AI-driven drones and airport cybersecurity: Legal challenges and international dimensions

Kateryna Vodolaskova[1,*,†], Yuliia Polishchuk[2,†], Svitlana Holovko[2,†], Olena Makeieva[2,†] and Viktoriya Cherevatiuk[2,†]

[1]University of Cologne, Albertus-Magnus-Platz, Cologne, 50923, Germany
[2]State University "Kyiv Aviation Institute", Liubomyra Huzara Ave., 1, Kyiv, 03058, Ukraine

Abstract

The rise of AI in unmanned aircraft systems (UAS) and airport operations is reshaping aviation law and cybersecurity. As AI-driven systems—like U-space, automated surveillance, and remote ID—expand, airports face growing cyber risks with unclear legal accountability. This paper explores international legal challenges tied to AI-enabled drones, digital sovereignty, and cyberattack attribution. Case studies from Gatwick, Frankfurt, Warsaw, and Madrid highlight regulatory gaps in counter-UAS measures and data protection. Ukraine's wartime use of dual-use drones shows how emerging threats demand national and supranational legal responses. The study calls for anticipatory legal models that treat AI as a legal subject, needing clear rules and global oversight to secure digital aviation systems.

Keywords

Unmanned Aircraft Systems (UAS), Artificial Intelligence (AI), airport cybersecurity, international aviation law, digital sovereignty, counter-UAS technologies, cyber diplomacy, drone disruption

1. Introduction

The exponential growth of artificial intelligence (AI) technologies in civil aviation, particularly in unmanned aircraft systems (UAS) and smart airport infrastructure, has introduced not only operational advantages but also unprecedented cyber-legal vulnerabilities. From AI-assisted navigation and surveillance to autonomous drone deployment and digital U-space management, the aviation sector is undergoing a structural transformation that challenges both domestic and international legal frameworks.

Airports have become increasingly dependent on integrated digital systems—remote identification tools, automated communication channels, and AI-based air traffic interfaces—that operate within a broader, often inadequately regulated, cyber-physical environment. This makes them critical targets for disruption, whether by hostile actors exploiting AI vulnerabilities in drones or through cascading failures triggered by algorithmic errors. In 2018, unauthorized drone activity at Gatwick Airport resulted in the cancellation of over 1,000 flights and brought global attention to the regulatory and institutional fragility of airport UAS responses [1, 2]. Subsequent incidents in Frankfurt, Madrid, and Warsaw have confirmed that this is not an isolated anomaly but part of a systemic vulnerability.

Despite the publication of harmonized drone regulations within the European Union—most notably Regulation (EU) 2019/947 and the U-space framework established by Regulation (EU) 2021/664—these legal instruments remain largely focused on technical interoperability, safety, and innovation promotion. Their cybersecurity and liability components, especially in cases involving AI-powered decision-making, remain underdeveloped or ambiguously framed.

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine

*Corresponding author.
†These authors contributed equally.
khusanova@gmail.com (K. Vodolaskova); polishchuk.yu.ya@gmail.com (Y. Polishchuk); svitlana.holovko@npp.kai.edu.ua (S. Holovko); maklena72@ukr.net (O. Makeieva); vitacherev@ukr.net (V. Cherevatiuk)
0000-0002-6133-822X (K. Vodolaskova); 0000-0002-0686-2328 (Y. Polishchuk); 0000-0003-0795-7166 (S. Holovko); 0000-0001-6101-2951 (O. Makeieva); 0000-0002-4077-206X (V. Cherevatiuk)

Table 1
Regulation Gaps and Focus

Regulation	Focus	Gaps Identified
EU 2019/947	Risk-based drone ops	No AI liability principles
EU 2021/664	U-space integration	No airport-specific mandates
Chicago Convention (Annexes)	International norms	Cyber-autonomy not covered

Moreover, international legal instruments such as the Chicago Convention and related ICAO guidelines offer limited coverage of cyber-autonomous threats posed by UAS. As drone autonomy increases, and AI becomes embedded in every phase of airport operations, these limitations become more than a legal inconvenience—they represent a structural blind spot in global aviation governance.

The purpose of this paper is to explore these legal gaps through the prism of AI-driven UAS and cyber-vulnerability in airport contexts. It proposes a framework for legal analysis grounded in international law, cyber diplomacy, and anticipatory regulation, aiming to inform both doctrinal scholarship and real-world policy-making.

2. Related work and legal background

The intersection of AI, drone technology, and airport cybersecurity remains underrepresented in mainstream legal scholarship, despite a growing body of technical literature addressing operational safety and automation [3, 4]. This section outlines relevant technological, regulatory, and legal developments, dividing the background into three analytical categories: (1) Legal evolution of UAS regulation; (2) AI adoption in aviation systems; and (3) Airport cybersecurity frameworks [5, 6].

2.1. Legal evolution of UAS regulation

Early drone legislation focused predominantly on airspace safety, privacy, and registration [7]. The European Union's landmark Regulation (EU) 2019/947 marked a shift toward harmonization, introducing a risk-based approach and operator categories [8]. The U-space package, especially Regulation (EU) 2021/664, further formalized the integration of drones into civil airspace with service-based architectures [9]. However, these frameworks give limited attention to AI-specific risks and often exclude airport-specific protocols [10]. Table 1 presents regulation gaps and focus.

2.2. AI integration in aviation systems

The aviation sector increasingly integrates AI in flight control, predictive maintenance, and surveillance [11, 12]. UAS traffic management (UTM) systems under development by SESAR and NASA feature autonomous decision-making capabilities, which raise legal uncertainties concerning explainability, predictability, and control [13, 14].

AI-powered drones, in particular, shift the traditional liability model—where a human pilot or operator was clearly accountable—to a more complex ecosystem involving AI agents, software developers, and airport managers [15, 16]. Legal doctrines remain ill-equipped to handle such distributed responsibility [17].

2.3. Cybersecurity and smart airports

Airports are evolving into complex digital ecosystems. Smart gates, biometric systems, and AI-based surveillance introduce new attack surfaces [18]. A 2023 EASA report warned about increasing cyber intrusions into airport control systems, yet legal harmonization is minimal across jurisdictions [19].

The Tallinn Manual 2.0 offers guidance on state behavior in cyberspace but lacks binding authority and rarely addresses infrastructure autonomy [20]. Furthermore, counter-UAS protocols often involve

Table 2
Legal and Technical Gaps in AI-Enabled Airport Environments

Dimension	Challenge	Legal Gap
AI Autonomy	Decision-making	Absence of standards for liability attribution
Cyber Threats	System hacking	Fragmented cross-border enforcement
Drone-Airport Ops	UAS services at airports	No unified licensing or operational law

security services without sufficient coordination with civil aviation legal authorities, which creates governance overlaps [21]. The corresponding information is shown in Table 2.

This background (Table 2) highlights the urgent need for interdisciplinary frameworks that link legal, technical, and policy elements of AI-powered drone integration in critical infrastructure like airports [22]. Subsequent sections will propose models for proactive legal governance and international cooperation [23].

3. Legal blind spots: Cybersecurity, liability, and international law

The increasing integration of AI-driven UAS into airport infrastructure has revealed significant legal vulnerabilities—particularly in relation to cybersecurity, responsibility attribution, and the applicability of international legal frameworks. While much of international aviation law is historically grounded in physical safety and sovereignty over airspace, the rise of autonomous and semi-autonomous aerial operations presents complex challenges that extend into the cyber domain. This section discusses the most salient blind spots in the current legal landscape, focusing on three critical areas: the lack of standardized cybersecurity norms, the ambiguity surrounding liability for AI-enabled drone operations, and the limited applicability of existing international legal instruments to emerging threats.

3.1. Lack of international cybersecurity standards for AI-driven UAS and airports

Currently, no binding international framework specifically addresses the cybersecurity vulnerabilities of UAS, particularly in the context of airport operations. Despite the technological advancement of unmanned systems and AI modules, international regulatory efforts remain fragmented. The Tallinn Manual 2.0 on the international law applicable to cyber operations provides interpretive guidance on state behavior in cyberspace [20]. However, it does not address the complexities arising from autonomous aviation systems or AI-enabled infrastructure. Similarly, while the Chicago Convention and its Annexes outline basic standards for aviation safety and security, they are largely silent on the cyber-autonomy interface [24].

The absence of targeted regulations leaves states and airports to interpret their obligations individually, leading to inconsistencies in implementation and enforcement. This fragmentation is particularly problematic given the inherently transboundary nature of cyber threats involving UAS, which often traverse multiple jurisdictions and implicate both civil and national security regimes [25].

Comparative Table 3 underscores the systemic lack of coordination and the legal void in which AI-enabled airport environments currently operate.

3.2. Attribution of liability in AI-enabled drone operations

One of the most challenging legal aspects of AI-powered UAS concerns the attribution of liability in the event of system malfunction, cyber intrusion, or damage caused by autonomous decision-making. Traditional aviation law is built upon the notion of a clearly identifiable operator or pilot, typically held accountable under both civil and criminal frameworks [26]. However, the introduction of autonomous systems, operating with varying degrees of human oversight, fundamentally alters this liability paradigm.

Table 3
Comparative Overview of International Norms on Cybersecurity and UAS

Legal Instrument	Scope & Relevance	Limitation
ICAO Chicago Convention (1944)	Civil aviation safety and sovereignty	No specific norms on cyber Nautonomy or AI-based decisions
Tallinn Manual 2.0 (2017)	Cyber operations under international law	Not legally binding; infrastructure-specific issues omitted
EU Cybersecurity Act (2019)	ICT and AI systems regulation in EU	Fragmented application to airport systems/UAS
UN GGE Reports on Cybersecurity	State responsibility in cyberspace	General in scope; not aviation-specific

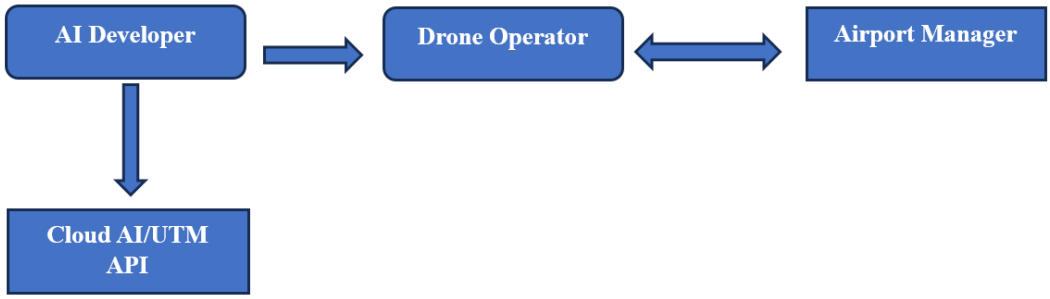

Figure 1: Liability landscape in AI-enabled drone ecosystems.

Table 4
Scenarios of Distributed Liability

Scenario	Legal Actor(s) Involved	Ambiguity in Law
AI misclassifies an object, leading to false alert	Developer, UAS Operator, Airport	No clear standard of explainability
UAS hacked en route to airport	UTM Provider, UAS Manufacturer	No uniform cybersecurity duty of care
Drone used for espionage near airport	State of registry, Operator	Overlap between civil and national security

Responsibility is now distributed across a complex ecosystem of actors, including AI developers, UAS manufacturers, operators, airport authorities, and third-party service providers such as cloud-based navigation and communication platforms. In the event of a cyber incident or operational failure, determining causality and legal fault becomes difficult, particularly in cases where the AI component functions as a "black box" with limited explainability [27].

Table 4 demonstrate the limitations of existing legal doctrines when applied to autonomous systems whose actions are not always traceable to a single point of human control [5].

3.3. International legal instruments: Do they apply?

While several international instruments address aspects of cyber behavior or aviation regulation, none are currently equipped to manage the emerging challenges at the intersection of AI, cybersecurity, and unmanned flight. The Chicago Convention, particularly Annex 17 on Security, outlines states' obligations to prevent unlawful interference with civil aviation. However, it does not explicitly reference cyber intrusions or AI-enabled threats. The Tallinn Manual, despite its interpretive value, remains non-binding and was never designed for application to civil aviation infrastructure. Meanwhile, the European Union's regulatory efforts, including the Cybersecurity Act and the NIS2 Directive, apply

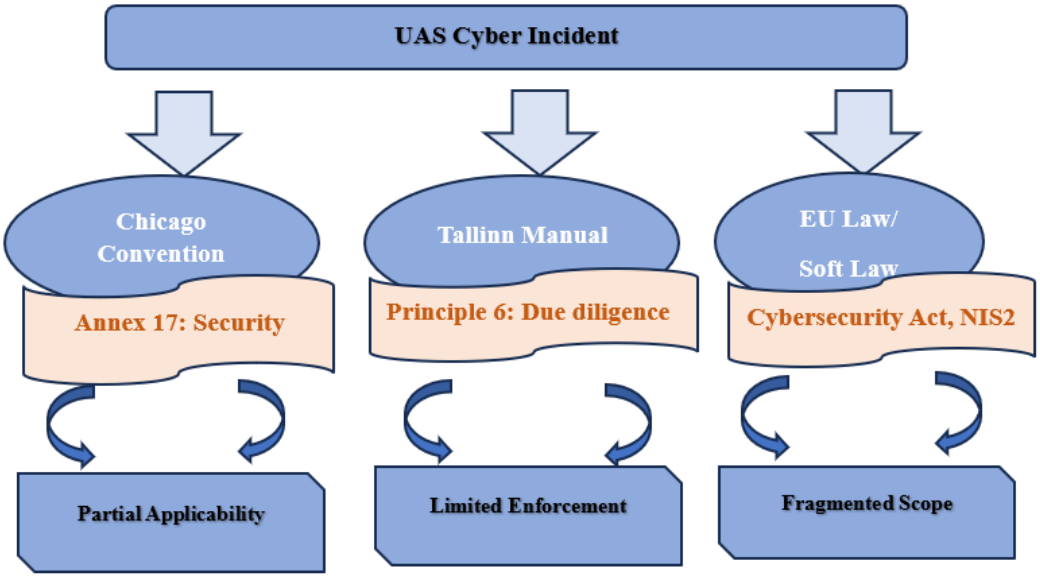

Figure 2: Legal applicability of international frameworks to UAS cyber incidents.

Table 5
Summary of Gaps

Domain	Existing Tools	Gap Identified
Cybersecurity	Tallinn Manual, ICAO Annex 17	Not AI/autonomy-specific
Liability	Domestic tort law, EU Product Liability	No shared liability model for AI/airport
International Law	Chicago Convention, UN Charter	Lack of norms for dual-use cyber threats

primarily within the EU and do not ensure interoperability with third-country regimes [28].

Figure 2 reveals the partial and uneven legal coverage currently afforded to AI-related cyber threats in aviation, particularly in cross-border contexts where jurisdictional overlaps are inevitable.

The legal regulation of AI-driven drones in airport environments is characterized by fragmentation, conceptual ambiguity, and a notable lack of anticipatory governance (Table 5). Existing frameworks are largely reactive, offering post-incident remedies rather than preventive or adaptive standards. In particular, the absence of international norms governing cybersecurity in AI-enabled aviation systems and the legal vacuum regarding liability attribution present serious risks to global aviation safety and legal coherence.

In the following sections, we propose normative and institutional responses to these challenges, focusing on the development of harmonized legal standards, AI-specific liability regimes, and multilateral cooperation mechanisms that align cyber diplomacy with aviation security.

4. Case studies: Drone incidents and legal implications

The evolution of UAS, increasingly enhanced with AI, has challenged traditional aviation security frameworks. While international law has largely focused on kinetic threats, the emergence of AI-enabled drones—capable of autonomous operations, real-time data processing, and adaptive behavior—creates new legal and operational risks for both civil and hybrid (dual-use) environments. This section analyses a set of illustrative case studies, including Ukraine's military-civil experience and incidents at major European airports (Gatwick, Frankfurt, Warsaw, and Madrid), to reveal key vulnerabilities and normative gaps.

Table 6
Legal Implications of AI-Driven Dual-Use Drones in Ukraine

Legal Issue	Description
Attribution	Civilian users and military actors often indistinguishable
State Responsibility	Volunteer units and informal command chains challenge legal accountability
AI Autonomy	Pre-programmed systems bypass human oversight; complicates intent assessment
Airspace Control	Conflict zones lack enforceable civil-military separation
Post-War Integration	Civil use of war-tested AI drones likely; lacks safety and legal vetting

4.1. Ukraine: A dual-use drone laboratory in wartime conditions

Ukraine presents a unique and urgent case of how AI-driven drones are deployed in both military and civilian contexts. Since 2022, the country has experienced an unprecedented surge in the adaptation of commercial drones—such as DJI Mavic, Autel EVO, and FPV quadcopters—for defense purposes. Many of these systems now incorporate basic AI modules, including object recognition, adaptive flight routing, and obstacle avoidance algorithms. These features increase operational efficiency but simultaneously obscure attribution and legal classification [29].

The decentralized and volunteer-based use of AI drones blurs the line between state and non-state actors, complicating the application of International Humanitarian Law (IHL) and the Chicago Convention's civil-military airspace separation. Furthermore, drones originally developed for agricultural mapping or logistics are now repurposed for reconnaissance and strike operations—raising critical questions about export controls, liability, and post-conflict reintegration of technology into civil aviation [24].

The full-scale war on the territory of Ukraine has turned the country into a testing ground for large-scale use of UAS, both in military and civil domains. Airports and critical aviation infrastructure became direct targets of kinetic and cyberattacks involving UAS, revealing systemic legal and institutional vulnerabilities. At the same time, this experience has catalyzed legal innovation, particularly in the domains of counter-UAS regulation, liability, and cybersecurity coordination (Table 6).

In 2022–2024, Ukraine adopted a number of legal acts and institutional reforms aimed at enhancing the resilience of its airspace management and critical infrastructure. The Law of Ukraine "On the National Security of Ukraine" and the Law "On the Basics of Ensuring Cybersecurity of Ukraine" serve as foundational texts outlining a hybrid approach to cyber and physical threats, including those involving AI-driven drones [27]. Additionally, Ukraine's Resolution of the Cabinet of Ministers No. 954 (2017)—amended after 2022—provides a basic regulatory structure for the operation of unmanned aerial vehicles in civilian contexts, though the wartime experience has shown its limitations [30].

Furthermore, Ukraine's Strategy for the Development of the Defense-Industrial Complex (2023–2030) directly references UAS and autonomous technologies as strategic assets, prompting the Ministry of Digital Transformation and the Armed Forces to cooperate on cyber protection protocols for dual-use systems [30]. However, the legal integration between civilian aviation regulators (such as the State Aviation Service) and defense structures remains underdeveloped, particularly in terms of jurisdiction, liability distribution, and international legal harmonization.

Cyberattacks on airports in Kyiv, Lviv, and Odesa during 2022–2023 included attempted spoofing of navigation systems and denial-of-service (DoS) attacks on communication networks, frequently linked to hostile drone activity. While international law offers only fragmented guidance on such hybrid threats, Ukraine's efforts to collect and document them—often in cooperation with partners such as the EU and NATO—have become part of a broader legal strategy aimed at evidencing violations of both aviation law and humanitarian law [31].

However, due to the martial law and ongoing threats of cyberattacks on infrastructure, including airports, Ukraine faces multiple challenges in ensuring cybersecurity and legal liability in cases of incidents caused by autonomous systems. The lack of clear standards and insufficient interagency coordination results in legal gaps that may be exploited during military conflicts and cyberattacks.

Table 7
Legal and Operational Features of the Gatwick Incident

Feature	Details
Duration	$\tilde{3}$3 hours of full or partial shutdown
Passengers Affected	$\tilde{1}$40,000 travelers
Legal Gaps Exposed	Attribution, drone detection, privacy in counter-UAS deployment
Policy Response	Expansion of exclusion zones; revised operator regulations
AI Indicators	None officially confirmed; pre-programmed behavior suspected by observers

In response, Ukrainian legislators and regulators are actively working to harmonize national regulations with international standards set by ICAO, the EU, and the UN, as well as developing specialized legal mechanisms for liability allocation in the field of AI and UAS, particularly regarding airports and transport security [31].

The Ukrainian experience with UAS deployment in a wartime context offers invaluable insights for the global legal community. It highlights the urgent need to develop resilient and adaptive regulatory frameworks capable of addressing both conventional and hybrid threats involving autonomous aerial technologies. Lessons learned from Ukraine's regulatory responses and operational challenges can inform international best practices, contributing to more robust legal standards and cybersecurity measures worldwide. Thus, Ukraine's practical experience plays a crucial role in shaping future legal trends in the governance of AI-enabled drones and airport security.

4.2. Gatwick airport (UK, 2018): A regulatory shock

In December 2018, London Gatwick Airport experienced the largest recorded drone-related disruption in civil aviation. Over a span of 33 hours, recurring drone sightings near the runway led to the cancellation of more than 1,000 flights, affecting approximately 140,000 passengers. Despite extensive deployment of police and military counter-UAS resources, no device or operator was officially identified [32].

The incident exposed the legal ambiguity surrounding the use of counter-drone technologies, such as jamming or interception, especially within densely populated airport environments. It also revealed significant gaps in national legislation, including unclear definitions of protected airspace and the absence of rapid attribution mechanisms. In response, the UK government revised its Air Navigation Order, expanding drone exclusion zones and enhancing operator licensing requirements (Table 7) [33].

4.3. Frankfurt, Warsaw, Madrid (2022–2023): The rise of AI-enhanced drones

More recent incidents in Germany, Poland, and Spain reveal a growing sophistication in rogue drone operations. These events, though shorter in duration than Gatwick, demonstrated potential hallmarks of AI-enhanced autonomy: erratic or randomized movement patterns, resistance to spoofing, and apparent pre-programming. Such patterns suggest the use of onboard algorithms to evade detection and maintain persistent presence in sensitive airspace [34].

At Frankfurt Airport, a drone sighting in March 2022 prompted a 30-minute suspension of departures. Authorities noted radar interference, possibly related to electronic countermeasures or spoofing-resistant systems.

In Warsaw (2023), a UAS entered a geo-fenced restricted area, causing several flights to reroute. Analysts noted behavior consistent with real-time adaptive routing, likely enabled by AI-based environmental mapping.

Madrid-Barajas Airport reported two unauthorized drones in June 2023. One device was able to maintain flight near terminal perimeters while evading conventional tracking systems, raising concerns about onboard decision-making and spoofing immunity [35].

The obtained information is shown in Table 8.

Table 8
Comparative Analysis of AI-Linked Airport Intrusions

Airport	Year	Incident Summary	Possible AI Indicators	Legal Follow-up
Frankfurt	2022	30-min disruption; radar anomalies detected	Signal resistance; suspected jamming	DFS internal review; no public prosecutions
Warsaw Chopin	2023	UAS in restricted airspace; several flight reroutes	Adaptive routing; non-linear trajectories	Investigation by Polish CAA
Madrid-Barajas	2023	Drones near terminal perimeter; tracking failure	Spoofing resistance; pre-programmed navigation	ENAIRE report issued; incident unresolved

4.4. Observations: Normative voids and operational risk

Across both war and peace contexts, a shared challenge is the lack of standardized legal responses to AI-enabled UAS threats. In Ukraine, the fusion of AI with dual-use drones operates in a legal grey zone, often outside conventional IHL frameworks. In civil settings like Gatwick, Frankfurt, or Madrid, attribution and technological sophistication outpace current aviation law. The common thread is the absence of international norms for defining and regulating autonomous or semi-autonomous drones.

There is also a notable lack of legal clarity regarding state obligations, especially when AI acts as an intermediate agent between the operator and the outcome. Moreover, AI-powered drones strain existing air navigation and cyber protection regimes, which remain largely reactive and nationally fragmented.

These insights point to the urgent need for harmonized international standards, technical-legal coordination, and anticipatory governance frameworks.

5. Recommendations: Toward a legal framework for AI-driven airport cybersecurity

The increasing integration of AI within UAS and airport infrastructure necessitates a comprehensive and forward-looking legal framework that addresses the complex challenges posed by these technologies. Current regulatory and legal mechanisms reveal significant gaps that hinder effective governance, particularly in the realms of cybersecurity, liability, and international coordination. This section proposes foundational recommendations aimed at establishing a robust legal architecture capable of managing the risks and opportunities presented by AI-driven airport cybersecurity.

5.1. The need for new legal definitions and terminology

A primary obstacle in regulating AI-enabled aviation systems is the absence of universally accepted definitions that precisely capture the technical and legal nuances of AI autonomy, decision-making capabilities, and intentionality. Concepts such as “autonomy,” “algorithmic intent,” and “machine learning liability” remain largely undefined within existing aviation and cybersecurity law. Clear and harmonized terminological frameworks are critical for delineating responsibilities, enabling consistent application of liability standards, and facilitating international legal cooperation [5, 11].

Developing these definitions should be a priority for standard-setting bodies such as the International Civil Aviation Organization (ICAO), the European Union Aviation Safety Agency (EASA), and international cybersecurity institutions. These definitions must be grounded in technical realities yet sufficiently flexible to accommodate rapid technological evolution [9].

5.2. Enhancing international diplomatic and regulatory cooperation

The inherently transnational nature of airspace and cyber-infrastructure requires enhanced international cooperation to address the cybersecurity risks posed by AI-driven UAS operations. Existing international

instruments, including the Chicago Convention and the Tallinn Manual on cyber operations, provide important foundations but lack specific provisions addressing AI-enabled drones and their unique threat profiles [24].

Multilateral diplomatic efforts should focus on establishing binding international agreements or protocols that define state responsibilities for preventing and responding to cyberattacks involving autonomous systems. Additionally, coordination mechanisms between civil aviation authorities, cybersecurity agencies, and defense sectors should be institutionalized to streamline incident response, information sharing, and counter-UAS measures [9].

5.3. Emphasizing the principle of preventive regulation and intersectoral responsibility

Given the rapid pace of AI innovation, the legal framework must adopt a principle of preventive regulation—anticipating and mitigating risks before they manifest in catastrophic incidents. This approach requires continuous monitoring of technological developments and dynamic updating of regulatory standards to reflect emerging threats [35].

Moreover, responsibility for AI-driven cybersecurity cannot rest solely with one stakeholder. Instead, it must be distributed across states, operators, AI developers, manufacturers, and airport authorities. Legal mechanisms should incentivize cooperation and accountability among all parties, including through clearly defined liability regimes and mandatory cybersecurity certifications for AI systems used in critical aviation infrastructure [9].

5.4. Institutionalizing legal and technical standards for AI safety and cybersecurity

To ensure resilience, international and national regulators should develop comprehensive standards covering AI system design, data protection, operational transparency, and cyber threat detection within airport environments. These standards must address vulnerabilities specific to AI algorithms, such as adversarial attacks, data poisoning, and automated decision errors, which can compromise flight safety and airport security [5].

Certification processes should incorporate rigorous testing and validation of AI modules used in UAS and airport systems, accompanied by continuous oversight to adapt to newly discovered threats. Collaboration with industry experts and academia will be essential for creating standards that are both practically feasible and legally enforceable.

6. Conclusions

The integration of AI in UAS and airport infrastructure fundamentally transforms the legal and cybersecurity landscape of civil aviation. This study has demonstrated that AI-driven technologies create novel challenges that current legal frameworks—both national and international—are ill-prepared to address. The rapid deployment of autonomous drone operations and smart airport systems introduces vulnerabilities that traditional aviation law, cybersecurity regulation, and international agreements inadequately cover [14].

Primarily, the absence of universally recognized definitions for key concepts such as AI autonomy, liability attribution, and malicious intent undermines effective governance. Furthermore, existing international instruments—including the Chicago Convention, ICAO standards, and the Tallinn Manual—do not sufficiently encompass the unique characteristics of AI-enabled drone operations, nor do they provide clear mechanisms for cross-border coordination in cybersecurity incidents involving autonomous systems [20].

The complex ecosystem involving multiple stakeholders—states, UAS operators, AI developers, and airport authorities—requires a shared responsibility model supported by harmonized regulations and international cooperation. In particular, the dual-use nature of drone technology, as evidenced by recent

international security challenges, underscores the urgency of developing legal frameworks that balance security, innovation, and civil liberties.

In conclusion, this research affirms that AI in aviation is not merely a technological issue but a profound legal challenge demanding anticipatory regulation, international diplomacy, and interdisciplinary collaboration. Legal systems must proactively evolve to safeguard airports and civil aviation against emerging AI-driven cybersecurity risks, ensuring resilience and global stability in an increasingly autonomous airspace.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] J. Smith, Artificial intelligence and aviation safety, Journal of Aviation Technology 45 (2022) 123–140.

[2] V. Larin, et al., Prediction of the final discharge of the uav battery based on fuzzy logic estimation of information and influencing parameters, in: IEEE 3rd KhPI Week on Advanced Technology, 2022, pp. 1–6. doi:10.1109/KhPIWeek57572.2022.9916490.

[3] L. Chen, R. Kumar, Drone technology and operational automation: A technical review, Aerospace Systems 39 (2023) 88–105.

[4] I. Ostroumov, et al., Relative navigation for vehicle formation movement, in: IEEE 3rd KhPI Week on Advanced Technology, 2022, pp. 1–4. doi:10.1109/KhPIWeek57572.2022.9916414.

[5] European Aviation Safety Agency (EASA), Integration of Drones in European Airspace, Technical Report 2023/14, EASA, 2023.

[6] P. Jackson, Y. Zhao, Legal challenges in UAS airspace management, International Journal of Air Law 12 (2021) 77–95.

[7] Federal Aviation Administration (FAA), Remote identification of unmanned aircraft, Federal Register 85 (2020) 29700–29745.

[8] European Parliament and Council, Regulation (EU) 2019/947 on the rules and procedures for the operation of unmanned aircraft, 2019. Official Journal of the European Union.

[9] European Parliament and Council, Regulation (EU) 2021/664 establishing the U-space framework, 2021. Official Journal of the European Union.

[10] D. Walker, Gaps in AI regulation for UAS operations at airports, Aviation Law Review 30 (2022) 35–52.

[11] NASA UTM Project, Unmanned Aircraft Systems Traffic Management Concept, Technical Report TP-2022-146, NASA, 2022.

[12] S. Lee, J. Park, AI in predictive maintenance of aircraft, IEEE Transactions on Aerospace 59 (2023) 23–36.

[13] SESAR Joint Undertaking, UAS Traffic Management – Autonomous Flight Operations, Technical Report SR-2021-07, SESAR, 2021.

[14] T. Brown, H. Nguyen, Legal implications of autonomous drones in civil airspace, Law and Technology Journal 19 (2023) 101–118.

[15] M. O'Connor, Liability models in AI-driven aviation systems, Harvard Journal of Law & Technology 35 (2022) 89–115.

[16] A. Zaporozhets, V. Babak, V. Isaienko, K. Babikova, Analysis of the air pollution monitoring system in ukraine, in: Studies in Systems, Decision and Control, volume 298, Springer, 2020, pp. 85–110. doi:10.1007/978-3-030-48583-2_6.

[17] K. Smithson, Distributed responsibility and AI agents in aviation law, Oxford Legal Studies 27 (2023) 203–221.

[18] International Air Transport Association (IATA), Smart Airports and Emerging Cyber Threats, Technical Report, IATA, 2023. IATA Cybersecurity Report.
[19] European Aviation Safety Agency (EASA), Cybersecurity in Airport Operations, Technical Report WP-2023-05, EASA, 2023. EASA White Paper.
[20] M. N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017.
[21] D. Kim, H. Albrecht, Governance challenges in counter-UAS protocols, Journal of Security Studies 44 (2022) 140–158.
[22] P. Green, F. Liu, Towards integrated legal-technical frameworks for UAS, International Journal of Critical Infrastructure Protection 15 (2024) 50–67.
[23] R. Torres, A. Smith, International cooperation in AI-powered drone regulation, Global Governance Review 10 (2024) 77–95.
[24] International Civil Aviation Organization (ICAO), Convention on International Civil Aviation (Chicago Convention), incl. Annex 17 on security, 1944.
[25] European Union Agency for Cybersecurity (ENISA), Cybersecurity in the Aviation Sector: Threat Landscape, Technical Report, ENISA, 2023.
[26] S. McBride, AI and Civil Liability: Towards a New Legal Framework for Autonomous Systems, Oxford University Press, 2021.
[27] U. Pagallo, The Laws of Robots: Crimes, Contracts, and Torts, Springer, 2019.
[28] European Commission, Regulation (EU) 2019/881 on ENISA and on cybersecurity certification (cybersecurity act); directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS2), 2019.
[29] Ukrainian Ministry of Digital Transformation, White Paper on Civil-Military Drone Use in Ukraine, Technical Report, Ministry of Digital Transformation, Kyiv, 2023.
[30] Cybersecurity of Aviation Infrastructure in Wartime: Analytical Report, Technical Report, Center for Strategic Cybersecurity Studies of Ukraine, Kyiv, 2024.
[31] I. Petrova, S. Ivanov, Harmonization of Ukraine's national legislation with international standards in drone security, Legal Journal of Ukraine (2024) 112–120.
[32] European Union Aviation Safety Agency (EASA), Drone incident at gatwick airport: Summary of disruptions and regulatory gaps, https://www.easa.europa.eu/, 2019.
[33] S. Truxal, Air Transport – A Critical Introduction, Routledge, 2019.
[34] Deutsche Flugsicherung (DFS), Frankfurt Airport Drone Disruption Report, Technical Report, Frankfurt, 2022. Internal Communication.
[35] ENAIRE, Drone Activity in Restricted Airspace Near Madrid-Barajas Airport, Technical Report Safety Bulletin No. 28, Madrid, 2023.