2 Critical Infrastructure and Airports

There is an upward trend of rogue or abused drones in airports and other important places, which demand effective counter-UAS (C-UAS) measures [8,11]. Drones near the airports may result in massive flight cancellations, safety risks, and general panic. Meanwhile, legitimate UAS are also introduced to monitor the perimeter of the airport and check the facilities, which accounts for defensive and offensive purposes in the same airspace [11,14].

In such cases, threat modeling should be considered:

- **High safety and availability criticality:** DoS, spoofing, or hijacking can translate into catastrophic outcomes.
- **High privacy stakes:** Surveillance of passengers, staff, and secure areas may expose sensitive behaviors and security procedures.
- **Complex stakeholder environment:** Multiple agencies and private actors share responsibility for C-UAS measures and data governance [8].

Surveys of C-UAS sensing technologies and STRIDE-based analyses for multi-UAV inspection systems at critical infrastructures demonstrate both the feasibility and the limits of current mitigation measures [14]. Resilience plans focus on layered identification, resilient processes, and contingency operations to minimize influences on society even with biased compromise [11].

6.3 Mega Sporting Events and Public Assemblies

UAVs are being deployed more in mega events like international sports events to monitor crowds, to supply logistics, and security chain management [15]. In their work, AL-Dosari et al. create and test a UAV-based security supply chain model of the mega events in Qatar and identify traceability, security, privacy, trust, acceptability, and preparedness as the essential factors that define the intention and practices of professional IT/security experts [15]. This work illustrates how:

- Societal trust in UAV-enabled security solutions depends on credible privacy protection and clear communication of safeguards.

- Security and privacy are strongly correlated with traceability and preparedness, suggesting that robust audit trails and contingency planning can mitigate public concerns [15].

Coupling these socio-technical insights with technical threat models enables a more realistic assessment of societal risks in high-density public gatherings and supports the design of privacy-respecting aerial security architectures. The proposed framework was analytically validated using representative civilian UAS deployment scenarios, including smart-city monitoring, critical infrastructure surveillance, and mega-event security operations. For each scenario, realistic threat events such as telemetry interception, GNSS spoofing, cloud-storage misconfiguration, and unauthorized surveillance were evaluated using the proposed quantitative privacy-risk model. The validation process incorporated likelihood of compromise, exposure severity, contextual amplification, downstream misuse potential, and regulatory impact to derive comparative privacy-risk scores across heterogeneous operational contexts. Although the current study does not utilize proprietary operational UAV datasets due to privacy, security, and regulatory limitations, the scenario-driven evaluation demonstrates the framework's capability to systematically assess cyber–privacy risks and propagate technical compromise into societal-impact analysis. The framework is intentionally designed to support future integration with real-world UAV telemetry, operational logs, intrusion-detection datasets, and live deployment environments for experimental validation and adaptive risk assessment.

7 Engineering Mitigation Strategies

7.1 Secure by Design UAS Architectures

More recent surveys stress that the addition of piecemeal security capabilities is not a viable solution to UAS, and security by design principles should be integrated in all aspects of architecture definition through the deployment [4,6,11].

Key elements include:

- Cryptographically protected C2 and data links, with robust key management and mutual authentication tailored to resource-constrained UAVs [12].
- Hardware roots of trust and secure boot mechanisms to prevent firmware tampering and unauthorized modifications [11].
- Defense in depth at each architectural level, sensors, controllers, networks, and backends, with segmentation to limit blast radius [14].
- Integration of regulatory and privacy requirements into design artifacts, ensuring that default configurations implement data minimization, access control, and logging.

As depicted in Fig. 5, effective mitigation requires coordinated controls across hardware, communications, analytics, and governance layers. Isolated security mechanisms are insufficient without an integrated privacy-aware architectural design.

Emerging frameworks conceptualize UAS cybersecurity similarly to industrial control or urban air mobility systems, advocating life cycle security management and continuous threat assessment [19].

7.2 Federated Learning, Privacy-Preserving Analytics, and Intrusion Detection

The detection and mitigation of active threats depend on the IoUAVs and FANETs adapted to an IDS and anomaly detection mechanisms [12]. Ntizikira et al. introduce SP IoUAV, which is a secure and privacy-aware IDS based on federated learning, differential privacy, and secure multi-party computation to ensure data confidentiality and high detection rates on benchmark data [16]. Their approach: Stores raw data on the UAVs/edge nodes, but only cryptic model updates. Combines CNN and LSTM to detect anomaly occurrences in real-time. Uses multi-factor authentication and automated blacklisting to increase

the security of access to the IDS infrastructure [16]. Zhu et al. introduce UBFL, a blockchain-based federated learning protocol to UAV MEC networks that substitutes noise, adding different privacy with adaptive nonlinear gradient encryption, which offers excellent privacy protection with high accuracy, including data poisoning situations [18]. Both works highlight:

- The feasibility of combining federated learning with advanced cryptography to protect privacy and security in distributed UAV networks.
- The emerging trade-off between transparency (for audit/compliance) and confidentiality (for privacy), mediated through secure ledgers and privacy-preserving ML [16,18].

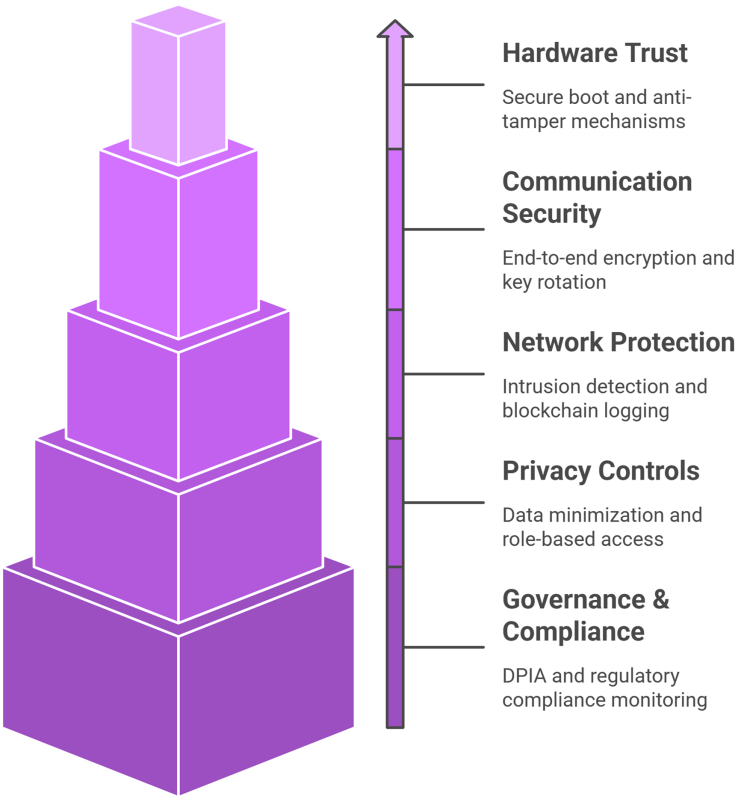

Figure 5: Defense-in-depth security and privacy mitigation stack for civilian UAS.

When differential privacy is used as the privacy-preserving mechanism, the formal guarantee can be stated as in Eq. (4).

$$\frac{\Pr[M(D_1) \in S]}{\Pr[M(D_2) \in S]} \leq e^{\epsilon} \tag{4}$$

where:

M = randomized mechanism (e.g., DP release mechanism, DP training/aggregation)

D_1, D_2 = two neighboring datasets (differ by one individual's data)

S = any set of possible outputs

ϵ = privacy parameter (smaller implies stronger privacy, generally more noise)

A common baseline for federated learning aggregation is weighted model averaging, shown in Eq. (5):

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^{(k)} \tag{5}$$

where:

w_{t+1} = global model parameters at round t

$w_{t+1}^{(k)}$ = client k's locally updated model parameters after local training

K = number of participating clients (UAVs/edge nodes) in round t

n_k = number of training samples used by client k

$n = \sum_{k=1}^{K} n_k$ = total samples across participating clients

To address the computational and communication limitations of civilian UAV platforms, the proposed framework supports a lightweight multi-layer defense architecture integrating federated learning, differential privacy, and blockchain-assisted trust management. Federated learning enables collaborative intrusion detection and anomaly analysis without centralized raw-data sharing, thereby reducing communication overhead and privacy exposure. Differential privacy mechanisms further protect sensitive operational data and model updates against inference and reconstruction attacks, while lightweight blockchain protocols provide decentralized identity management, immutable audit trails, and resilient trust coordination among distributed UAV nodes. The combined integration of these technologies enables privacy-preserving situational awareness, adaptive threat intelligence sharing, and scalable collaborative defense suitable for resource-constrained swarm-based UAS deployments.

7.3 Blockchain and Decentralized Trust

UAV communication systems that are assisted with blockchain have been suggested to improve the security properties, including authentication, authorization, integrity, and privacy in peer-to-peer UAV networks [10,17]. The potential benefits are listed in the surveys and include:

- Decentralized identity and access control management, reducing reliance on single points of failure.
- Immutable logging of mission data and security-relevant events, supporting forensic analysis and regulatory accountability [17,18].
- Tokenized or reputation-based mechanisms for managing multi-stakeholder UAS ecosystems [8,17].

However, resource constraints, latency requirements, and air-to-ground link variability constrain the direct adoption of heavyweight blockchain protocols, motivating lightweight and hybrid approaches tailored to UAS [10,17].

7.4 Policy, Governance, and Societal Safeguards

Policy and governance mechanisms should enhance the technical measures. In the comparative regulatory studies, it is observed that safety regulations are already more advanced than privacy regulations, and some areas of harmonization and improvement can be made:

- UAV-specific privacy policies which deal with continuous air surveillance, data storage, and machine-generated analytics.
- Privacy by design and security risk assessment requirements in the UAS certifications, like data protection impact assessments (DPIAs).

- Social visibility and engagement in the implementation of UAVs in sensitive situations (e.g., policing, protests, mega events) to preserve legality and trust [8].

The examples of socio-technical research conducted at mega events and critical infrastructure projects support the idea that effective and socially acceptable UAV-based security solutions require organizational readiness, traceability, and de facto allocation of responsibilities [15]. Practical deployment of civilian UAS security architectures requires scenario-aware implementation strategies aligned with operational criticality, airspace density, and regulatory obligations. Smart-city monitoring deployments should prioritize privacy-preserving analytics, continuous audit logging, and adaptive citizen-data minimization policies. Critical infrastructure and airport environments require stronger resilience mechanisms including multi-factor UAV authentication, redundant navigation verification, anti-jamming coordination, and fail-safe supervisory control. Large-scale collaborative swarm operations additionally require distributed trust coordination, inter-UAV anomaly sharing, lightweight consensus validation, and dynamic mission-isolation capabilities to prevent cascading compromise propagation. From a governance perspective, deployment frameworks should incorporate privacy-by-design principles, continuous compliance monitoring, retention-limitation policies, explainable AI auditing, and harmonization with regional UTM and data-protection regulations to support socially acceptable and legally compliant civilian UAS integration.

8 Research Challenges and Future Directions

8.1 Automated, Regulatory Aligned Threat Modeling

UAVThreatBench proves the capability of LLMs to be able to detect a high percentage of expert-reported threats in a regulatory-congruent industrial UAV setting, but is still systematically vulnerable, especially to availability threats and backend vulnerabilities [17]. The following points should be investigated:

- Hybrid human–AI workflows for UAS threat modeling, where automated tools provide coverage and suggestions while experts refine assessments.
- Datasets and benchmarks that capture diverse civilian UAS contexts, regulatory clauses, and socio-technical impacts [18,19].

8.2 Privacy Metrics, Differential Protections, and Human Factors

The quantitative privacy risk modeling is not well developed in UAV research, particularly in terms of:

- Measurable privacy guarantees (e.g., differential privacy parameters) for aerial data and analytics [10].
- Human in the loop privacy controls, including real-time consent, opt-out zones, and interface designs that inform affected communities of UAV operations [8].
- Cross-jurisdictional frameworks that reconcile differing privacy expectations and legal regimes in global UAS services.

8.3 Resilience Engineering for Large-Scale UAS Ecosystems

The resilience-related views promote the existence of systems capable of predicting, enduring, restoring, and adjusting to cyber and privacy attacks [4,11]. In the case of civilian UAS, this entails:

- Hardened fail-safe and graceful degradation characteristics on partial compromise.
- Risk-aware mission planning, which is dynamic and considers the threat intelligence and privacy constraints.
- Cooperation among C-UAS metrics, security telemetry, and impact monitoring of the society to offer situational awareness [14].

To support reproducibility, the proposed framework explicitly defines the layered UAS architecture, STRIDE-based threat mappings, privacy-risk equations, scoring variables, and contextual evaluation criteria used throughout the analysis. The methodology is intentionally designed to be modular and adaptable, enabling other researchers to replicate the assessment process across different civilian UAS deployment scenarios and operational conditions. In addition, the scenario-based validation workflow, attack categories, and privacy-risk scoring procedures can be reproduced using publicly available UAV threat datasets and cybersecurity benchmarks. Future work will focus on developing open-source software implementations, standardized benchmark datasets, and automated evaluation pipelines to facilitate reproducible large-scale experimental validation and comparative assessment against AI-driven UAV security frameworks.

9 Conclusion

Civilian UAS have evolved from remote aerial platforms into highly networked cyber-physical systems embedded in the infrastructure of smart cities, critical infrastructure, and mass-scale government operations. Such architectural integration has not only increased the technological attack surface but also heightened exposure to privacy and cybersecurity violations, making them a matter of societal concern. The traditional analyses are too narrow, as they only concentrate on navigation integrity or the availability of communication to show the wider impacts of civilian deployments. This manuscript proposed a systematic guide combining the layered system decomposition, multidimensional threat taxonomies, and the modeling based on STRIDE and a quantitative privacy risk metric that is specific to UAS ecosystems. The proposed model allows considering the implications of technical compromise on societal harm in a more organized way by connecting the risk of attack, the sensitivity of data, the amplification in the context, and regulatory disclosure. Urban surveillance case studies, airport setting, and mega-event case studies indicated the significance of threat modeling and governance alignment based on the context. Defense-in-depth architecture, security by design engineering, privacy-sensitive analytics, distributed trust mechanisms, and regulations across the system lifecycle are mitigation requirements. With the increased rate of civilian UAS acceptance going forward, resiliency will rely on both technical hardening and harmonized standards of threat modelling, operational transparency, and adaptive privacy protection policies that are built into system design at its earliest inception.

Acknowledgement: This work has not received any kind of support from any organization.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: Conceptualization, Ahmed Murtaza and Abdullah Memon; methodology, Ahmed Murtaza and Ghulam E Mustafa Abro; software, Ahmed Murtaza; validation, Ahmed Murtaza, Abdullah Memon and Sana Hafeez; formal analysis, Ahmed Murtaza; investigation, Ahmed Murtaza; resources, Ahmed Murtaza, Sana Hafeez and Ghulam E Mustafa Abro; data curation, Ahmed Murtaza; writing—original draft preparation, Ahmed Murtaza; writing—review and editing, Ahmed Murtaza and Muzammil Ali; visualization, Ahmed Murtaza, Muzammil and Sana Hafeez; supervision, Sana Hafeez and Ghulam E Mustafa Abro; project administration, Muzammil and Abdullah Memon; funding acquisition, Ghulam E Mustafa Abro and Sana Hafeez. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are available from the Corresponding Author, upon reasonable request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Yaacoub JP, Noura H, Salman O, Chehab A. Security analysis of drones systems: attacks, limitations, and recommendations. Internet Things. 2020;11(2):100218. doi:10.1016/j.iot.2020.100218.
2. Mohsan SAH, Othman NQH, Li Y, Alsharif MH, Khan MA. Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends. Intell Serv Robot. 2023;16(1):109–37. doi:10.1007/s11370-022-00452-4.
3. Bai N, Hu X, Wang S. A survey on unmanned aerial systems cybersecurity. J Syst Archit. 2024;156(5):103282. doi:10.1016/j.sysarc.2024.103282.
4. Jacobsen RH, Marandi A. Security threats analysis of the unmanned aerial vehicle system. In: Proceedings of the 2021 IEEE Military Communications Conference (MILCOM); 2021 Nov 29–Dec 2; San Diego, CA, USA. p. 316–22. doi:10.1109/MILCOM52596.2021.9652900.
5. Lee D, Hess DJ, Heldeweg MA. Safety and privacy regulations for unmanned aerial vehicles: a multiple comparative analysis. Technol Soc. 2022;71(1):102079. doi:10.1016/j.techsoc.2022.102079.
6. Mekdad Y, Aris A, Babun L, El Fergougui A, Conti M, Lazzeretti R, et al. A survey on security and privacy issues of UAVs. Comput Netw. 2023;224(4):109626. doi:10.1016/j.comnet.2023.109626.
7. Almuthaybiri M, Murphy D. Cybersecurity risk in unmanned aircraft systems (UASs): strategic cybersecurity threats of unmanned aerial systems. ICCWS. 2025;20(1):520–9. doi:10.34190/iccws.20.1.3356.
8. Hafeez S, Khan AR, Al-Quraan MM, Mohjazi L, Zoha A, Ali Imran M, et al. Blockchain-assisted UAV communication systems: a comprehensive survey. IEEE Open J Veh Technol. 2023;4(1):558–80. doi:10.1109/OJVT.2023.3295208.
9. Zhi Y, Fu Z, Sun X, Yu J. Security and privacy issues of UAV: a survey. Mobile Netw Appl. 2020;25(1):95–101. doi:10.1007/s11036-018-1193-x.
10. Mohsan SAH, Khan MA, Noor F, Ullah I, Alsharif MH. Towards the unmanned aerial vehicles (UAVs): a comprehensive review. Drones. 2022;6(6):147. doi:10.3390/drones6060147.
11. Xi H, Ru L, Tian J, Lu B, Hu S, Wang W, et al. Enhanced cybersecurity framework for unmanned aerial systems: a comprehensive STRIDE-model analysis and emerging defense strategies. IET Inf Secur. 2025;2025(1):9637334. doi:10.1049/ise2.9637334.
12. Pandey GK, Gurjar DS, Nguyen HH, Yadav S. Security threats and mitigation techniques in UAV communications: a comprehensive survey. IEEE Access. 2022;10:112858–97. doi:10.1109/ACCESS.2022.3215975.
13. Morshedi R, Matinkhah SM. Cybersecurity challenges and solutions in unmanned aerial vehicles (UAVs). J Field Robot. 2026;43(1):314–29. doi:10.1002/rob.70040.
14. Cordill B, Fang D, Xu S. A comprehensive survey of security and privacy in UAV systems. IEEE Access. 2025;13(3):117843–66. doi:10.1109/ACCESS.2025.3583985.
15. AL-Dosari K, Deif AM, Kucukvar M, Onat N, Fetais N. Security supply chain using UAVs: validation and development of a UAV-based model for Qatar's mega sporting events. Drones. 2023;7(9):555. doi:10.3390/drones7090555.
16. Ntizikira E, Lei W, Alblehai F, Saleem K, Ali Lodhi M. Secure and privacy-preserving intrusion detection and prevention in the Internet of unmanned aerial vehicles. Sensors. 2023;23(19):8077. doi:10.3390/s23198077.
17. Iyenghar P. UAVThreatBench: a UAV cybersecurity risk assessment dataset and empirical benchmarking of LLMs for threat identification. Drones. 2025;9(9):657. doi:10.3390/drones9090657.
18. Zhu C, Zhu X, Qin T. An efficient privacy protection mechanism for blockchain-based federated learning system in UAV-MEC networks. Sensors. 2024;24(5):1364. doi:10.3390/s24051364.
19. Dehbi F, Zraib M, Chebak A. PASTAD: a context-aware threat modeling methodology for unmanned aerial systems. Cyber Secur Appl. 2025;3(294):100111. doi:10.1016/j.csa.2025.100111.
20. National Institute of Standards and Technology (NIST). Guide for conducting risk assessments. In: NIST special publication 800-30 revision 1. Gaithersburg, MD, USA: National Institute of Standards and Technology; 2012. doi:10.6028/NIST.SP.800-30r1.